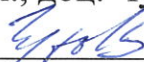


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ У МЕДИЦИНІ ТА ТЕЛЕКОМУНІКАЦІЯХ

УДК 629.97:629.389

«Допущено до захисту»

Завідувач кафедри
комп'ютерних технологій у
медицині та телекомунікаціях
к.т.н., доц. Чухов В.В.


« 19 » 12 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

на тему "Дослідження методики захисту передачі інформації в локальній мережі"

за спеціальністю 172 «Телекомунікації та радіотехніка»

освітній ступінь «магістр»

Виконавець роботи
студент 2 курсу, гр. ГРМ-22-1


(дата, підпис)

Боцян К.В.

Керівник роботи
к.т.н., доц.


(дата, підпис)

Ципоренко В.В.

Житомир
2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ У МЕДИЦИНІ ТА ТЕЛЕКОМУНІКАЦІЯХ

Пояснювальна записка

до кваліфікаційної магістерської роботи

на тему "Дослідження методики захисту передачі інформації в локальній мережі"

Виконав: студент 2 курсу,
групи ТРм-22-1 спеціальності
172 «Телекомунікації та радіотехніка»

Боцян К.В. _____

Керівник Ципоренко В.В. _____

Рецензент Коренівська О.Л. _____

Житомир
2023

«Затверджено»

Завідувач кафедри комп'ютерних
технологій у медицині та
телекомунікаціях

 Владислав ЧУХОВ
« 27 » 10 2022 р.

Завдання на кваліфікаційну магістерську роботу

Боцян Катерина Вячеславівна

(прізвище, ім'я, по батькові)

1. Тема роботи: «Дослідження методики захисту передачі інформації в локальній мережі».

Затверджено наказом по університету від «22» листопада 2023 р. № 679

2. Мета дослідження: аналіз та реалізація методів протидії зловмисному доступу до інформації в локальній мережі.

3. Основні задачі дослідження :

- аналіз загроз втрати інформації в комп'ютерних мережах;
- технології виявлення несанкціонованого вторгнення в комп'ютерній мережі;
- реалізація реактивної системи протидії несанкціонованому доступу.

4. Термін подання роботи до захисту грудень 2023 р.

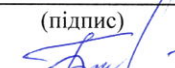
5. Дата видачі завдання «21» 01 2023 р.

Науковий керівник


(підпис)

Ципоренко В.В.
(прізвище, ініціали)

Завдання прийняв
до виконання


(підпис)

Боцян К.В.
(прізвище, ініціали)

АНОТАЦІЯ

Темою даної кваліфікаційної роботи є дослідження методики захисту передачі інформації в локальній мережі.

Дана робота дозволить отримати програмну модель та алгоритм, результати дослідження реактивного захисту інформації в локальній мережі.

ANNOTATION

The topic of this qualification work is the study of the method of protection of information transmission in the local network.

This work will make it possible to obtain a software model and algorithm, research results of reactive protection of information in local networks.

РЕФЕРАТ

Робота присвячена дослідженню методики захисту передачі інформації в локальній мережі.

Перший розділ присвячено аналізу загроз втрати інформації в комп'ютерних мережах.

Другий розділ містить розробку технологій виявлення несанкціонованого доступу до інформації в комп'ютерній мережі.

Третій розділ містить дослідження та реалізація реактивної системи протидії несанкціонованому доступу.

Об'єкт дослідження – процес захисту інформації в локальній комп'ютерній мережі.

Предмет дослідження – розроблення програмного забезпечення та налаштування систем безпеки для захисту інформації в локальній комп'ютерній мережі.

Метою є аналіз та реалізація методів протидії зловмисному доступу до інформації в локальній мережі.

Для досягнення даної мети необхідно виконати наступні **завдання**:

- аналіз загроз втрати інформації в комп'ютерних мережах;
- технології виявлення несанкціонованого вторгнення в комп'ютерній мережі;
- реалізація реактивної системи протидії несанкціонованому доступу.

Методи дослідження: розробка програмного забезпечення для захисту інформації в локальній комп'ютерній мережі.

Встановлено, що розроблена програмна система дозволяє за короткий час виявити дії зловмисника і встановлених ним програм.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ	8
ВСТУП	
РОЗДІЛ 1 АНАЛІЗ ЗАГРОЗ ВТРАТИ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ....	13
1.1. Аналіз способів проникнення у внутрішню мережу компанії і способів протидії ним.	13
1.1.1. Приклади проникнення в комп'ютерні мережі	1
3	
1.1.2. Принципи <i>DDos</i> атак на комп'ютерну мережу	1
8	
1.1.3. Протидія атакам засобами системи <i>Cisco Stealthwatch</i>	2
4	
1.1.4. Технології <i>Encrypted Traffic Analytics</i>	3
0	
1.1.5. Методи захисту від <i>DDoS</i>	3
1	
Висновки за розділом	36
РОЗДІЛ 2 ТЕХНОЛОГІЇ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ МЕРЕЖІ	37
2.1. Проблеми реактивного захисту в системах промислової автоматизації	37

2.2. Вимоги до реактивного захисту в системах промислової автоматизації	39
2.3. Захист кінцевих точок від складних кібератак	41
2.4. Методи протидії несанкціонованому доступу шляхом використання EDR та XDR	43
Висновки за розділом	48

РОЗДІЛ 3 РЕАЛІЗАЦІЯ РЕАКТИВНОЇ СИСТЕМИ ПРОТИДІЇ

НЕСАНКЦІОНОВАНОМУ ДОСТУПУ	49
3.1. Концепція реактивного захисту для систем промислової автоматизації	49
3.1.1. Попередні вимоги та обмеження системи реактивного захисту	4
3.1.2. Компоненти системи реактивного захисту	5
3.2. Політика безпеки, операційна політика та реактивні дії в реальних системах автоматизації	52
3.2.1. Політика безпеки	5
3.2.2. Оперативні політики	5
3.2.3. Реактивні дії	5

3.2.4. Реактивний захист сегмента мережі	5
8	
3.3. Інтеграція технологій захисту інформації в системи промислової автоматизації	60
3.3.1. Політика безпеки та вторгнення	6
2	
3.3.2. Реактивні дії за наявності вторгнень	6
4	
3.4. Реалізація системи реактищщного захисту інформації комп'ютерної мережі	66
3.5. Оцінка доцільності та застосовності Концепції реактивного захисту	67
3.5.1. Сценарій і модель змагальності	6
8	
3.5.2. Емуляція тестового сценарію	6
9	
3.5.3. Варіанти використання сценарію	7
0	
3.6. Налаштування корпоративної мережі для розширеного захисту	71
3.6.1. Описання атак на корпоративні сервери	7
2	
3.6.2. Описання атак на сервери баз даних <i>SQL/MySQL</i>	7

3	
3.6.3. Описання атаки через віддалене підключення до робочого столу	7
4	
3.6.4. Описання атак на доменні та файлові сервери	7
4	
3.6.5. Приклад налаштування розширеного захисту в <i>Adaptive Defense 360</i>	7
6	
Висновки за розділом	84
ВИСНОВКИ	
СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ	89
Перелік умовних позначень, скорочень, термінів	
<i>ARP</i>	– <i>Address Resolution Protocol</i> (протокол канального рівня, служить для визначення MAC-адреси отримувача)
<i>BGP</i>	– <i>Border Gateway Protocol</i> (основний протокол динамічної маршрутизації в Інтернеті)
<i>FDB</i>	– <i>Forwarding DataBase</i> (таблиця комутації)
<i>MAC</i>	– <i>Media Access Control</i> (унікальний ідентифікатор, який присвоюється кожному вузлу комп'ютерних мереж)
<i>OSPF</i>	– <i>Open Shortest Path First</i> (протокол динамічної маршрутизації, який використовує Алгоритм Дейкстри)
<i>PAP</i>	– <i>Password Authentication Protocol</i> (протокол простої перевірки автентифікації)

<i>PoE</i>	–	<i>Power over Ethernet</i> (технологія передачі харчування по <i>Ethernet</i>)
<i>RIP</i>	–	<i>Routing Information Protocol</i> (протокол маршрутної інформації)
<i>VLAN</i>	–	<i>Virtual Local Area Network</i> (віртуальна локальна мережа)
KIC	–	корпоративна інформаційна система

ВСТУП

За останнє десятиліття інтеграція безпеки в системи промислової автоматизації (IAS) перетворилася з товару на необхідність. Це сталося завдяки новим технологічним досягненням і тенденціям, які призвели до посилення стандартизації та взаємозв'язку систем (наприклад, Індустрія 4.0 [1]), які породжують нові загрози та вразливості, які можуть бути використані, щоб поставити під загрозу безпеку таких систем [2,3]. Ця безпека складається з набору політик безпеки та інших механізмів безпеки, які дозволяють застосовувати такі політики. Ці політики безпеки представляють собою набір правил, які вказують, як система має бути захищена [2]. Вони можуть включати, але не обмежуючись ними, дозволу чи несанкціоновану поведінку щодо фізичної безпеки, контролю доступу користувачів і мережі тощо [[2].

Вважається, що безпека системи скомпрометована, коли її політика безпеки була порушена або її механізми безпеки були обхідні. Ці події часто називають вторгненнями [6]. Щоб зменшити або протидіяти впливу, який такі вторгнення можуть мати на цільову систему, рекомендується виявляти їх, як тільки вони трапляються. Існує багато рішень безпеки, які дозволяють виконувати такі дії (наприклад, перевірки цілісності файлів, антивіруси, системи керування подіями та авторизацією користувачів тощо). Однак сфера захисту деяких з них обмежена, оскільки вони можуть зосередитися на конкретних компонентах системи. Прикладом цього є засоби перевірки цілісності файлів (*FIC*). *FIC* здатні виявляти лише вторгнення, які відбуваються на рівні файлової системи. Інші рішення, такі як системи виявлення вторгнень (*IDS*), забезпечують більш широкий спектр захисту, оскільки вони спеціалізуються на виявленні вторгнень на рівні мережі та хоста. однак,

Ці пасивні реакції на вторгнення часто вимагають подальшого аналізу або людського втручання, щоб протидіяти наслідкам вторгнення [7], що призводить до уповільнених реакцій. Ці відстрочені реакції можуть забезпечити достатньо часу для успішного вторгнення. Успішне вторгнення є особливо клопітним при роботі з критичними системами, такими як промислові кібер-фізичні системи (промислові *CPS*). Ці типи систем є системами автоматизації, що складаються з фізичної (тобто, блоку керування, датчиків, виконавчих механізмів тощо) та кібернетичної частини (тобто, керуючого програмного забезпечення), які дозволяють фізичній частині взаємодіяти з реальним світом [8,9]. Отже, пасивних відповідей може бути недостатньо для захисту цих систем через катастрофічні наслідки, які можуть мати на них вторгнення в систему безпеки. Деякі з цих наслідків можуть негативно вплинути на навколишнє середовище навколо цих систем і створити великий ризик для нормальної роботи, що призведе до грошових втрат, проблем безпеки або політичних наслідків [10,11]. Тому часто потрібне рішення безпеки, здатне не тільки виявляти вторгнення, але й активно реагувати на нього після його виявлення, щоб захистити систему.

Хоча існують рішення безпеки (наприклад, системи запобігання

вторгненням, системи реагування на вторгнення, система управління інцидентами безпеки та подіями тощо), здатні автоматично й активно реагувати на вторгнення, їх інтеграція в *IAS* часто не помічається. Це сталося через занепокоєння, що деякі реактивні дії за наявності вторгнень можуть вплинути на експлуатаційні вимоги *IAS* [12,13,14].

Ця дипломна робота намагається вирішити цю проблему та подолати інші проблеми, пов'язані з реактивним захистом, які існують в *IAS*, шляхом впровадження нової концепції реактивного захисту. Ця концепція є основним внеском цієї дипломної роботи. Він складається з архітектури для системи реактивного захисту, здатної автоматично виконувати активні відповіді за наявності вторгнень. Виконання цих дій не впливає негативно на роботу *IAS* через врахування операційної політики. Ця концепція також передбачає інші тенденції безпеки та архітектури *IAS*. Більш конкретно, він інтегрує управління як безпекою, так і операційною політикою на основі мережевої зони, яка відповідає стандартам серії *ISA/IEC 62443* Міжнародного товариства автоматизації (*ISA*) та Міжнародної електротехнічної комісії (*IEC*). Таким чином, надаючи здійснення та відповідне рішення, здатне забезпечити активний захист у режимі реального часу від вторгнень у систему безпеки. Доцільність і застосовність представленої концепції реактивного захисту продемонстровано за допомогою прототипової реалізації Системи реактивного захисту та тестового сценарію з урахуванням програми віддаленого обслуговування.

З огляду на вищесказане визначимо мету, об'єкт та предмет дослідження.

Об'єкт дослідження – процес захисту інформації в локальній комп'ютерній мережі.

Предмет дослідження – розроблення програмного забезпечення та налаштування систем безпеки для захисту інформації в локальній комп'ютерній мережі.

Мета дипломної роботи – аналіз та реалізація методів протидії

зловмисному доступу до інформації в локальній мережі.

Метод дослідження – розробка програмного забезпечення для захисту інформації в локальній комп'ютерній мережі.

РОЗДІЛ 1

АНАЛІЗ ЗАГРОЗ ВТРАТИ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

1.1. Аналіз способів проникнення у внутрішню мережу компанії і способів протидії ним

1.1.1. Приклади проникнення в комп'ютерні мережі

Роздивимось варіанти проникнення у корпоративну мережу і в яких випадках ваш *Firewall* вам ніяк не допоможе.

Один із прикладів, з яким компанії *Cisco* вдалося зіткнутися, - це використання протоколу *DNS* для крадіжки інформації.

Зазвичай зловмисники використовують протокол *DNS* для того, щоб підвантажувати якісь нові модулі, або використовувати *DNS* як взаємодію вже встановлених модулів усередині корпоративної/відомчої мережі на заражених комп'ютерах з деякими «командними серверами». У цьому випадку протокол *DNS* використовувався у тому, щоб у назві домену відбувався витік інформації. За статистикою, більшість доменів, імен доменів третього рівня містять не більше 25-30 символів, проте, бачимо що у правому графіку ми довжини доменів становлять 200-230 символів.

Людина не здатна вигадати такого роду домен. Запам'ятати його він теж не спроможний. Це в чистому вигляді якась «аномалія» яка може нам говорити про те, що використовуються деякі домени для якихось маркетингових цілей, але зазвичай такі довгі навіть в маркетингових цілях не використовуються, або це дії зловмисників.

В даному випадку 1 з *DNS*-серверів, що обслуговує цей шкідливий домен, якраз і використовувався для того, щоб назви доменів, що містять досить довгі текстові рядки (231 символ), були розшифровані, і в них виявляли вкрадені номери кредитних карток. Як ми розуміємо, враховуючи, що *DNS* є стандартом де-факто для роботи сучасної мережі інтернет, корпоративної чи відомчої мережі, заблокувати *DNS* ми не можемо і навіть інспекція *DNS* на *Firewall*-і далеко не завжди нам допомагає,

Коли компанія *Cisco* суттєво змінила архітектуру безпеки мережного обладнання. Були додані програмно-апаратні компоненти, які дозволяють відслідковувати закладки в устаткуванні, а також запобігати появі цих закладок, але на початку двохтисячних років такі приклади були.

Їх було кілька, які вдалося зафіксувати, і в даному випадку ми стикаємося із ситуацією, коли в рамках якогось постачання замовник отримує обладнання з уже встановленим шкідливим кодом. Оскільки він спочатку довіряє своєму постачальнику, він не замислюється над тим, що треба перевірити мережеве обладнання. Перевірку можна здійснити через програмне забезпечення, яке замовник може завантажити з офіційного сайту. Потрібно це для того, щоб переконатися, що в обладнанні немає жодних закладок, і воно не краде інформацію, яка передається через мережевий пристрій. Також було кілька випадків, коли адміністратори, не маючи контракту на технічну підтримку на придбане ними обладнання, змушені були завантажувати нові прошивки зі сторонніх сайтів. Це також призводило до того, що в цих прошивках містився шкідливий код, який «дзеркував» весь трафік та відправляв його зловмиснику. Тобто в даному випадку ми також розуміємо, що класичні засоби безпеки не можуть нічого з цим зробити, тому що закладки знаходяться на обладнанні, що стоїть перед міжмережевими екранами.

Один з прикладів атаки, коли компанія *Cisco* (її підрозділ *Cisco Talos*) виявила загрозу під назвою *VPN-Filter*, коли зловмисники заражали різні мережеві пристрої різних виробників (*D-Link*, *Asus* і так далі) і встановлювали на них відповідний шкідливий код, який також крав трафік і перенаправляв

його зловмисникам. Тобто недооцінка цієї проблеми призводить до того, що у нас нижній рівень мережевої інфраструктури залишається абсолютно не захищеним, і ніякі *Firewall*-и, зрозуміло, тут не допомагають, оскільки мережеві пристрої знаходяться до *Firewall*-ів, вони можуть передавати весь трафік, особливо якщо він не зашифрований, зловмисникам.

У 2017 році зловмисники знайшли вразливість на *Web*-порталі одного з найбільших кредитних бюро *Equifax*. Ця вразливість дозволила отримати доступ до *Web*-порталу та виконувати на ньому деякі команди. Після ідентифікації вразливості зловмисники запустили експлоїт та отримали доступ до системи з адміністративними правами. Жодних даних викрадено на той момент ще не було. Тобто зловмисники лише протестували можливість роботи на *Web*-порталі з адміністративними правами. А ось далі десь через 2 місяці вразливість, яка з якихось причин не була усунена, була проексплуатована.

Зловмисники проникли у внутрішні системи кредитного бюро та замаскували свою діяльність від засобів мережевої безпеки. По-перше, за рахунок довірчих відносин між *Web*-порталом та внутрішніми серверами, у тому числі серверами баз даних, система захисту ніяк не контролювала дані з'єднання та пропустила зловмисника всередину корпоративної мережі. Крім того, зловмисники використовували зашифроване з'єднання і воно залишилося безконтрольним з точки зору засобів мережевої безпеки.

Зловмисникам протягом кількох місяців вдавалося красти інформацію, внаслідок чого постраждало понад 140 мільйонів громадян США, Великобританії та інших країн, чиї дані були вкрадені в результаті даної атаки, незважаючи на наявність засобів захисту периметра, які, на жаль, в даному випадку ніяк не допомогли.

Ще один приклад, що стався у 2018 року, коли в двотижневий період між 21 серпня і 5 вересня хакерська група під назвою *Magic Art* зламала сервери авіакомпанії *British Airways*, викрала дані 380 000 клієнтів, включаючи персональні дані та дані кредитних карток. За даними *British Airways*, постраждали близько півмільйона клієнтів за два тижні.

Зловмисники навіть не намагалися проникнути в корпоративну мережу. Вони зламали сайт авіакомпанії, підмінили скрипт, який збирав дані клієнтів, і переслали ці дані на шкідливий ресурс, який контролювали зловмисники. Також в одній з версій цього інциденту розглядається, що зловмисники зламали не основний сайт *British Airways*, а його копію кешування (CDN, використовуваний провайдерами зв'язку для кешування популярних ресурсів). Таким чином, периметрові засоби захисту не допомогли захиститися від цієї атаки.

Ще одна атака, яку називали «водопій» (*water hole*), яка була зафіксована деякий час тому американськими правоохоронними органами. Зафіксували атаки на ряд енергетичних компаній у Сполучених Штатах Америки, і в рамках розслідування було виявлено дуже нестандартну схему, яка, проте, з того часу стала досить популярною.

Якщо ми згадаємо життя тварин (особливо тварин Африки), то під час посухи багато тварин приходять на рідкісні водопої, які не пересохли під час посухи, і природа робить так, що тварини не нападають одна на одну під час водопою, але справа в тому, що саме по дорозі на водопій хижаки дуже часто чатують на тварин і їдять їх для того, щоб прогодувати себе і свої прайди. Замість того, щоб ламати компанії-жертви, на які вони орієнтують свої зусилля, а таких компаній може бути багато (одиниці, десятки або навіть сотні), іноді достатньо зламати всього лише одного виробника програмного забезпечення. Забезпечення, із сайту якого потім всі починають завантажувати оновлення програмного забезпечення (нові прошивки, патчі, апдейти або нові версії софту). Якщо зламали саме виробника, то далі разом із цими оновленнями, які завантажуються з його сайту, можна розмістити в мережі компанії-жертви ще й шкідливий код, який потім полегшує хакерам розвиток плацдарму всередині вже скомпрометованої мережі жертвою. Тобто таким манівцем, але хакери досягли своєї мети. Така атака була зафіксована в 2016 році в Сполучених Штатах Америки. Після цього було кілька схожих сценаріїв. Було зафіксовано атаку на компанію *Asus*, яка зі свого сайту розповсюджувала шкідливі

оновлення. Те саме робилося в компанії *Avast*, яка розповсюджувала заражену програму для дефрагментації та оптимізації роботи системи під назвою *CCleaner*.

18 червня 2019 року аерокосмічне агентство НАСА зафіксувала та оголосила про те, що у внутрішню мережу одного з її підрозділів (одного з її лабораторій) проникли хакери ще у квітні 2018 року. Тобто вони протягом тривалого часу залишалися непоміченими та змогли вкрати понад 500 МБ даних щодо місії на Марс. Найцікавіше, що сталося це за рахунок впровадження апаратного портативного комп'ютера *Raspberry Pi*, який був встановлений у мережі НАСА, який крав інформацію та передавав її назовні.

Ось всі ці приклади дуже добре демонструє, що навіть наявність дуже потужних, добре спроектованих, грамотно спроектованих систем захисту периметра не дає гарантії, що зловмисники не проникнуть.

Є частина каналів, які залишаються за рамками розгляду (припустимо, звичайне *VPN*-з'єднання, або *site-to-site VPN* з віддаленими майданчиками, або *Remote Access VPN* з віддаленими користувачами), але в разі наявності захищеного з'єднання по ньому, крім легального трафіку, може проникнути та впровадитись у внутрішню мережу компанії. *USB*-флешки, підкинуті на парковці перед входом в організацію, також є улюбленим інструментом, яким користуються зловмисники для того, щоб обійти периметрові засоби корпоративної інформаційної безпеки або відомчої інформаційної безпеки, тому що флешка, будучи встроєна в комп'ютер, обходить всі периметрові засоби захисту. Залишається сподіватися тільки на те, що на комп'ютері встановлено щось сучасніше, ніж застарілий за ідеологією антивірус.

Генеральний директор великої української енергетичної компанії "заразився" на своєму домашньому ноутбукі шкідливим кодом *WannaCry*. Це сталося в п'ятницю ввечері, якраз коли *WannaCry* став поширюватися світом. У суботу вранці директор привіз заражений ноутбук.

Поки ці фахівці, терміново викликані генеральним директором, їхали на роботу, шкідливий код встиг поширитися корпоративною мережею, тому що

генеральний директор підключив цей ноутбук до корпоративної мережі. Автоматом він підключився, після чого навіть ізольована від зовнішнього світу, корпоративна мережа постраждала від *WannaCry*.

Якщо організація активно використовує хмари, жодні корпоративні засоби захисту периметра не допоможуть. Необхідно розширювати систему забезпечення безпеки за межі периметра та здійснювати моніторинг внутрішньої інфраструктури.

Допоможе в цьому протокол *NetFlow*, який спочатку розроблявся для траблшутинга, для аналізу статистики мережного трафіку, але за рахунок своїх можливостей, особливо за рахунок розширених можливостей, що існують у дев'ятій версії протоколу *NetFlow*, або його стандартизованої версії *IPFIX*, з'являється можливість відповідати на запитання, які цікавлять інженерів з погляду інформаційної безпеки. Потім, наклавши на це відповідні алгоритми прийняття рішень, з'являється можливість робити висновки про наявність тієї чи іншої загрози, тієї чи іншої аномалії, які можуть бути цікавими у контексті інформаційної безпеки.

Одним із прикладів рішення, які використовують саме цю конструкцію з метою інформаційної безпеки, є рішення *Cisco Stealthwatch*. Це рішення, яке займається аналізом *Flow*-протоколів (не лише *NetFlow*). Це може бути *sFlow*, *Jflow*, *IPFIX*, *NetStream* – не має значення. Тобто це рішення працюватиме не тільки на інфраструктурі *Cisco*, але і на інфраструктурі інших вендорів (у тому числі навіть українських виробників, які підтримують протокол з *Flow*) або коли є можливість передавати трафік через *PAN* або *Airspan* на рішення *Cisco Stealthwatch*, та за рахунок аналізу існуючої інфраструктури можна виявляти ті чи інші аномалії, ті чи інші загрози в корпоративній чи відомчій мережі.

1.1.2. Принципи *DDoS* атак на комп'ютерну мережу

За даними опитування компанії *HaltDos*, *DDoS*-атаки розглядаються половиною організацій як одна з найсерйозніших кіберзагроз. Небезпека *DDoS* навіть вища, ніж небезпека несанкціонованого доступу, вірусів, шахрайства та фішингу, не кажучи про інші загрози.

Середні збитки від *DDoS*-атак оцінюються у світі в 50 тис. доларів для невеликих організацій і майже 500 тис. доларів для великих підприємств. Усунення наслідків *DDoS*-атаки вимагатиме додаткового робочого часу співробітників, відволікання ресурсів з інших проектів на забезпечення безпеки, розробки плану оновлення ПЗ, модернізації обладнання та ін.

Репутація атакованої організації може постраждати не лише через погану роботу сайту, але й через крадіжку персональних даних або фінансову інформацію.

За даними опитування компанії *HaltDos*, кількість *DDoS*-атак зростає щороку на 200%, щодня у світі повідомляють про 2 тис. атак такого типу. Вартість організації *DDoS*-атаки тижневої тривалості – близько 150 доларів, а втрати жертви в середньому перевищують 40 тис. доларів на годину.

Основні типи *DDoS*-атак: масовані атаки, атаки на протокольному рівні та атаки на рівні додатків. У будь-якому випадку мета полягає в тому, щоб вивести сайт з ладу або вкрати дані. Інший вид кіберзлочинів – загроза скоєння *DDoS*-атаки для отримання викупу. Цим славляться такі хакерські угруповання як *Armada Collective*, *Lizard Squad*, *RedDoor* та *ezBTC*.

Організація *DDoS*-атак помітно спростилася: зараз є широко доступні автоматизовані інструменти, які практично не вимагають від кіберзлочинців спеціальних знань. Існують і платні послуги *DDoS* для анонімної атаки мети. Наприклад, сервіс *vDOS* пропонує свої послуги, не перевіряючи, чи є замовник власником сайту, який бажає протестувати його «під навантаженням», чи це робиться з метою атаки.

DDoS-атаки являють собою атаки з багатьох джерел, що перешкоджають доступу легітимних користувачів до сайту, що атакується. Для цього в систему, що атакується, направляється величезна кількість запитів, з якими та впоратися не може. Зазвичай з цією метою використовуються скомпрометовані системи.

Щорічне зростання кількості *DDoS*-атак оцінюється в 50% (за даними www.leaseweb.com), але дані різних джерел розходяться, і не всі інциденти стають відомими. Середня потужність *DDoS*-атак *Layer 3/4* зросла останніми

роками з 20 до кількох сотень Гбайт/с. Хоча масові DDoS-атаки та атаки на рівні протоколів вже самі по собі – штука неприємна, кіберзлочинці все частіше комбінують їх із DDoS-атаками *Layer 7*, тобто на рівні додатків, які націлені на зміну чи крадіжку даних. Такі «багатовекторні» атаки можуть бути дуже ефективними. Багатовекторні атаки становлять 27% від загальної кількості атак DDoS.

У разі масової DDoS-атаки (*volume based*) використовується велика кількість запитів, які нерідко надсилаються з легітимних IP-адрес, щоб сайт «захлинувся» у трафіку. Мета таких атак - "забити" всю доступну смугу пропускання та перекрити легітимний трафік.

У разі атаки на рівні протоколу (наприклад, *UDP* чи *ICMP*) метою є вичерпання ресурсів системи. Для цього надсилаються відкриті запити, наприклад, запити *TCP/IP* з підробленими IP, і в результаті вичерпання мережевих ресурсів стає неможливою обробка легітимних запитів. Типові представники - DDoS-атаки, відомі у вузьких колах як *Smurf DDos*, *Ping of Death* та *SYN flood*. Інший вид DDoS-атак протокольного рівня полягає у надсиланні великої кількості фрагментованих пакетів, з якими система не справляється.

DDoS-атаки *Layer 7* – це відправлення невинних на вигляд запитів, які виглядають як результат звичайних дій користувачів. Зазвичай для їх здійснення використовують ботнети та автоматизовані інструменти. Відомі приклади - *Slowloris*, *Apache Killer*, *Cross-site scripting*, *SQL-injection*, *Remote file injection*.

Протокол *UDP* схильний до спуфінгу – заміни адреси. Наприклад, якщо потрібно атакувати сервер *DNS* за адресою 56.26.56.26, використовуючи атаку *DNS Amplification*, можна створити набір пакетів з адресою відправника 56.26.56.26 і відправити їх DNS-серверам по всьому світу. Ці сервери надішлють відповідь за адресою 56.26.56.26.

Той самий метод працює для серверів *NTP*, пристроїв із підтримкою *SSDP*. Протокол *NTP* – чи не найпопулярніший метод: у другій половині 2016

року він використовувався в 97,5% *DDoS*-атак. Правило *Best Current Practice (BCP) 38* рекомендує провайдерам конфігурувати шлюзи для запобігання спуфінгу – контролюється адреса відправника. Але такої практики йдуть не всі країни. Крім того, атакуючі обходять контроль *BCP 38*, переходячи на атаки типу *Stateful*, на рівні *TCP*. За даними *F5 Security Operations Center (SOC)*, останні п'ять років такі атаки домінують. У 2016 році *TCP*-атак було вдвічі більше, ніж атак із використанням *UDP*.

До атак *Layer 7* вдаються переважно професійні хакери. Принцип наступний: береться «важкий» *URL* (з *PDF* або запитом до великої БД) і повторюється десятки або сотні разів на секунду. Атаки *Layer 7* мають тяжкі наслідки та важко розпізнаються. Нині вони становлять близько 10% *DDoS*-атак.

Співвідношення різних типів *DDoS*-атак за даними звіту *Verizon Data Breach Investigations Report (DBIR)*.

Нерідко *DDoS*-атаки приурочують до періодів пікового трафіку, наприклад до днів інтернет-розпродажів. Великі потоки персональних та фінансових даних у цей час приваблюють хакерів.

Доменна система імен (*Domain Name System, DNS*) відіграє фундаментальну роль у продуктивності та доступності сайту. Зрештою – в успіху вашого бізнесу. На жаль, інфраструктура *DNS* часто стає метою *DDoS*-атак. Пригнічуючи інфраструктуру *DNS*, зловмисники можуть зашкодити вашому сайту, репутації вашої компанії та вплинути на її фінансові показники. Щоб протистояти сучасним загрозам, інфраструктура *DNS* має бути дуже стійкою та масштабованою.

По суті, *DNS* – розподілена база даних, яка, крім іншого, ставить у відповідність зручні для читання імена сайтів *IP*-адрес, що дозволяє користувачеві потрапити на потрібний сайт після введення *URL*. Перша взаємодія користувача з сайтом починається з *DNS*-запитів, що надсилаються на сервер *DNS* з адресою домену вашого сайту. На їхню обробку може припадати до 50% часу завантаження веб-сторінки. Таким чином, зниження

продуктивності *DNS* може призводити до відходу користувачів із сайту та втрат для бізнесу. Якщо ваш сервер *DNS* перестав відповідати в результаті *DDoS*-атаки, то на сайт ніхто не зможе потрапити.

DDoS-атаки важко знайти, особливо спочатку, коли трафік виглядає нормальним. Інфраструктура *DNS* може піддаватися різним типам *DDoS*-атак. Інколи це пряма атака на сервери *DNS*. В інших випадках використовують експлойти, задіявши *DNS* системи для атаки на інші елементи ІТ-інфраструктури або сервіси.

При атаках *DNS Reflection* ціль піддається масованим підробленим відповідям *DNS*. Для цього застосовують бот-мережі, заражаючи сотні та тисячі комп'ютерів. Кожен бот в такій мережі генерує кілька *DNS*-запитів, але як *IP* джерело використовує ту саму *IP*-адресу мети (спуфінг). *DNS*-сервіс відповідає за цією *IP*-адресою.

При цьому досягається подвійний ефект. Цільову систему бомбардують тисячі та мільйони відповідей *DNS*, а *DNS*-сервер може «лягти», не впоравшись із навантаженням. Сам запит *DNS* - це зазвичай менше 50 байт, відповідь же раз на десять довша. Крім того, повідомлення *DNS* можуть містити чимало іншої інформації.

Припустимо, що атакуючий видав 100 000 коротких запитів *DNS* по 50 байт (всього 5 Мбайт). Якщо кожен відповідь містить 1 Кбайт, то сумі це вже 100 Мбайт. Звідси назва – *Amplification* (посилення). Комбінація атак *DNS Reflection* та *Amplification* може мати дуже серйозні наслідки.

Запити виглядають як звичайний трафік, а відповіді – це безліч повідомлень великого розміру, що спрямовуються на цільову систему.

Для захисту насамперед, не варто відкладати це «на потім». Якись заходи слід брати до уваги при конфігуруванні мережі, запуску серверів та розгортанні програмного забезпечення. І кожна наступна зміна не повинна збільшувати вразливість від *DDoS*-атак.

Безпека програмного коду. При написанні програмного забезпечення повинні братися до уваги міркування безпеки. Рекомендується дотримуватися

стандартів «безпечного кодування» та ретельно тестувати програмне забезпечення, щоб уникнути типових помилок та вразливостей, таких як міжсайтові скрипти та *SQL*-ін'єкції.

Розробте план дій під час оновлення програмного забезпечення. Завжди має бути можливість "відкату" у тому випадку, якщо щось піде не так.

Не забувайте про обмеження доступу. Аккаунти *admin* та/або повинні бути захищені сильними та регулярно змінюваними паролями. Необхідний також періодичний аудит прав доступу, своєчасне видалення акаунтів співробітників, що звільнилися.

Інтерфейс адміністратора повинен бути доступний лише з внутрішньої мережі або через *VPN*. Вчасно закривайте *VPN*-доступ для звільнених і звільнених співробітників.

Увімкніть усунення наслідків *DDoS*-атак у план аварійного відновлення. План має передбачати способи виявлення факту такої атаки, контакти для зв'язку з інтернет-або хостинг-провайдером, дерево «ескалації проблеми» для кожного департаменту.

Сканування на наявність вразливостей допоможе виявити проблеми у вашій інфраструктурі та програмному забезпеченні, знизити ризики. Простий тест *OWASP Top 10 Vulnerability* виявить найкритичніші проблеми. Корисними будуть тести на проникнення – вони допоможуть знайти слабкі місця.

Апаратні засоби захисту від *DDoS*-атак можуть бути недешеві. Якщо ваш бюджет такого не передбачає, то є хороша альтернатива – захист від *DDoS* «на вимогу». Таку послугу можна включати простою зміною схеми маршрутизації трафіку в екстреній ситуації, або перебуває під захистом постійно.

Використовуйте *CDN*-партнера. Мережі доставки контенту (*Content Delivery Network*) дозволяють доставляти контент сайту за допомогою розподіленої мережі. Трафік розподіляється по безлічі серверів, зменшується затримка доступу користувачів, зокрема географічно віддалених. Таким чином, хоча основна перевага *CDN* – це швидкість, вона є також бар'єром між основним сервером та користувачами.

Використовуйте *Web Application Firewall* – файл для веб-додатків. Він моніторить трафік між сайтом або програмою та браузером, перевіряючи легітимність запитів. Працюючи на рівні додатків, *WAF* може виявляти атаки по шаблонах, що зберігаються, і виявляти незвичайну поведінку. Атаки на рівні додатків нерідкі в електронній комерції. Як і *CDN*, можна скористатися сервісами *WAF* у хмарі. Проте конфігурування правил потребує певного досвіду. В ідеалі захистом *WAF* мають бути забезпечені всі основні програми.

1.1.3. Протидія атакам засобами системи *Cisco Stealthwatch*

Однією з ключових відмінностей даного підходу від захисту периметра є те, що адміністратору не треба ставити окремі сенсори, окремі крани у контрольних місцях мережі у контрольних точках. *Cisco* перетворює існуючу мережну інфраструктуру на таку розподілену систему моніторингу.

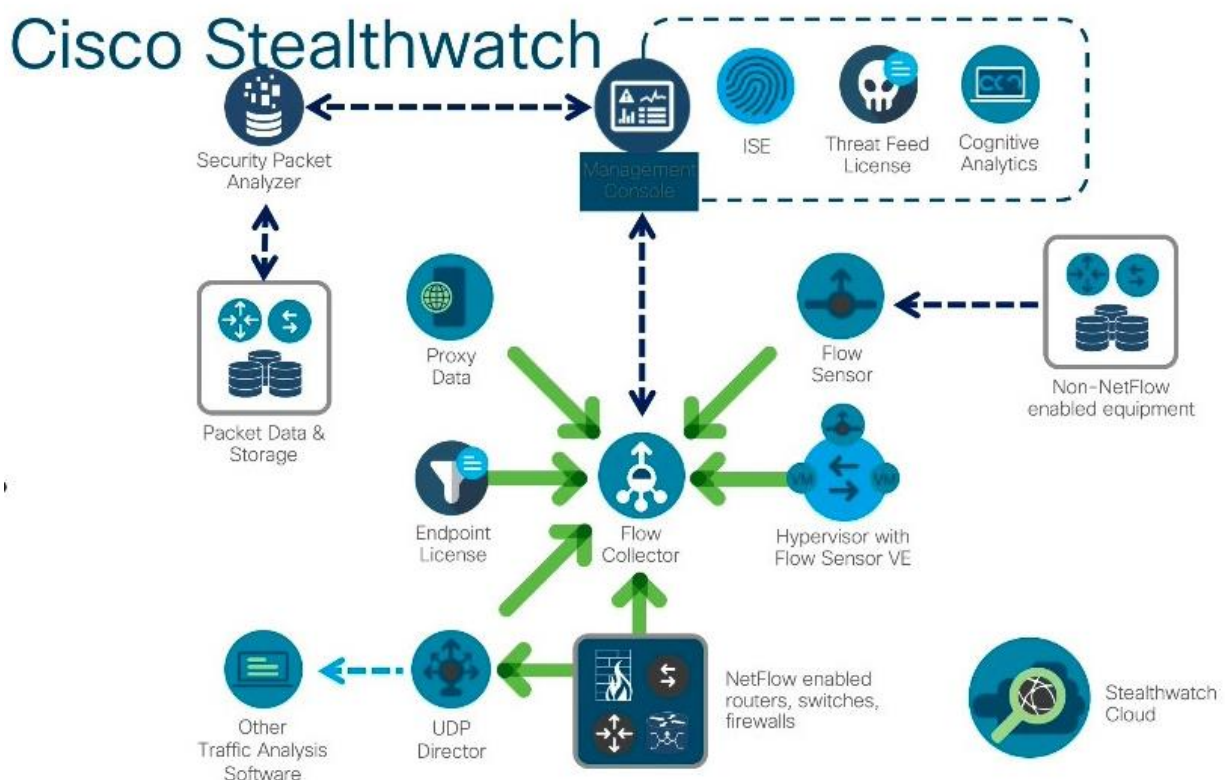


Рис. 1.1. Компоненти системи *Cisco Stealthwatch*

У своєму мінімальному варіанті рішення *Cisco stealthwatch* складається з двох компонентів - *Flow Collector*, який збирає дані від пристроїв, що

підтримують *Flow* протоколи, та менеджмент консоль, яка відповідає за керування, візуалізацію, генерацію звітів і так далі. У тих випадках, коли з якихось причин пристрій або не підтримує *Flow* або підтримка включення *Flow* призводить до істотного завантаження процесора, можна використовувати так звані «*Flow* сенсори». Це апаратне або віртуальне рішення, яке пропускає через себе мережевий трафік, транслює його *NetFlow* і передає на *Flow Collector*. Тим самим, до *Flow Sensor* можна підключати чим підключати *span port* якогось обладнання, яке спочатку не підтримує *Flow* протокол і забезпечувати повну та більшу видимість внутрішньої мережі, а не лише її периметра.

Крім *Flow sensors* існує ще такий компонент як *UDP Direcot*, який дозволяє ефективно обробляти дані з віддалених майданчиків. Коли слабкий інтернет канал між віддаленими майданчиком та штаб-квартирою, але при цьому треба передавати дані *NetFlow*, *UDP Direcot* здійснює оптимізацію передачі такого трафіку.

Крім цього, компанії *Cisco* розробила спеціальний протокол *nvzFlow*, який дозволяє інтегрувати мережеву складову з хостової та за рахунок модуля *Network Visibility* модуль, який вбудований у *AnyConnect* (це програмний захисний клієнт, який встановлюється на *Windows, Linux, Mac OS, iOS, Android* і так далі)). Завдяки цьому, з'явилася можливість транслювати поведінку вузла, поведінку додатків користувачів у схожий з *NetFlow* протокол і здійснювати автоматичну кореляцію події, що відбуваються на вузлах з подіями, що відбуваються на рівні мережі, покращуючи стан моніторингу інформаційної безпеки в корпоративній або відомчій мережі.

Ще одним з елементів, який може віддавати дані на *Flow Collector*, є проксі-сервера і тим самим можна корелювати дані мережевого рівня, які виходять після аналізу *NetFlow* або інших *Flow* протоколів і прикладного рівня, які ми отримуємо від різних проксі-серверів, тим самим є можливість фіксувати роботу шифрувальників, взаємодію з командними серверами, роботу мережі мережею Тор тощо.

Для того, щоб збирати докази протиправної діяльності, для того, щоб

зберігати їх, проводити розслідування, або передавати до правоохоронних органів рішення *Cisco Stealthwatch* інтегруються з компонентом *Cisco Security Packet Analyzer*, який якраз і зберігає всю необхідну для подальшого розслідування та взаємодії з правоохоронними органами інформацію.

Найцікавіше, що дане рішення працює не тільки всередині корпоративної/відомчої мережі, не тільки всередині ЦОДу, не тільки всередині промислового майданчика (наприклад, в АСУ ТП), але також може працювати на різних хмарних платформах, тим самим єдине рішення дозволяє побачити різні ділянки корпоративної чи відомчої мережі. Побачити в них аномалії, побачити загрозою та відповідним чином сигналізувати та при необхідності блокувати ці загрози, спираючись не тільки на те, що проходить через корпоративний периметр. Якщо помічається якась флешка, незахищений *Wi-Fi*, підкинутий *Raspberry Pi* у корпоративну мережу тощо, цього не побачить периметр. Це побачить *Stealthwatch* котрий належним чином контролює все що проходить через мережну інфраструктуру. Як би зловмисниками маскувався він завжди проходитиме через комутатори та маршрутизатори, які у нас розміщені в корпоративній чи відомчій мережі. Він не може в принципі їх пройти і в цьому випадку працює *Stealthwatch*, який бачить весь мережевий трафік і за рахунок накладання великої кількості різних алгоритмів, може виявляти ті чи інші аномалії чи загрози (рис. 1.2).

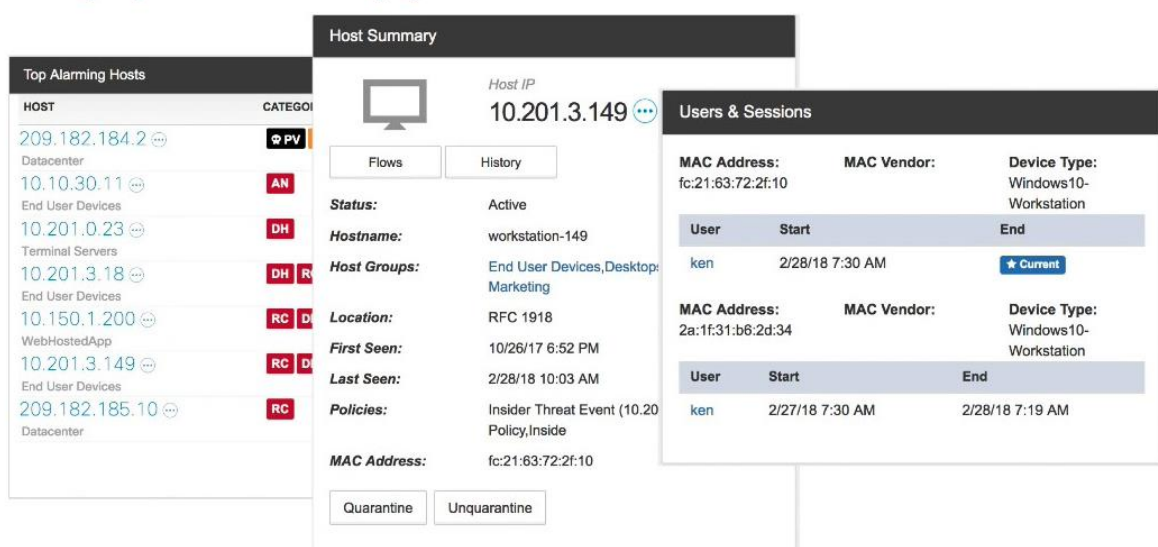


Рис. 1.2. Вікно з перехоленими діями зловмисника

На малюнку видно топ вузлів, зафіксованих за певний інтервал часу. Один із цих вузлів має адресу 10.201.3.149. Це – робоча станція. Вона знаходиться в групі пристроїв. Видно коли та яка активність відбувався на цьому вузлі. Видно, які політики застосовуються до цього вузла. Видно що користувач працює на даному вузлі, наприклад за рахунок інтеграції з *Active directory*. Таким чином, ми знаємо конкретного користувача, конкретного співробітника організації, який працює в конкретний момент на даному хості і це дозволяє оперативніше проводити розслідування інцидентів.

Якщо бачимо події з дуже високим рівнем підозрілості, так званий «*Concern Index*» і хочемо отримати більш детальну інформацію про те, що ховається за даною подією (рис. 1.3).

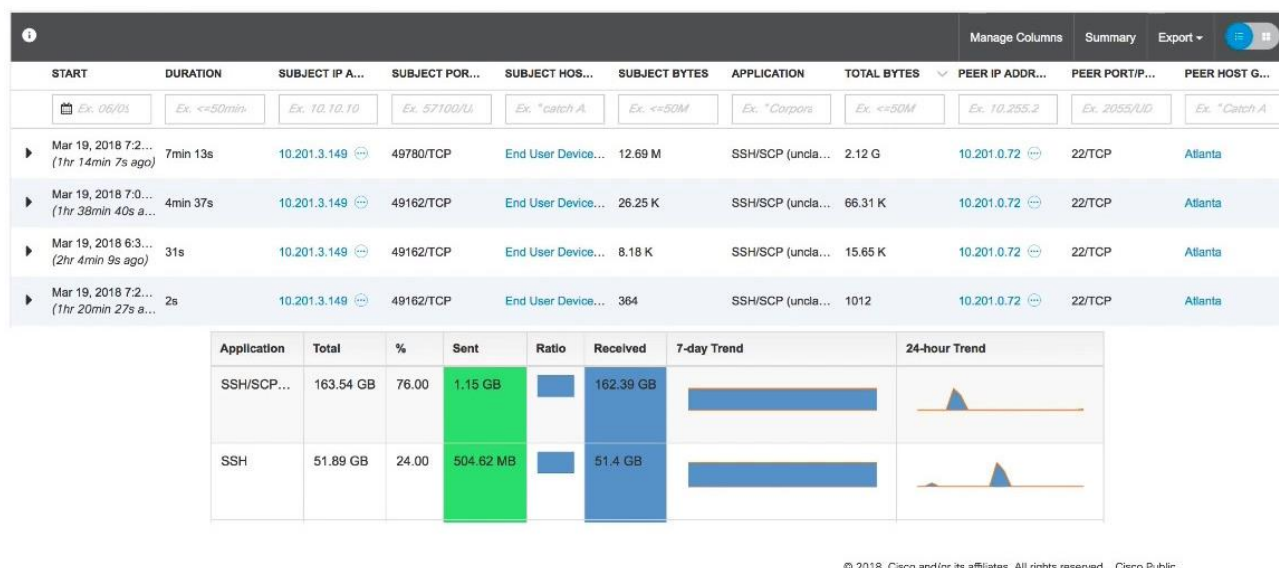


Рис. 1.3. Внутрішній порушник з доступом через *SSH*

Зробивши це, виявлено, що внутрішній порушник використовує протокол *SSH*, щоб захопити дані з внутрішньої корпоративної мережі. Зверніть увагу, при тому, що з вузла зловмисника відправлено всього близько одного гігабайта даних, отримано більше 160 ГБ даних. Цілком можливо, що йдеться про зловмисника, який намагається захопити дані, до яких він встигає «дотягнутися» і завантажити їх собі на комп'ютер.

В даному випадку, видно, що хакер «зливає» дані через *HTTPS* з'єднання кудись на зовнішній вузол. Тобто, можливо, це справді зловмисник, який, як якщо згадати історію зі Сноуденом, на початку скопіював до себе всі дані, до яких зміг дотягнутися, а потім він намагається їх винести за межі компанії.

Ще один приклад, як допоможе *Cisco Stealthwatch*. Наприклад, поширення черв'яка або шкідливого коду всередині корпоративної мережі. Зазвичай, щоб зафіксувати це, необхідно мати агент/агентів на хості. Там може бути антивірус. Це можливо рішення класу і *EDR (endpoint detection and response)*. Це може бути щось інше, що за рахунок аналізу активності на вузлі виявляє дії шкідливого коду. Але що робити, якщо ми не можемо встановлювати агенти на вузлах (наприклад, ці агенти занадто «зжирають» потужності процесора, або збільшують навантаження на нього, або «зжирають» оперативну пам'ять)? Комп'ютер гальмує і тому не хочеться ставити на нього жодних захисних агентів (наприклад, ЦОД). Або це сегмент, на який взагалі не можна поставити якісь захисні агенти. Це може бути промисловий сегмент (АСУ ТП), це може бути сегмент із операційними системами, для яких не розроблено захисних агентів. Причин може бути багато. Іншими словами, за відсутності хостових засобів захисту інженери залишаються сліпі. У них єдине джерело даних для виявлення шкідливої активності – це мережевий трафік і тут знову допомагає *Stealthwatch*, який у даному випадку зафіксував дії шкідливого коду. Видно події сканування вузлів і в деталях цієї події можна побачити, що ця активність властива поширенню черв'яків по мережі (рис. 1.4).

Відбувається візуалізація, де була точка відліку, хто далі потрапив під роздачу і швидко локалізувати проблему, не даючи їй розвиватися по нашій мережі, не даючи зловмисникам розширювати «плацдарм» у нашій корпоративній або відомчій мережі.

На жаль, за статистикою *Cisco*, зловмисники за останній рік втричі збільшують кількість шкідливих програм, які використовують для своєї діяльності, а точніше для її приховування – шифрування. З теорії відомо, що

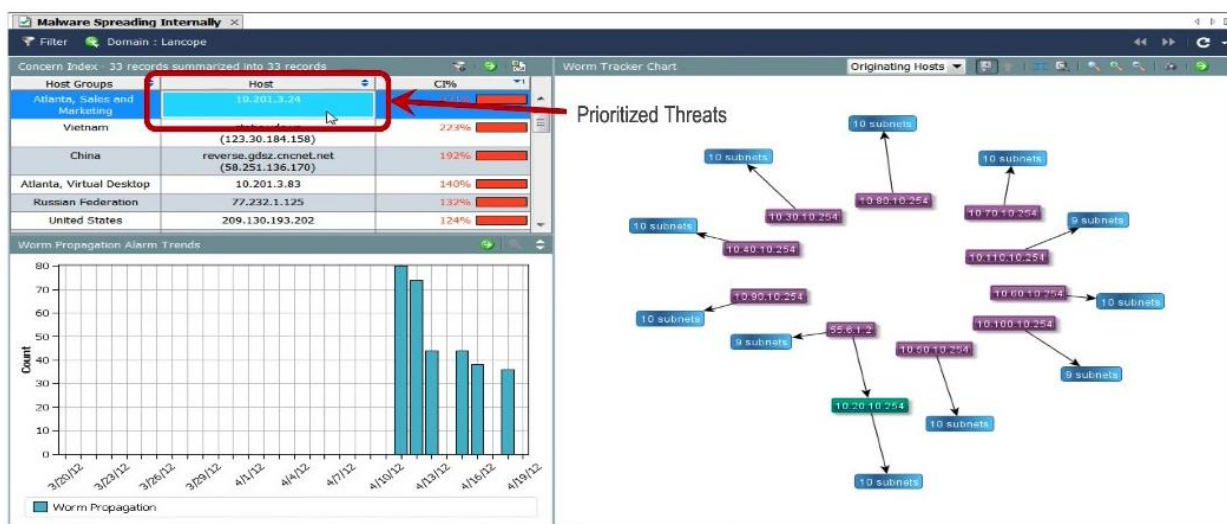


Рис. 1.4. Візуалізація комп'ютерної мережі

«правильний» алгоритм шифрування може бути зламаний. Для того щоб зрозуміти, що ховається всередині зашифрованого трафіку, необхідно або його розшифровувати знаючи ключ, або спробувати дешифрувати його різними хитрощами, або зломом в лоб, або використовуючи якісь уразливості в криптографічних протоколах.

Насправді виявилось, що на практиці існують інші методи аналізу зашифрованого трафіку без його розшифровки. Цей метод називається просто - "машинне навчання". Виявилось, що якщо на вхід спеціального класифікатора подати дуже великий обсяг різного трафіку, які використовуються зловмисниками, і навчити цей класифікатор розпізнавати такого роду шкідливу дію, навіть усередині зашифрованого трафіку, який ми не можемо розшифрувати або дешифрувати, система з дуже високим ступенем ймовірності дії шкідливого коду всередині зашифрованого трафіку

Точність виявлення становить 99,99 %. Хибні спрацьовування – це соті частки відсотка. Тобто, спираючись на аналіз телеметрії, яку компанія Cisco отримує з мережевого обладнання, навіть без якихось криптографічних перетворень, можна сказати, що всередині того чи іншого зашифрованого трафіку ховається шкідлива активність і це дозволяє ефективніше здійснювати моніторинг внутрішньої інфраструктури. Програми-сервіси переходять на

протокол *TLS 1.3*, який не можна спочатку розшифровувати. Тобто він спеціально спроектований для того, щоб не можна було робити навіть легальний *Man In The Middle*. Зроблено це задля забезпечення приватності даних користувачів. Ця приватність користувача, на жаль, грає не на руку, а проти корпоративних служб безпеки, які раніше (до *TLS 1*). 3) ще могли робити розшифрування трафіку на периметрі за допомогою тих чи інших *SCAfferder*-ів, то зараз, на жаль, це зробити вже неможливо. Але технологія, яка закладена в *Cisco Stealthwatch* під назвою *Encrypted Traffic Analytics*, дозволяє без розшифрування трафіку зрозуміти, що знаходиться всередині. Зрозуміло, ніхто не зрозуміє, що там написано. Це неможливо. Криптографія тут працює. Але можна зрозуміти тип цього трафіку і якщо він шкідливий, то ухвалити відповідні рішення. Криптографія тут працює. Але можна зрозуміти тип цього трафіку і якщо він шкідливий, то ухвалити відповідні рішення. Криптографія тут працює. Але можна зрозуміти тип цього трафіку і якщо він шкідливий, то ухвалити відповідні рішення.

1.1.4. Технології *Encrypted Traffic Analytics*.

Видно, що здійснюється витік інформації (напис «*Exfiltration*» – витік даних) з конкретного вузла, за яким працює користувач на ім'я Роланда Торсієлло та помітна позначка «*Encrypted*». Це означає трафік зашифрований. Тобто, незважаючи на наявність шифрування, все одно можна зафіксувати факт витоку інформації, тобто заподіяння шкоди корпоративному ресурсу.

Хочеться відзначити, що рішення *Cisco Stealthwatch* має ряд дуже важливих особливостей. Важливих переваг.

По-перше, це можливість аналізу зашифрованого трафіку, що останнім часом стає дуже важливою функцією засобу забезпечення інформаційної безпеки.

По-друге, це захист зроблених інвестицій у мережну інфраструктуру. *Cisco* не тільки має мережну інфраструктуру, яку передає трафік з точки А в точку Б, *Cisco* перетворює її на розподілену систему виявлення атак.

Ця система не вимагає перебудови мережі. Не треба ставити нові залозки

всередину корпоративної мережі, не треба переконвертувати трафік, міняти його адресацію тощо. З існуючою інфраструктурою йде складання *Flow* і починається аналіз його на предмет тих чи інших аномалій чи загроз.

Незважаючи на те, що рішення *Cisco Stealthwatch* розроблено і пропонується компанією *Cisco*, в основі якої необхідно захистити, може бути не тільки інфраструктура компанії *Cisco*, але і структури різних інших виробників. У цьому випадку *Cisco Vendor Agnostic* (виробник системи захисту). Не важливо, що «лежать» в основі. Це може бути *Cisco*, це може бути *Huawei*, це може бути *Juniper*, *Zcom*, *Hewlett* і так далі. Будь-яку мережну інфраструктуру, яка підтримує або протоколи *Flow*, або *SPAN/RSPAN* можна перетворити на розподілену систему виявлення атак.

У цьому випадку дуже добре підходить рішення *Cisco ISE (Identity Services Engine)*, яка перетворює мережеву інфраструктуру, яку вже перетворилася на розподілену систему виявлення атак, *Cisco ISE* перетворює її на розподілений міжмережевий екран. Це коли кожен комутатор, кожен маршрутизатор, кожна точка доступу використовується як точка прийняття рішення – «пускати чи не пускати?», «пускати користувача?», «пускати пристрій?», «пускати програму?» до запитаного ресурсу. *Cisco ISE* перетворює існуючу інфраструктуру (причому не лише походження *Cisco*, це можна робити на інших вендорах) на розподілений міжмережевий екран. Якщо на периметрі зазвичай використовується *NG Firewall*-и (наприклад, *Cisco FirePower*) і *NGIPS* (наприклад, *Cisco Firepower IPS*), то у внутрішній мережі можна використовувати зв'язку *Cisco Stealthwatch* і *Cisco ISE*.

1.1.5. Методи захисту від *DDoS*

Звичайні файрволи та *IPS* тут не допоможуть, вони безсилі проти комплексної *DDoS*-атаки на *DNS*. Насправді брандмауери та системи запобігання вторгненням самі є вразливими для атак *DDoS*.

На допомогу можуть прийти хмарні послуги очищення трафіку: він прямує в якийсь центр, де перевіряється і перенаправляється назад за призначенням. Ці послуги є корисними для *TCP*-трафіку. Ті, хто самі керують

своєю інфраструктурою *DNS*, можуть для послаблення наслідків *DDoS*-атак вжити таких заходів.

Моніторинг *DNS*-серверів щодо підозрілої діяльності є першим кроком у справі захисту інфраструктури *DNS*. Комерційні рішення *DNS* та продукти з відкритим вихідним кодом, такі як *BIND*, надають статистику в реальному часі, яку можна використовувати для виявлення атак *DDoS*. Моніторинг *DDoS*-атак може бути ресурсомістким завданням. Найкраще створити базовий профіль інфраструктури за нормальних умов функціонування і потім оновлювати його час від часу в міру розвитку інфраструктури та зміни шаблонів трафіку.

Додаткові ресурси *DNS*-сервера допоможуть впоратися із дрібномасштабними атаками за рахунок надмірності інфраструктури *DNS*. Ресурсів сервера та мережевих ресурсів має вистачати не обробку більшого обсягу запитів. Звичайно, надмірність коштує грошей. Ви платите за серверні та мережеві ресурси, які зазвичай не використовуються в нормальних умовах. І за значного «запасу» потужності цей підхід навряд чи буде ефективним.

Увімкнення *DNS Response Rate Limiting (RRL)* знизить ймовірність того, що сервер буде задіяний в атаці *DDoS Reflection* – зменшиться швидкість реакції на повторні запити. *RRL* підтримує багато реалізації *DNS*.

Використовуйте конфігурацію високої доступності. Можна захиститись від *DDoS*-атак шляхом розгортання *DNS* на сервері високої доступності (*HA*). Якщо в результаті атаки впаде один фізичний сервер, *DNS*-служба може бути відновлена на резервному сервері. Найкращим способом захисту *DNS* від *DDoS*-атак буде використання географічно розподіленої мережі *Anycast*. Розподілені мережі *DNS* можуть бути реалізовані за допомогою двох різних підходів: адресації *Unicast* або *Anycast*. Перший підхід набагато простіше реалізувати, але другий набагато стійкіший до *DDoS*-атак.

У разі *Unicast* кожен із серверів *DNS* вашої компанії отримує унікальну *IP*-адресу. *DNS* підтримує таблицю *DNS*-серверів вашого домену та відповідних *IP*-адрес. Коли користувач вводить *URL*-адресу, для виконання запиту вибирається одна з *IP*-адрес у випадковому порядку.

При схемі адресації *Anycast* різні сервери *DNS* використовують спільну *IP*-адресу. Коли ви вводите *URL*-адресу, повертається колективна адреса серверів *DNS*. *IP*-мережа маршрутизує запит на найближчий сервер.

Anycast надає фундаментальні переваги перед *Unicast* щодо безпеки. *Unicast* надає *IP*-адреси окремих серверів, тому нападники можуть ініціювати цілеспрямовані атаки на певні фізичні сервери та віртуальні машини, і коли вичерпані ресурси цієї системи, відбувається відмова служби. *Anycast* може допомогти пом'якшити *DDoS*-атаки шляхом розподілу запитів між групою серверів. *Anycast* також корисно використовувати для ізоляції наслідків атаки.

Проектування, розгортання та експлуатації глобальної *Anycast*-мережі потребує часу, грошей та ноу-хау. Більшість ІТ-організацій не мають у своєму розпорядженні для цього фахівцями та фінансами. Можна довірити функціонування інфраструктури *DNS* провайдеру – постачальнику керованих послуг, який спеціалізується на *DNS*. Вони мають необхідні знання для захисту *DNS* від *DDoS*-атак.

Постачальники послуг *Managed DNS* експлуатують великомасштабні *Anycast*-мережі та мають точки присутності по всьому світу. Експерти з безпеки мережі здійснюють моніторинг мережі в режимі 24/7/365 та застосовують спеціальні засоби для пом'якшення наслідків *DDoS*-атак.

Послуги захисту від *DDoS*-атак пропонують і деякі постачальники послуг хостингу: аналіз мережного трафіку проводиться в режимі 24/7, тому ваш сайт буде відносною безпекою. Такий захист здатний витримати потужні атаки – до 1500 Гбіт/сек. Оплачується у своїй трафік.

Ще один варіант – захист *IP*-адрес. Провайдер поміщає *IP*-адресу, яку клієнт вибрав як захист, в спеціальну мережу-аналізатор. При атаці трафік до клієнта зіставляється із відомими шаблонами атак. В результаті клієнт отримує лише чистий, відфільтрований трафік. Таким чином, користувачі сайту можуть і не дізнатися, що на нього була зроблена атака. Для організації такого створюється розподілена мережа фільтруючих вузлів так, щоб для кожної атаки можна було обрати найближчий вузол і мінімізувати затримку передачі

трафіку.

Результатом використання сервісів захисту від *DDoS*-атак буде своєчасне виявлення та запобігання *DDoS*-атак, безперервність функціонування сайту та його постійна доступність для користувачів, мінімізація фінансових та репутаційних втрат від простоїв сайту чи порталу.

Концепція розподіленої атаки на відмову в обслуговуванні до примітивного проста: цільовий хост бомбардують безліччю запитів із різних *IP*-адрес. Вимушений обробляти ці запити, хост виходить з ладу, у результаті сервіси, які він надавав, стають недоступними для звичайних користувачів. За припинення атаки зазвичай вимагають викуп.

Основні типи *DDoS*-атак - *Layer 3* і *Layer 7*. Вони названі так відповідно до рівня мережевої моделі *OSI*, на яких виконуються.

Layer 3 DDoS націлений на мережеве обладнання та з'єднання. У ході атаки створюється величезний паразитний трафік, наприклад за допомогою *SYN*-пакетів (*syn-flood*). Цей трафік забиває канал зв'язку та блокує проходження легітимних пакетів. В даний час більшість великих хостинг-провайдерів і дата-центрів сьогодні добре захищені від атак *Layer 3*, тому в цьому пості ми зосередимося на іншому різновиді атак, протистояти якому трохи складніше.

DDoS-атаки *Layer 7* націлені безпосередньо на програми, що працюють на сервері. Мета тут - не відключити мережу, а домогтися зупинки програми або навіть сервера шляхом навантаження його штатними прикладними запитами. Це призводить до нестачі ресурсів процесора, оперативної пам'яті або того й іншого і фактично зупиняє роботу.

Існує безліч способів та інструментів для проведення такого роду атак та безліч способів захисту. Сьогодні ми зосередимося на захисті від розподілених атак на відмову в обслуговуванні на рівні додатків (рівень 7), скорочено *L7 DDoS*.

Стандартною практикою для таких атак є надсилання безлічі запитів з різних публічних *IP*-адрес. Наприклад, для атаки на інтернет-магазин це

можуть бути *http/https*-запити, що викликають інтенсивну роботу з базою даних - реєстрація нового користувача або пошук товарів.

Складність захисту від таких атак полягає в тому, щоб відрізнити запит звичайного користувача від шкідливого запиту. Якщо в розпорядженні атакуючого є достатній пул *IP*-адрес, він може надсилати з кожного з них буквально два-три запити, після чого переходити до наступного. Це забезпечує перевантаження цільового хоста, але унеможлиблює блокування атаки по *IP*-адресі.

Зупинити такі атаки дозволяє блокування *IP*-адреси геолокації або автономної системи (*AS*). Якщо атаки в основному йдуть із країн *X* та *Y* або автономних систем *M* та *N*, їх блокування дозволить частково вирішити проблему. Але заборона означатиме, що легітимні користувачі цих країн та автономних систем не зможуть отримати доступ до сайту. Такий підхід є неприйнятним, якщо йдеться про захист інтернет-магазину або провайдера послуг, який доставляє товари та надає послуги по всьому світу.

Під час атаки *Layer 7* для країн, звідки в основному йде атака, показуватиметься капча (Китай, Індонезія та Індія у нашому прикладі), але легітимні користувачі звідти все одно потраплять на сайт, тоді як користувачі з інших країн (тут - Франція та Іспанія) проходитимуть без перевірок.

Для досягнення цієї мети агент *CrowdSec* читатиме журнали *Apache*, виявлятиме джерела атаки і видаватиме рішення, які використовуватиме баунсер *Cloudflare*, щоб відправити *Cloudflare* команду блокування атакуючих.

Для коректної роботи *Apache* повинен бути налаштований на роботу з заголовком *HTTP X-forwarded-for*, щоб відображати реальні *IP* атакуючих, а не адреси *Cloudflare*.

Після виявлення джерел атак ми можемо використовувати функції *Cloudflare* для вибіркової зупинки атак: баунсер буде створювати і оновлювати правила брандмауера в *Cloudflare* через його *API*. Ми не хочемо забороняти доступ легальним користувачам із заблокованих країн, тому можемо встановити правила, які змушуватимуть користувачів проходити лише капчу.

Rule name
Give your rule a descriptive name

CrowdSec challenge rule

When incoming requests match...

Field	Operator	Value	
Country	is in	Brazil × China × Indonesia × India × Russian Federation × United States ×	And ×
Or			
AS Num	is in	37963 ×	And ×
Or			
IP Source Address	is in list	crowdsec_challenge 55 records	And Or ×

[Manage lists](#)

Expression Preview [Edit expression](#)

```
(ip.geoip.country in {"BR" "CN" "ID" "IN" "RU" "US"}) or (ip.geoip.asnum in {37963}) or (ip.src in $crowdsec_challenge)
```

Рис. 1.5. Використання *Cloudflare* для протидії атакам

Правило, згенероване баунсером, включає капчу для різних країн, *IP* та *AS*, ефективно блокуючи ботів.

Висновки за розділом

В даному розділі було проведено аналіз прикладів несанкціонованого доступу до комп'ютерних мереж для викрадення інформації, супутні методи атак на мережі (на прикладі *DDoS* атак) та методи протидії даним діям зловмисників.

РОЗДІЛ 2

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ МЕРЕЖІ

2.1. Проблеми реактивного захисту в системах промислової автоматизації

Щоб обговорити проблеми, які існують для інтеграції реактивного захисту в *IAS*, важливо спочатку окреслити поточні архітектурні тенденції та тенденції безпеки. Для цього довідкова архітектура *IAS* (Рис. 2.1) походить від [15,16]. Ця архітектура складається з п'яти рівнів (від 0 до 4), що відповідають рівням добре відомої ієрархії піраміди автоматизації (як визначено стандартом *ISA-95* [17]).

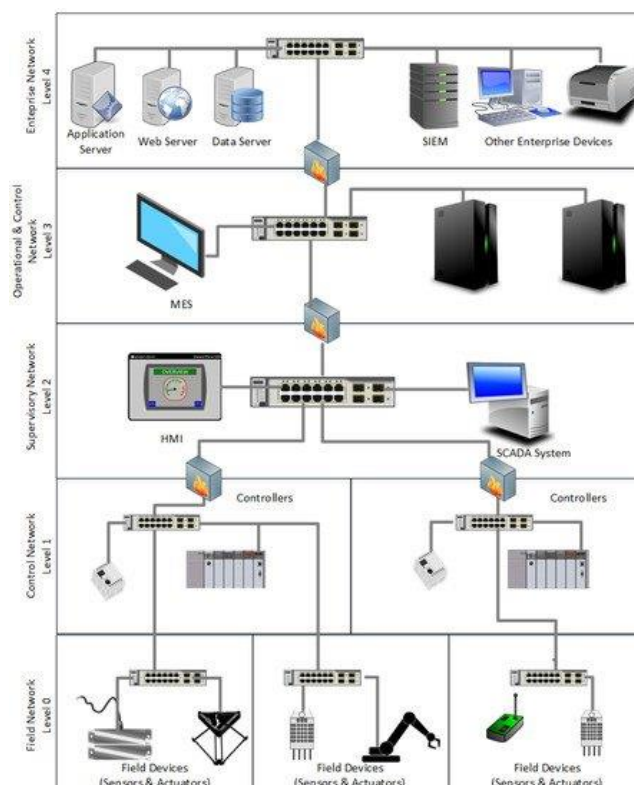


Рис. 2.1. Приклад архітектури системи промислової автоматизації

Рівень 0 (тобто рівень поля) складається з датчиків і виконавчих механізмів, які становлять фізичний процес. Пристрої, які контролюють і керують локальними фізичними процесами (наприклад, програмовані логічні контролери та віддалені термінальні блоки), утворюють рівень 1 (тобто рівень керування). Моніторинг та інші види управлінської діяльності (тобто, тривога та обробка попереджень) здійснюються операторами на рівні 2 (тобто, на рівні нагляду) за підтримки наглядових технологій, таких як системи контролю та збору даних (системи *SCADA*), історики та інтерфейси людини-машини (*HMI*). Рівень 3 (тобто рівень операцій) керує виробничими робочими потоками. На цьому рівні популярні системи виробництва та виконання (*MES*). Нарешті, рівень 4 (тобто

Крім того, кожен з цих рівнів також може бути розділений на підмережі та розподілений у різних географічних місцях. Такий розподіл і велика кількість компонентів, які становлять *IAS*, створюють проблеми для їх управління та безпеки. Для цього в *IAS* було інтегровано кілька рішень, які інтегрують централізоване управління та можливості безпеки. Два з найпопулярніших рішень – це технології управління інцидентами та подіями безпеки (*SIEM*) і системи управління операційними технологіями (*OT*).

Технології *SIEM* широко використовуються в ІТ-сфері [18]. Вони дозволяють відстежувати компоненти системи та керувати подіями та попередженнями безпеки за допомогою агрегації, аналізу та звітування інформації про безпеку. Деякі з цих технологій *SIEM* включають можливості, які полегшують роботу та керування системою промислового контролю, що зробило їх придатними для *IAS* [15]. Системи управління *OT* забезпечують подібні можливості до технологій *SIEM*, однак вони більше зосереджені на специфічних для *IAS* операціях, таких як моніторинг мережі управління та управління ризиками (наприклад, *Industrial Defender Automation Systems Manager (ASM)*).19)).

І технології *SIEM*, і системи управління *OT* централізують компоненти аналізу та візуалізації. Технології *SIEM* часто розгортаються на рівні 4 (тобто на

інформаційному рівні), тоді як системи управління *OT* часто розгортаються на рівнях 2 і 3 (тобто рівень нагляду та рівень операцій). Для того, щоб ці технології забезпечували захист нижчих рівнів ієрархії автоматизації, необхідно, щоб вони забезпечували можливості, які дозволяли б їм контролювати мережу та компоненти, розташовані на цих нижчих рівнях, або щоб вони могли отримувати інформацію від інших рішень безпеки, розташованих на ці рівні мережі. Деякі з рішень безпеки, які можуть надати цю інформацію, - це бази даних, антивіруси, системи виявлення вторгнень (*IDS*) (як для корпоративних, так і промислових мереж) і системи запобігання вторгненням (*IPS*) [15].

На жаль, хоча консолідація цих централізованих технологій управління безпекою (тобто технологій *SIEM* та систем управління *OT*) та їх додаткових рішень безпеки дозволяє ефективно виявляти та повідомляти про вторгнення в систему; обсяг підтримуваних ними запобіжних можливостей (тобто дії, здатні блокувати, порушувати, модифікувати, затримувати та/або зупиняти вторгнення) може не охоплювати нижчі рівні ієрархії автоматизації (тобто рівні 0–2). Це відбувається, оскільки ці можливості запобігання часто надаються рішеннями безпеки, чия область активного реагування не враховує специфічні характеристики *IAS*. Крім того, існують занепокоєння, пов'язані з інтеграцією активних відповідей в *IAS* через страх, що вони потенційно вплинуть на правильну роботу *IAS* [12,13,14], впливаючи на його доступність, продуктивність або перериваючи зв'язок з компонентами, розташованими на вищих рівнях системної ієрархії (наприклад, технології *SIEM*, системи управління *OT*, системи *SCADA* тощо). Отже, сучасні тенденції промислової архітектури та безпеки створюють виклик для інтеграції реактивного захисту в *IAS*.

2.2. Вимоги до реактивного захисту в системах промислової автоматизації

Метою представленої концепції є отримання можливого рішення, здатного активно захищати *IAS* від вторгнень. Отже, необхідно визначити та узгодити вимоги, властиві рішенням реактивного захисту, та інші вимоги промислової сфери (тобто архітектурні та експлуатаційні вимоги).

Втручання людини під час реагування на вторгнення часто дає певні недоліки, які призводять до збільшення витрат і більшої вразливості системи. Вищі витрати пов'язані з людськими зусиллями, необхідними для аналізу вторгнення, щоб вибрати та виконати відповідну дію. Підвищена вразливість виникає через проміжок часу між виявленням вторгнення та виконанням його відповіді. Протягом цього часу вторгнення продовжується, і воно навіть може бути успішно завершено. Отже, необхідно зменшити кількість людського втручання, необхідного за рахунок автоматизації деяких завдань, які зазвичай виконуються нею. в [7,22], підкреслюється, що *IPS* і системи реагування на вторгнення (*IRS*) можуть вимагати настроювання людини, щоб вирішити, які запобіжні дії увімкнути/вимкнути для якого типу оповіщення. Ця настройка гарантує, що небажані реактивні дії, які можуть поставити під загрозу поведінку базової системи, не будуть виконуватися. Таким чином, забезпечується вища впевненість, що дозволяє (напів) автоматизувати завдання аналізу та виконання – таким чином дозволяючи відповідні реакції (майже) у реальному часі на вторгнення.

Серія стандартів *ISA/IEC 62443* [23] вважаються майбутніми де-факто еталонними стандартами безпеки в *IAS* [24]. Однією з інтегральних концепцій цієї серії є сегментація мережі *IAS* на різні зони безпеки. Це дозволяє групувати компоненти в набори, які мають подібні вимоги безпеки. Таким чином, дозволяючи керувати політикою та механізмами безпеки від зони до зони. Це дозволяє захистити зони від несанкціонованого доступу, зводячи до мінімуму можливі ризики безпеці, враховуючи принципи найменших привілеїв і внесення в білий список. Ці принципи часто досягаються шляхом контролю та обмеження зв'язку між зонами, щоб дозволити лише зв'язок, необхідний для роботи *IAS*.

Під час роботи *IAS* має відповідати трьом важливим експлуатаційним вимогам [25,26]: можливості реального часу, висока доступність і висока продуктивність. Недотримання цих вимог може негативно вплинути на надійність і безпеку таких систем. Тому важливо, щоб будь-які додаткові компоненти, не пов'язані з самим автоматизованим процесом, не впливали негативно на ці вимоги. Це може бути виконано шляхом визначення критичних компонентів, які необхідно враховувати, а також обмежень або умов, які забезпечують їх нормальну або очікувану роботу.

Завдяки досягненням четвертої промислової революції на ринку промислових рішень існує широкий спектр системних платформ і пристроїв [27]. Це вимагає, щоб нові рішення могли бути розгорнуті в таких компонентах, щоб довести їх конкурентоспроможність. Крім того, важливо, щоб вони могли взаємодіяти з іншими компонентами від різних постачальників [28]. Це дає змогу повністю використати їхній потенціал, доповнюючи певні функції (наприклад, активні реакції) з тими, що існували раніше, щоб покращити їхні можливості. І сумісність, і незалежність від платформи гарантують, що системні інтегратори можуть вибрати продукти, які найкраще відповідають їхнім потребам, не турбуючись про залежність від виробника, що забезпечує більшу гнучкість на етапі проектування *IAS*.

2.3. Захист кінцевих точок від складних кібератак

Для протидії комплексним загрозам *Solar JSOC* пропонує спеціалізований захист кінцевих точок на базі рішення класу *Endpoint Detection and Response (EDR)* Лабораторії Касперського. Сервіс контролю кінцевих точок та серверів дозволяє на ранній стадії виявляти складні атаки та оперативно реагувати на них. Він підключається як доповнення до базової послуги *Solar JSOC* з моніторингу та реагування на інциденти інформаційної безпеки.

Завдяки контролю за пристроями співробітників, які зловмисники часто обирають як вихідну точку для проникнення в мережу компанії, атаки можна

виявити швидше та локалізувати ще до того, як зараження набуде серйозного масштабу. Це, у свою чергу, знижує вартість інцидентів безпеки компанії. Компонент *EDR* сигналізує у тому числі і про підозрілі активності на пристроях, не охоплених сервісом з моніторингу та реагування на інциденти ІБ, що розширює можливості захисту та локалізації загроз.

Автоматичний збір слідів присутності сторонніх в інфраструктурі спрощує та прискорює як реагування на інциденти, так і їхнє подальше розслідування. Компонент *EDR* збагачує інформацію про інциденти, зафіксовані іншими СЗІ, та надає дані щодо підозрілої активності, що не потрапила в їхнє поле зору.

Сервіс підходить організаціям, які вже підписані на послуги *Solar JSOC* з моніторингу та реагування на інциденти ІБ, якщо вони зацікавлені в ефективному захисті кінцевих пристроїв від складних атак та прагнуть локалізувати поширення загрози у найкоротший термін.

Діяльність зловмисників не зупиняється о 18.00. За даними *Solar JSOC*, 2020 року 47,2% критичних зовнішніх інцидентів відбувається вночі. З кожною хвилиною бездіяльності розмір шкоди зростає, а нейтралізація загрози стає набагато складнішим і трудомістким процесом. В рамках сервісу моніторинг кінцевих точок ведеться цілодобово і без вихідних 6 філій *Solar JSOC* у різних часових поясах - так що атака буде зупинена вчасно.

Базові засоби безпеки, такі як антивірус і брандмауер, захищають від простих загроз, але цілеспрямовані атаки, підготовлені просунутими зловмисниками можуть обдурити їх. Контроль кінцевих точок і серверів на базі *EDR* зміцнює захист від складних загроз за рахунок виявлення загроз не лише за сигнатурами, а й за *IoC*.

Навіть найкращі захисні рішення іноді видають неправдиву тривогу. Щоб не турбувати вас, сповіщення про інциденти перевіряються ще раз вручну, і помилкові спрацьовування відсіваються.

Зловмисники постійно вдосконалюють свій арсенал, прагнучи обійти засоби захисту. Щоб не пропустити нові атаки, необхідно регулярно розробляти

актуальні сценарії виявлення атак і вдосконалювати наявні. Експерти *Solar JSOC* розробляють та вдосконалюють правила детектування інцидентів, проводять ретроспективний аналіз подій та виявлених інцидентів для оцінки загального рівня захищеності клієнта, аналізують інформацію про нові загрози, що отримується із зовнішніх джерел та бази знань *Solar JSOC CERT*.

Клієнти сервісу можуть самостійно вирішити, яку частину дій з реагування довірити автоматичі, а що виконати силами своїх фахівців за результатами отримання рекомендацій і чи потрібно залучити до вирішення завдання експертів *Solar JSOC* (у разі потреби провести глибоке технічне розслідування інциденту). Список доступних автоматичних дій обмежений, і їхній набір завжди узгоджується із замовником.

Переваги:

- створення єдиного вікна для роботи служби ІБ у компанії;
- Скорочення часу реагування на кібератаки та мінімізація їх наслідків;
- Наскрізний контроль за життєвим циклом інциденту;
- Формування загальної звітності та візуалізація даних;
- Застосування досвіду найбільшого комерційного SOC в Україні у протидії передовим кіберзагрозам;
- Повний цикл експертизи в управлінні інцидентами;
- Просте та централізоване управління розширеним захистом хостів без необхідності самостійної експлуатації спеціалізованих рішень або підтримки *open-source*;
- Наявність необхідних ліцензій та сертифікатів;
- Власна дослідницька лабораторія та база знань *Solar JSOC CERT*, що щодня актуалізується, про нові атаки;
- Цілодобовий моніторинг завдяки 6 філіям у різних часових поясах; для вирішення складних питань у будь-який час доступний бізнес-аналітик.

2.4. Методи протидії несанкціонованому доступу шляхом використання

EDR та XDR

EDR автоматично збирає первинну інформацію про події ІБ на робочих місцях та надає докладну телеметрію. Експерти *Solar JSOC* аналізують отримувану інформацію, зіставляють її з даними *Threat Intelligence* з різних джерел і, якщо потрібно, вживають заходів реагування та проводять розслідування. Звіти про інциденти та дані розслідування регулярно передаються клієнту. У разі потреби у рамках сервісу можна підключити систему захисту від цілеспрямованих атак *Kaspersky Anti Targeted Attack Platform*, яка дозволяє виявити складні загрози на мережевому рівні.

Зловмисники найчастіше розпочинають атаку на бізнес із зараження пристроїв співробітників. Тому дуже важливо виявляти та блокувати шкідливу активність саме на таких пристроях. Проте базові засоби захисту робочих місць – спам-фільтри, антивіруси та брандмауери – можуть виявити лише прості атаки. У разі складної цілеспрямованої атаки висока ймовірність, що вони не спрацюють.

Навіть кіберзлочинці середньої кваліфікації нерідко використовують складні шкідливі програми та вдаються до особливих прийомів, таких як багатоступінчаста обфускація або використання ланцюжка викликів легальних утиліт, які дозволяють обдурити та обійти базові засоби захисту. Атаки кіберзлочинців високої кваліфікації найчастіше базовим СЗІ не до зубів.

Саме тому для повноцінного захисту потрібні додаткові інструменти. Серед них найважливіші – системи виявлення та локалізації атак на кінцеві пристрої (*EDR*).

За даними *Solar JSOC* у зв'язі за 2021 рік:

- 49,2% інцидентів не виявляються за допомогою базових СЗІ;
- 75% атак професійні зловмисники реалізували за допомогою фішингу
- 15% користувачів здійснюють потенційно небезпечні дії при отриманні фішингових листів;
- 16% компаній здатні ефективно чинити опір кібератакам.

Ядерна тріада – це термін, який означає стратегічні збройні сили держави, оснащені ядерним озброєнням. У тріаду входять три компоненти: повітряний – стратегічна авіація, сухопутний – міжконтинентальні балістичні ракети, морський – атомні підводні ракетоносці.

Свого часу Мартін Гартнер [12] провів аналогію стратегічних збройних сил держави з центром моніторингу та оперативного реагування на інциденти (SOC), виділяючи такі елементи тріади SOC: *Security information and event management (SIEM)*, *Network Traffic Analysis (NTA)*, *Endpoint Detection and Response (EDR)*. Дивлячись на цю аналогію стає очевидним, що SOC може бути максимально ефективним лише в тому випадку, якщо буде оснащений усіма компонентами захисту: у «повітрях», на «землі» та в «морі».

На жаль, сьогодні більшість організацій використовують лише "стратегічну авіацію" - *SIEM* системи. Досить рідко «міжконтинентальні балістичні ракети» – *NTA*, замінюючи повноцінний аналіз мережного трафіку лише збиранням логів зі стандартних засобів захисту. І зовсім не часто «атомні підводні ракетоносці» – *EDR*.

У світі інформаційної безпеки, технологія *EDR* - це вже набагато більше, ніж просто передовий захист робочих станцій та серверів від складних загроз. З року в рік робочі місця залишаються ключовою метою зловмисників та найпоширенішими точками входу в інфраструктуру організацій, що потребує належної уваги та відповідного захисту. А телеметрія є цінною інформацією, необхідною для якісного розслідування інцидентів, значимість доступу до якої зростає ще більшою мірою з появою нового протоколу шифрування *TLS 1.3* та його активного поширення.

XDR – це, переважно, концепція, що є крос-продуктову історію, збагачену поверх додатковими значущими функціональними можливостями з реагування на інциденти. Це єдиний центр збору, нормалізації, аналізу, кореляції даних, розширеного розслідування та реагування із застосуванням максимально можливої автоматизації. У складі також єдина база даних, єдина консоль, єдина видимість того, що відбувається в інфраструктурі, єдиний інструментарій з

аналізу першопричин та проактивного пошуку загроз, єдиний покращений процес пріоритезації інцидентів, одна точка взаємодії з *Threat Intelligence* та ін.

XDR передбачає постійну доставку оновлень, нових правил, плейбуків і т.д. Це не просто коробка, що відвантажується - це живий і зростаючий організм, що актуалізується з кожною зміною в ландшафті загроз.

Концепцію і саму назву *XDR* придумали цього разу не аналітики, його нав'язав ринок та вендори. *XDR* – насамперед це логічна консолідація портфеля рішень від одного виробника, який з роками ріс (розроблявся та/або доповнювався придбаннями) та елементами якого було б правильно, по-перше, управляти з єдиної точки та мати єдине середовище обміну даними, а, по-друге, було б непогано посилити крос-продуктові сценарії. Для покупця це виглядає як отримання додаткового і важливого функціоналу при покупці декількох захисних рішень від одного постачальника, а для виробника - простіші варіанти додаткових продажів рішень зі свого портфеля.

Захисні засоби, такі як *EPP+EDR*, шлюзи (поштовий та веб), *NTA/NTDR*, *CASB*, *IDM* та ряд інших (залежить від конкретного вендора), а також рішення щодо захисту індустріально-специфічних систем (банкомати, АСУ ТП, *IoT*, пр.) виступають сенсорами для *XDR* і, зокрема, елементами, якими можливо проводити дії з реагування.

Мінімальний комплект *XDR* – це охоплення кінцевих точок та мережі, поштового та веб трафіку, тобто найбільш популярні та важливі точки проникнення зловмисників, які слід контролювати в першу чергу. І, звичайно, цей комплект має бути збагачений актуальними даними про загрози *Threat Intelligence*.

Незважаючи на закладену спочатку моновендорну історію, *XDR* не виключає взаємодію з сторонніми постачальниками, обробки даних від них і, зокрема, включення базових *SOAR* можливостей, переважно пов'язаних з реагуванням. Вендори, які мають у своєму портфелі *SIEM* отримувати додатковий бонус для швидкого підключення сторонніх рішень у загальну концепцію *XDR*.

XDR – це насамперед хмарна історія, але *XDR on-premise* можливий як одна з опцій. Це актуально для України, але не всі вендори на ринку це зможуть забезпечити. Якщо вендор історично був і є з *on-premise* рішеннями - він підтримає історію з *on-premise XDR*, при цьому, що логічно, у тому числі й у хмару.

XDR концепція може лежати в основі сервісів з боку *MSSP* провайдерів, що надається сервісу *MDR*, наприклад.

XDR і *MDR* - це про відмінне доповнення один одного, в першу чергу, для великих організацій зі своєю побудованою системою ІБ. Ми знаємо, що для невеликих організацій без ІБ-штату сервіс *MDR* - це можливість швидко підвищити свій рівень захисту за рахунок цілодобового сервісу. Для великих це все ж таки більше для вивільнення внутрішніх ресурсів під найважливіші завдання, про складний якісний *Threat Hunting* (проактивний пошук загроз) і про рекомендації, зокрема, щодо реагування.

Великі компанії рідко віддають на аутсорсинг питання, пов'язане з реагуванням сторонніми командами у їхній інфраструктурі. Ось якраз для таких організацій надання *MDR* сервісу поверх збудованого *XDR* буде ідеальним і справді мега ефективним.

В даний час для протистояння більш складним загрозам, цілеспрямованим атакам та загрозам типу *APT* організаціям необхідно приділяти особливу увагу не тільки рівню кінцевих точок, але й іншим потенційним точкам проникнення зловмисника в інфраструктуру та, найголовніше, на взаємозв'язку між ними.

Організації повинні мати розуміння того, що відбувається у них у рамках всієї інфраструктури, контролювати ключові точки проникнення і отримувати повну картину атаки, мати можливість швидко аналізувати першопричини,

Сьогоднішня ситуація з великою кількістю розрізнених не інтегрованих рішень, відсутністю достатньої кількості ресурсів та знань для роботи з цим зоопарком рішень та неможливістю отримати оперативно з усього повну картину того, що відбувається. А також недолік автоматизації, необхідної в

процесі виявлення, розслідування та реагування, відсутність крос-продуктових сценаріїв, наявність величезної кількості помилково-позитивних спрацьовувань, низький рівень пріоритезації, не найкращі показники *MTTD/MTTR* – весь цей набір проблем вимагає пошуку якогось рішення.

Завдяки *XDR* різні продукти від одного вендора знаходять єдине середовище обміну даними та отримання єдиної картини, що відбувається в інфраструктурі. Єдина консоль управління для зручності роботи аналітика, що надається високий рівень автоматизації дій у рамках розслідування та реагування, удосконалений процес пріоритезації інцидентів, покращені показники *MTTD* і *MTTR*, скорочення числа хибно-позитивних спрацьовувань та часу, яке аналітики витрачають на процес розслідування та реагування на ін. Сьогодні *XDR* є дуже привабливим.

Висновки за розділом

У другому розділі було проаналізовано технології реактивного захисту *EDR* та *XDR*.

XDR повинен будуватися на сильному *EDR*, який сам по собі в рамках кінцевих точок повинен охоплювати велику кількість джерел даних: ПК, ноутбуки, віртуальні машини, мобільні пристрої плюс різні операційні системи (*Windows, Linux, MacOS, Android, iOS*, ін.).

XDR не те ж саме, що *EDR*. *XDR* базується на розширенні технології *EDR*. Літера “X” на початку скороченого варіанта назви “*XDR*” означає кількість джерел/продуктів, що підключаються, які беруть участь у процесі виявлення, розслідування та реагування. Кількість «X», що підключаються, залежить від потреб замовника, від вже впроваджених рішень від одного вендора, а також від обраного постачальника *XDR*, тобто від його підтримуваних джерел (класів продуктів).

РОЗДІЛ 3

РЕАЛІЗАЦІЯ РЕАКТИВНОЇ СИСТЕМИ ПРОТИДІЇ НЕСАННКЦІОНОВАНОМУ ДОСТУПУ

3.1. Концепція реактивного захисту для систем промислової автоматизації

У вигляді практичної реалізації та дипломного дослідження представлена концепція реактивного захисту для *IAS*, з якої походить система реактивного захисту. Ця концепція відповідає вимогам, які розглядалися в Розділі 2. Особлива увага приділяється його придатності для загальних архітектур *IAS* (Рис. 3.1) та розгляд концепцій, представлених у серії стандартів *ISA/IEC 62443*. По-перше, представлено сферу захисту, що забезпечується Системою реактивного захисту. Це включає попередні вимоги та очікувані можливості захисту. Далі представлені компоненти, які становлять систему реактивного захисту. Нарешті, глибше обговорюється політика безпеки та експлуатації, а також реактивні дії, які можна розглядати в представленій концепції з урахуванням відомих архітектурних та експлуатаційних тенденцій реальних систем автоматизації.

3.1.1. Попередні вимоги та обмеження системи реактивного захисту

Представлена система здатна виконувати активні відповіді. Ці відповіді в цій роботі називаються реактивними діями, оскільки вони відбуваються як активні відповіді на конкретні події безпеки (тобто вторгнення). Для цього необхідно надати інформацію про ці події до системи реактивного захисту. Цю інформацію можуть надавати сторонні компоненти, які відстежують та аналізують системну інформацію для виявлення вторгнень, таких як *IDS* мережі або хосту [25, 26], технології *SIEM* [18] та інші системи кореляції подій.

З цієї причини представлена система не визначена як *IPS*, оскільки в неї відсутня можливість захоплення та аналізу інформації для виявлення вторгнень та генерування подій, пов'язаних із безпекою.

Отже, можливості представленої Системи реактивного захисту обмежуються аналізом подій, пов'язаних із безпекою, ідентифікованих або виявлених сторонніми компонентами. На основі цього аналізу система вирішує, чи можлива відповідна реактивна дія. За умови, що ця дія можлива (тобто підтримується системою і не впливає на роботу базової системи автоматизації), система її виконує. Це може призвести до того, що реактивна дія буде повністю виконана самою системою реактивного захисту, або система реактивного захисту надасть необхідну інформацію іншому компоненту, здатному її виконати, що може призвести до запобігання вторгненню.

3.1.2. Компоненти системи реактивного захисту

Представлена система реактивного захисту складається з чотирьох різних компонентів, як зазначено в Рис. 3.1: модуль конфігурації, база знань про політику та дії, модуль активного реагування та модуль зв'язку. Ця архітектура була розроблена з урахуванням вимог до реактивного захисту в *IAS*.

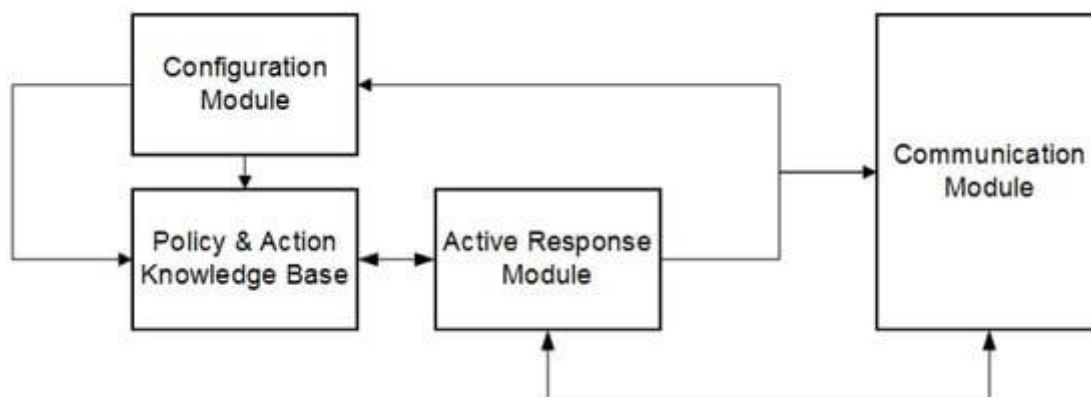


Рис. 3.1. Компоненти системи реактивного захисту

Цю систему можна розгорнути в кожному сегменті мережі, розташованому на рівнях 0–2 ієрархії автоматизації (див. розділ 2, Рис. 2.1) для того, щоб керувати своєю політикою (тобто політикою безпеки та операційної політики) та забезпечити безпеку за допомогою реактивного захисту за

наявності вторгнень.

Комунікаційний модуль забезпечує комунікаційні можливості представленої системи. Він отримує події безпеки від сторонніх компонентів. Ці події пересилаються в модуль активного реагування для аналізу. За умови, що цей аналіз призводить до виконання дії, яка вимагає надання інформації стороннім компонентам, щоб порушити або протидіяти вторгненню, цей модуль також надає інформацію, необхідну для таких компонентів. Прикладом цього є наступне. Модуль активного реагування отримує інформацію про здійснення атаки «Відмова в обслуговуванні» (DoS). Після аналізу цієї інформації було вибрано додавання нового правила до брандмауера, розташованого на іншому пристрої. Отже, модуль активної відповіді надає інформацію, необхідну для додавання такого правила до комунікаційного модуля,

Цей модуль також здатний отримувати конфігураційну інформацію, специфічну для системи реактивного захисту, що дозволяє налаштовувати його віддалено. Ця інформація про конфігурацію складається з політики безпеки та операційної політики, а також інформації, необхідної для налаштування реактивних дій.

Модуль конфігурації перевіряє конфігурації системи реактивного захисту. Ця перевірка підтверджує, що нові або оновлені конфігурації не конфліктують з уже існуючими. Ці конфігурації складаються з політики безпеки та операційної політики, а також конфігурацій, пов'язаних із дією. Ці пов'язані з дією конфігурації дозволяють налаштувати реактивні дії. Після перевірки цих конфігурацій вони зберігаються в базі знань про політику та дії. З іншого боку, конфігурації, пов'язані з виконанням реактивної системи під час виконання, також застосовуються до модуля *Active Response*.

Модуль активного реагування отримує та аналізує події безпеки від компонентів сторонніх розробників через модуль зв'язку. Аналіз цих подій безпеки виконується шляхом консультацій з базою знань про політику та дії з використанням підходів на основі асоціацій (наприклад, на основі правил [31]).

Після того, як подія безпеки була ідентифікована як порушення відповідних політик безпеки сегмента (тобто ідентифікована як вторгнення), модуль активного реагування перевіряє, чи існує відповідна реактивна дія для протидії такій події. Якщо ідентифікована пов'язана реактивна дія, модуль активної відповіді перевіряє, чи порушує ця дія оперативну політику сегмента, що міститься в базі знань політик і дій. За умови, що жодна операційна політика не порушується, модуль активного реагування виконує відповідну дію. Він також забезпечує відповідність стандартам серії *ISA/IEC 62443* (тобто *R2*), дозволяючи виконувати стратегії пом'якшення, запропоновані цими Стандартами.

База знань про політику та дії складається з енергонезалежних політик безпеки та операцій, які становлять реактивний захист сегмента мережі, а також інші конфігурації системи реактивного захисту. Операційні політики представляють обмеження, які необхідно підтримувати, щоб забезпечити правильну роботу системи автоматизації. З іншого боку, політики безпеки дозволяють перевірити, чи подія безпеки, отримана від комунікаційного модуля, ставить під загрозу безпеку відповідної зони (тобто порушує політику безпеки сегмента). Політики безпеки можуть мати відповідні реактивні дії, які дозволяють порушувати, блокувати або іншим чином протидіяти вторгненню в систему безпеки, визначеному з інформації про події безпеки, таким чином забезпечуючи відповідність стандартам серії *ISA/IEC 62443*.

3.2. Політика безпеки, операційна політика та реактивні дії в реальних системах автоматизації

Основою представленої концепції реактивного захисту є поточні архітектурні тенденції в *IAS* та політика безпеки та експлуатації, а також реактивні дії, що відповідають цим тенденціям.

Сучасні промислові мережі часто поділяються на сегменти та відокремлені [20]. Це покращує їхню продуктивність, полегшує керування

ними та підвищує їх безпеку [20, 26]. Серія стандартів *ISA/IEC 62443* включала та вдосконалювала ці поняття. Він також вважав, що операційна політика та управління політикою безпеки від зони до зони критично важливі для підтримки безпеки *IAS*. Ця серія стандартів, а також рекомендації, представлені в [20], особливо підкреслюють важливість механізмів безпеки, розташованих на краю кожної зони мережі.

З огляду на вищезгадані архітектурні тенденції та тенденції безпеки, класифікація безпеки та операційної політики, а також можливі реактивні дії представлені в наступних підрозділах. Важливо підкреслити, що політику та дії, які можуть відповідати конкретним *IAS*, слід аналізувати в кожному конкретному випадку. Однак у цьому розділі вони представлені в більш загальному вигляді, щоб окреслити обсяг можливостей, які надає представлена концепція.

По-перше, політики безпеки впливають із вимог безпеки, чітко обговорених у *ISA/IEC 62443-3-3* (тобто *ISA/IEC 62443* Частина 3-3 Вимоги до безпеки системи та рівні безпеки). Ця стандартна частина була розглянута, оскільки вона надає набір чітко визначених вимог безпеки, які слід враховувати системним інтеграторам, щоб захистити коректну роботу своїх систем [47]. Після цього оперативна політика впливає з керівних принципів [20], які краще розуміють поведінку систем автоматизації та вплив безпеки на них. Після цього обговорюються можливі реактивні дії. Ці реактивні дії впливають із самих політик безпеки, а також пропозицій, наданих вищезгаданими стандартами безпеки та інструкціями для *IAS*. Нарешті, надається обговорення того, як безпека, оперативна політика та реактивні дії забезпечують реактивний захист сегмента мережі.

3.2.1. Політика безпеки

Наступні класи політик безпеки були визначені на основі чотирьох різних компонентів, які становлять систему: зв'язок, комп'ютерні ресурси, користувачі та сеанси, а також послуги. П'ятий клас був інтегрований для представлення добре відомих подій, які потребують негайної уваги. Ці політики були обрані,

оскільки вони актуальні для *IAS* і надають можливості для реактивних дій, які можуть бути інтегровані в концепцію реактивного захисту, представлену в цій роботі.

Управління зв'язком (S1): Ці політики визначають обмеження, пов'язані з дозволим або забороненим зв'язком між системними компонентами. Ці політики часто враховують специфічні для зв'язку атрибути, такі як адреси джерела та призначення (тобто *IP*-адреси, *MAC*-адреси), номери логічних портів тощо. Цей клас дозволяє забезпечити безпеку виключно на основі характеристик зв'язку без урахування більш детальної інформації, наприклад інформація про користувача або послугу.

Управління обчислювальними ресурсами (S2): Ці політики визначають обмеження, пов'язані з обчислювальними ресурсами, знайденими в системі автоматизації. Ці політики часто враховують ресурси, які можна виміряти на рівні системи, кількох пристроїв або пристроїв. Прикладами таких ресурсів є: навантаження мережі, використання оперативної пам'яті, ПЗУ та ЦП тощо.

Контроль доступу користувачів і керування сеансами (S3): Ці політики стосуються ідентифікації та аутентифікації користувачів, пристроїв чи інших об'єктів, які мають ідентифікацію, а також сеансів та інших подій, що виникають у результаті такої автентифікації. Конкретні політики цієї категорії можуть включати, але не обмежуючись ними, обмеження, пов'язані з ідентифікацією, автентифікацією та інформацією про сеанс (наприклад, кількість невдалих спроб автентифікації, автентифікацію та статус сеансу та іншу детальну інформацію).

Управління послугами (S4): ці політики визначають дозволені або заборонені послуги чи протоколи, а також їх конфігурації. Вони не враховують специфічну для користувача інформацію щодо використання таких послуг.

Інциденти (S5): Ці політики представляють добре відомі умови, які вимагають негайних дій. Деякі з них: виявлення зловмисного програмного забезпечення та виявлення вразливостей.

Вищезгадана класифікація дозволяє визначити прості та зрозумілі

політики. Хоча існує кілька мов і стандартів політики безпеки [28], представлена концепція не розглядає її конкретно. Це зроблено для того, щоб забезпечити неоднозначність, яка може дозволити в майбутньому адаптувати цю концепцію для будь-якої бажаної мови або стандарту. Отже, в цій концепції політики розглядаються як абстрактні правила. Це можливо, оскільки політика часто містить інформацію, яка стосується наступних питань [29]: що, хто, коли і де. Крім того, більшість мов політики засновані на двох різних парадигмах [28]: парадигми «Подія-Умова-Дія» або «Умова-Дія».

З цих двох парадигм найбільш підходящою для концепції реактивного захисту, представленої в цій роботі, є парадигма «Подія-Умова-Дія», оскільки вона вимагає елемента *Event*, який запускає виконання дії. У представленій концепції подія – це будь-яка подія безпеки, отримана Системою реактивного захисту від сторонніх компонентів. Умова складається з обмежень безпеки, які повинні бути виконані (наприклад, служба *A* не повинна бути запущена). Нарешті, дією може бути будь-яка реактивна дія, яка допомагає виконати визначену Умову або допомагає протидіяти наслідкам вторгнення.

Крім того, ця проста класифікація політик дозволяє створювати більш складні політики, які можуть об'єднувати два або більше класів. Це зроблено, оскільки може бути можливим, що інформація про подію безпеки, яка надається в систему реактивного захисту, надходить із простих або складніших рішень безпеки. Приклади цього випадку: проста інформація про подію безпеки може бути отримана з простого системного журналу [50] клієнт, розташований на пристрої. Інформація про подію, надану цим клієнтом, може бути обмежена лише сповіщенням, яке містить інформацію про час та просту інформацію про подію (наприклад, послуга *A* почала працювати).

Цей випадок може потрапити до класу політики *S4*. З іншого боку, більш складна інформація про події безпеки може бути отримана від *IDS*, яка надає не тільки зміну статусу послуги, а й додаткову інформацію, таку як джерело зміни (наприклад, користувач *Y* запустив послугу *A*). Отже, цей приклад може потрапити до класів *S4* і *S3*.

3.2.2. Оперативні політики

На основі чотирьох важливих активів систем автоматизації були визначені наступні класи операційних політик: зв'язок, послуги, продуктивність і конфігурації.

Доступність зв'язку (O1): Ці політики зосереджені на визначенні стану комунікації, який слід завжди підтримувати і ніколи не переривати чи впливати. Цей зв'язок представлений специфічними для зв'язку атрибутами, як описано в S1. Однак ці політики зосереджені виключно на зв'язку, необхідному для виконання завдань автоматизації та управління системою (наприклад, зв'язок від пристрою А до пристрою В завжди має підтримуватися).

Доступ користувача та доступність послуг (O2): Ці політики визначають умови щодо доступу користувачів і послуг, які завжди повинні виконуватися. Ці умови необхідні для виконання завдань автоматизації або управління. Цей клас відрізняється від O1 тим, що надається більш конкретна інформація про послугу (наприклад, користувач А завжди повинен мати доступ до послуги Х).

Обмеження продуктивності (O3): Ці політики визначають умови продуктивності, які повинні підтримуватися в усій системі автоматизації або на кількох або окремих її пристроях. Вимірювання продуктивності має забезпечуватися компонентом третьої сторони (наприклад, навантаження мережі не повинно перевищувати поріг Т).

Обмеження конфігурації (O4): Ці політики визначають умови щодо конфігурацій, які необхідно підтримувати. Ці умови забезпечують коректну роботу системи автоматизації і, отже, часто пов'язані з пристроями автоматизації (наприклад, версія мікропрограми Х повинна бути встановлена у всіх пристроях типу Z).

Вищезгадані класи дозволяють визначати політики, які допомагають задовольнити вимоги до продуктивності та доступності для IAS. Важливо також підкреслити, що, хоча ці політики схожі на політики безпеки, згадані вище, вони не є однаковими. Політики безпеки отримуються з вимог безпеки, тоді як

оперативні політики отримуються з операційних вимог. Крім того, порушення політики безпеки є результатом чогось, що загрожує системі (наприклад, вторгнення), тоді як порушення операційної політики може бути результатом інших подій, не пов'язаних із безпекою (наприклад, збоїв). Крім того, операційна політика зосереджується виключно на вимогах або умовах самої системи автоматизації, а не на інших компонентах системи, не пов'язаних з автоматизацією.

3.2.3. Реактивні дії

Наведені нижче класи реактивних дій були отримані шляхом виявлення можливих контрзаходів щодо порушень вищезгаданих політик безпеки. Ці дії є елементом дії вищезгаданих політик безпеки:

Блокувати обліковий запис користувача (A1): Обліковий запис користувача заблоковано. Це може призвести до збою під час аутентифікації.

Відкликати привілеї користувача (A2): Привілеї, що належать обліковому запису користувача, анулюються. Це може призвести до невдалої авторизації для виконання певних дій або доступу до певних служб.

Завершення сеансу зв'язку (A3): Сеанс зв'язку або блокується, або припиняється на основі інформації про сеанс (наприклад, користувач, який бере участь у сеансі).

Завершення зв'язку (A4): Активний зв'язок припиняється на основі специфічних для зв'язку атрибутів (наприклад, протокол, логічний порт, адреси маршрутизації тощо).

Аналіз на вимогу (A5): Аналіз конкретних компонентів системи здійснюється на вимогу. Прикладами такого аналізу можуть бути аудити на вимогу, сканування або інші види перевірки (наприклад, антивірусна перевірка).

Конфігурація після вторгнення та збір інформації на вимогу (A6): Після виявлення вторгнення в поточну конфігурацію та стан активу вносяться зміни. Крім того, інформація, яка може використовуватися сторонніми компонентами для подальшого аналізу, може бути зібрана з певних компонентів системи

(наприклад, збираються журнали подій).

Виконання кожної з цих дій без урахування вищезгаданих операційних політик може вплинути на оперативні вимоги *IAS* (наприклад, можливості реального часу, висока продуктивність і доступність).

Крім того, важливо підкреслити, що концепція реактивного захисту, представлена в цій роботі, не обов'язково вимагає повного виконання реактивних дій, які повинні виконуватися Системою реактивного захисту. Ця система може лише підготувати інформацію, необхідну для виконання дії, а потім переслати її відповідному компоненту, який має функції для цього. Прикладами цього можуть бути: блокування облікового запису користувача або відкликання прав користувача може здійснюватися системою керування користувачами. Зв'язок може бути припинено через одну зі сторін зв'язку (наприклад, припинення сеансу віртуальної приватної мережі на сервері або клієнті) або компонентом третьої сторони (наприклад, динамічне додавання нового правила брандмауера). Сканування мережі може виконуватися брандмауером. нарешті,

3.2.4. Реактивний захист сегмента мережі

Політики безпеки та реактивні дії здатні забезпечити захист від вторгнень. Однак їх придатність для *IAS* може бути поставлена під сумнів. Для вирішення цієї проблеми необхідно також розглянути оперативну політику. Для цього представлена концепція передбачає розгляд як операційної політики, так і політики безпеки на міжзонній основі. Це дозволяє забезпечити децентралізований захист системи автоматизації. Ще одна перевага цього децентралізованого підходу полягає в тому, що він дає змогу аналізувати події безпеки з кількох джерел (наприклад, сторонні рішення безпеки).

На рис. 3.2 представлено процес, який здійснюється за допомогою Системи реактивного захисту, представленої в цій роботі. Цей процес починається з отримання події, пов'язаної з безпекою. Ця подія може бути отримана від стороннього компонента через мережу. Після цього ця подія аналізується, щоб перевірити, чи була порушена політика безпеки сегмента

мережі. Якщо порушення сталося, то вибирається відповідна реакція. Якщо реактивна дія підтримується системою реактивного захисту, тоді вона оцінюється відповідно до операційної політики сегмента. Якщо реактивна дія порушує операційну політику, вона не виконується і цей результат реєструється. З іншого боку, якщо реактивна дія не порушує жодної операційної політики, реактивна дія виконується.

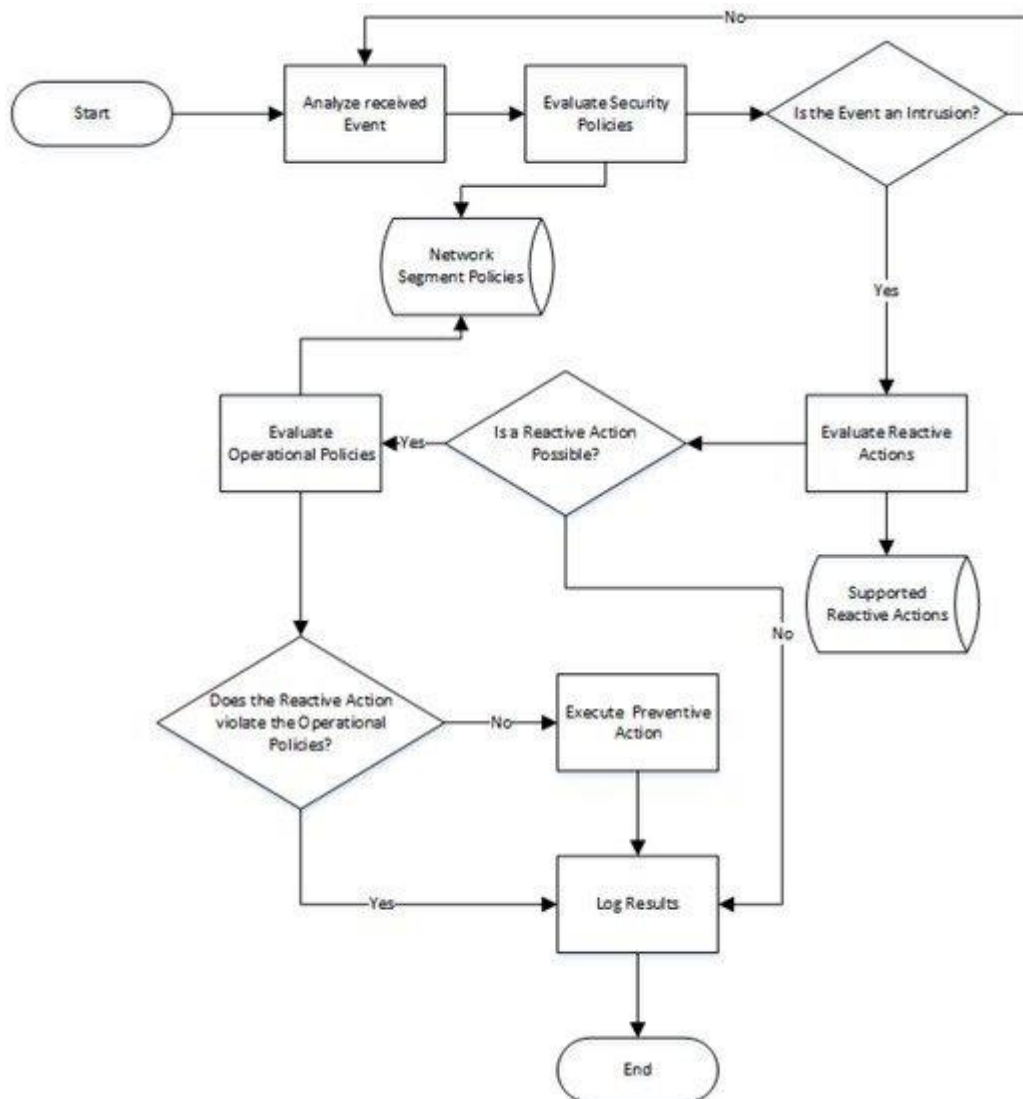


Рис. 3.2. Інформаційний потік представленої концепції реактивного захисту

Як було помічено, ця концепція гарантує, що жодна реактивна дія не буде виконана, якщо вона порушить роботу системи автоматизації, доки операційна політика чітко визначена. Хоча це вимагає людських зусиль для її конфігурації,

вона дає перевагу можливості реагувати на вторгнення без втручання людини, отже, забезпечує швидку відповідь за наявності вторгнень під час нормальної роботи системи.

3.3. Інтеграція технологій захисту інформації в системи промислової автоматизації

Щоб продемонструвати, як систему реактивного захисту можна інтегрувати в *IAS*, звернемось до представленої до цього архітектури *IAS* (рис. 2.1) було змінено та розширено (Рис. 3.3) для інтеграції компонентів безпеки та архітектурних схем, які зазвичай використовуються для промислових мереж.

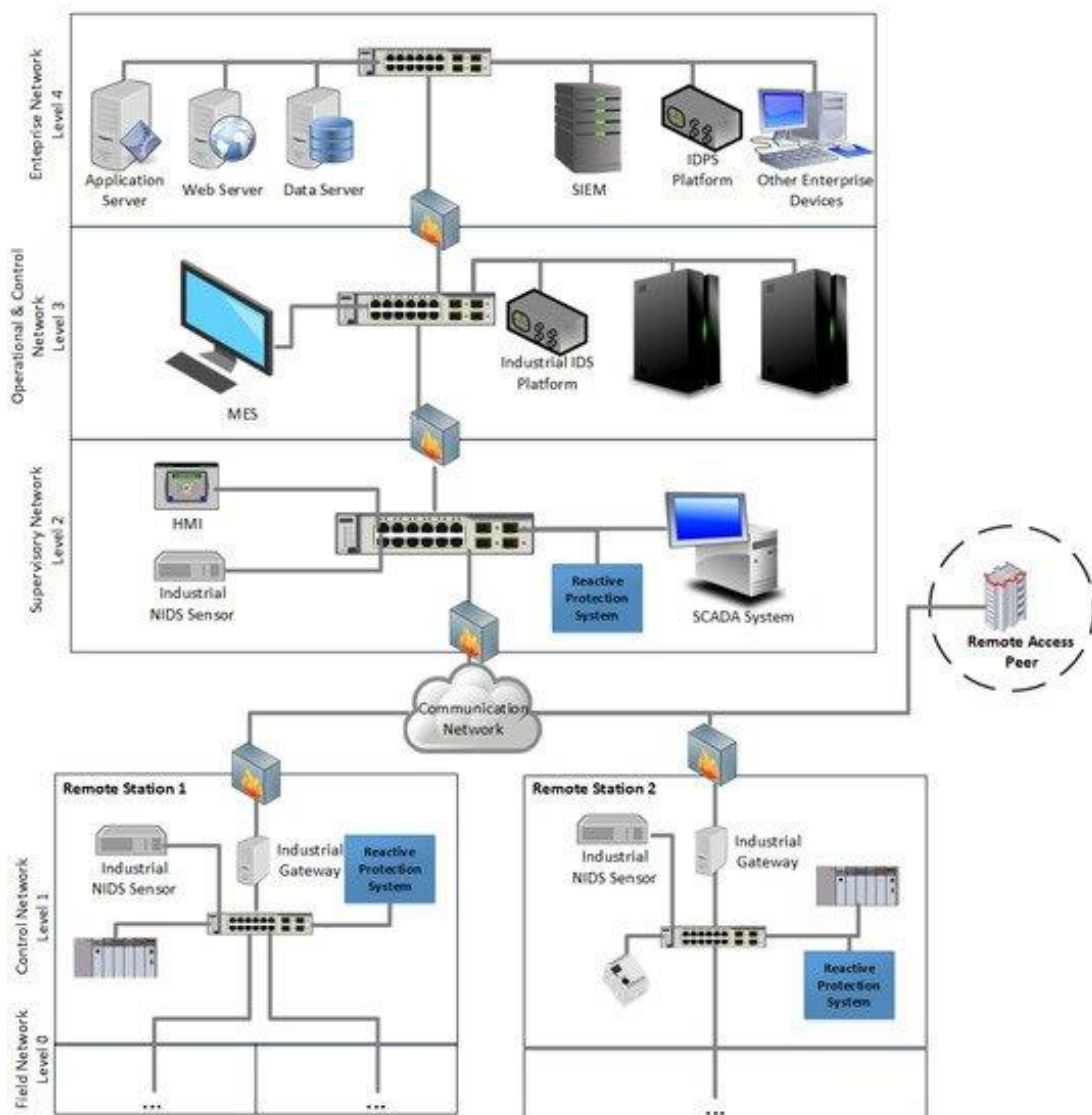


Рис. 3.3. Розширена архітектура *IAS* з віддаленим доступом і компонентами безпеки

Система виявлення та запобігання вторгненням (*IDPS*) була інтегрована в корпоративну мережу (рівень 4). Цей *IDPS* дозволяє контролювати цю мережу для виявлення вторгнень, що відбуваються на цьому рівні. З іншого боку, промислова мережа *IDS* була інтегрована в промислову мережу управління (рівні 1, 2 і 3). Ця промислова мережа *IDS* складається з централізованої платформи, розташованої в операційній і контрольній мережі, яка аналізує інформацію, надану датчиками, розташованими на нижчих рівнях (тобто мережами нагляду та контролю).

Польова та контрольна мережі були розділені на дві віддалені станції. Це сталося для того, щоб представляти розподілений *IAS*. Крім того, промисловий шлюз (також відомий як шлюз *IoT*) був розгорнутий на кожній із цих віддалених станцій. Промислові шлюзи – це новий тренд в *IAS*, який набирає популярності протягом останніх років [51,52,53]. Це пристрої, які дозволяють «встановлювати та підтримувати безпечне, надійне, відмовостійке з'єднання між хмарою та периферійними пристроями для збору й агрегації даних пристрою та керування пристроєм» [24]. Ці пристрої також можуть надавати розширені можливості залежно від їх виробника.

Була інтегрована точка віддаленого доступу для мереж нагляду та управління. Це відбувається, оскільки віддалений доступ до служб є поширеною програмою в *IAS*, особливо в розподілених *IAS*. Приклади цього: віддалені оновлення програмного забезпечення [25], віддалене керування виправленнями та обслуговування [21], дистанційне програмування, параметризація, моніторинг та діагностика [20, 26] тощо

Абстрактна мережа зв'язку являє собою зв'язок між віддаленими станціями, наглядовою мережею та однорангом віддаленого доступу. Ця комунікаційна мережа може бути будь-якою з наступного: Інтернет, глобальна мережа (*WAN*), локальна мережа (*LAN*) тощо. Система реактивного захисту розташована в кожній зоні мережі на рівнях контролю та нагляду (тобто рівнях 1 і 2). Системи реактивного захисту отримують події, пов'язані з безпекою, від

компонентів безпеки третіх сторін, розташованих в *IAS*. Ці події можуть стосуватися вторгнення або іншого порушення безпеки. Після того як система реактивного захисту отримує подію, пов'язану з безпекою, вона аналізує її, щоб перевірити, чи була порушена політика безпеки сегмента для відповідної зони мережі. Якщо відбулося порушення політики безпеки, він перевіряє, чи можлива реактивна дія (тобто підтримується Системою реактивного захисту та не порушує жодної з її операційних політик зони). Якщо реактивна дія можлива, то вона виконує її або надає необхідну інформацію сторонньому компоненту безпеки. Компоненти безпеки третьої сторони, які можуть надавати інформацію про події, пов'язані з безпекою, до системи реактивного захисту або які можуть виконувати реактивні дії в розширеній архітектурі *IAS*: *SIEM*, платформа *IDPS*, промислова платформа *IDS*, промисловий шлюз або брандмауери. Більше компонентів безпеки можна вбудувати в інші пристрої *IAS*, такі як інженерні робочі станції; однак у цій архітектурі ними нехтують, щоб забезпечити більшу ясність і простоту для обговорення.

Прикладом взаємодії між системою реактивного захисту та компонентами безпеки сторонніх розробників є наступний: промислова *IDS* виявила ненормальну поведінку в комунікації віддаленої станції 1, про яку вона повідомляє Систему реактивного захисту, розташовану на віддаленій станції 1. Цей реактивний Система захисту містить політику безпеки з підтримуваною реактивною дією, яка обробляє таку подію. Ця реактивна дія відноситься до сканування пристрою, яке виконується промисловим брандмауером, розташованим на віддаленій станції 1. Отже, система реактивного захисту надає інформацію, необхідну для промислового брандмауера для виконання такого сканування. Це сканування потенційно може виявити поточне або успішне вторгнення, що дає можливість протидіяти його наслідкам.

3.3.1. Політика безпеки та вторгнення

Було отримано п'ятнадцять політик безпеки. Ці правила та інформація про події представлені природною мовою, щоб забезпечити простий і зрозумілий опис кожної з них. Однак для їх технічної реалізації рекомендується

використовувати одну з багатьох мов політики та форматів подій.

IDS промислової мережі може надавати інформацію щодо подій зв'язку, користувачів і послуг (тобто *S1*, *S4*). Одним із прикладів цього є ідентифікація нової версії мікропрограми, яка завантажується в ПЛК. Після того, як система реактивного захисту отримує сповіщення про цю подію *IDS* промислової мережі, вона перевіряє політику безпеки зони мережі. Ця перевірка може призвести до виявлення порушеної політики безпеки (тобто *SP9*), що призведе до необхідності реактивної дії (тобто активної реакції).

Ця активна відповідь не залежить від будь-якої іншої відповіді (тобто активної чи пасивної), яка може підтримуватися *IDS* промислової мережі. Системні інтегратори та експерти з безпеки вирішують, які відповіді є доречними за наявності яких подій; отже, це має бути налаштовано та визначено до розгортання *IAS* або під час технічного обслуговування.

Перевага системи реактивного захисту полягає в тому, що вона також здатна доповнювати інші компоненти, які не забезпечують високого рівня складності та аналізу, як промислова мережа *IDS*. Прикладом цього є політика безпеки *SP4*, яка перевіряє поріг використання *RAM*. Його відповідну подію, пов'язану з безпекою, можна отримати від хост-пристрою, а не від складного рішення безпеки. Ця подія може бути забезпечена простою клієнтською програмою, яка відстежує використання оперативної пам'яті на хост-пристрої або *Host IDS*.

Ці вторгнення включають атаки безпеки та інші події (наприклад, неправильне використання та неправильні налаштування) в *IAS*, які можуть загрожувати безпеці системи (тобто порушувати політику безпеки). Вони були отримані з [24, 28]. Важливо підкреслити, що деякі з цих вторгнень можуть порушувати більше ніж одну політику безпеки. Отже, необхідно правильно налаштувати як політики безпеки, так і їх реактивні дії, щоб уникнути конфліктів (наприклад, одне вторгнення породжує два порушення політики безпеки, що виконує дві конфліктуючі реактивні дії).

Як *DoS*, так і *SYN Flood* атаки (*I1* і *I3*) можуть призвести до великої

кількості одночасних з'єднань і накладних витрат на продуктивність цільового пристрою (тобто порушує *SP2* і *SP4*). У бездротових пристроях атака перешкоджання (*I2*) може бути викликана неавторизованим бездротовим пристроєм (тобто, порушенням *SP15*). Атака грубої сили (*I4*) та зловживання користувачами в аутентифікації користувачів (*I8*) можуть перевищувати максимальну кількість спроб входу або підключення (тобто порушувати *SP6* і *SP7*).

З іншого боку, зловмисне програмне забезпечення (*I5*) може відкривати небажані логічні та фізичні порти (тобто, порушуючи *SP1* і *SP3*), створюючи бекдор для зловмисників. Він також може споживати небажані обчислювальні ресурси цільового пристрою, що призводить до перевищення попередньо визначених порогових значень (тобто, порушення *SP4*) та завантаження шкідливого програмного забезпечення (тобто, порушення *SP9*, *SP10*, *SP12* та *SP14*). Аналогічно, шкідливе програмне забезпечення можна завантажити в ПЛК, порушивши політику безпеки, яка описує час обслуговування, конфігурації та інші обставини (наприклад, *SP8*, *SP11*, *SP12* і *SP14*). Неправильне використання обчислювальних ресурсів може призвести до порушення політики безпеки, пов'язаної з максимальним порогом використання оперативної пам'яті та пам'яті аудиту (тобто порушення пакетів *SP4* і *SP5*). нарешті, неправильна конфігурація компонентів системи може призвести до порушення політик безпеки, подібних до тих, які виконує зловмисне програмне забезпечення. Можуть використовуватися небажані служби, логічні та апаратні порти (наприклад, *SP12*, *SP1* і *SP3*). Поріг зберігання аудиту можна обійти (тобто *SP5*). Уразливі програмні компоненти можуть бути встановлені на цільовому пристрої, що надає можливості для зловмисників (наприклад, *SP10* і *SP13*).

3.3.2. Реактивні дії за наявності вторгнень

З вищезгаданих політик безпеки та вторгнень (Таблиця 3 і Таблиця 4), відомо, що інформація про події, пов'язані з безпекою, аналізована Системою реактивного захисту, може надаватися сторонніми компонентами. Аналогічно,

система реактивного захисту може надавати інформацію цим компонентам, щоб виконувати реактивні дії, необхідні для кожної політики безпеки.

З метою пом'якшення та протидії вторгненням, представленим в Таблиця 4 (тобто *I1–I10*), було отримано п'ятнадцять можливих реактивних дій.

Таблиця 5 представляє ці реактивні дії, їх відповідні сторонні компоненти безпеки, здатні їх виконувати, і вторгнення, які кожне з них допомагає протидіяти або пом'якшувати. Важливо підкреслити, що ці реактивні дії виконуються відповідно до політики безпеки та операційної політики Системи реактивного захисту. Дія виконується лише в тому випадку, якщо була порушена політика безпеки, з нею пов'язана реактивна дія, і ця дія не порушує оперативну політику.

Атаки грубої сили, зловживання, спричинені користувачами та сеансами зв'язку (тобто *I4* та *I8*), можуть бути пом'якшені системою керування користувачами. Ця система може блокувати обліковий запис користувача, анулювати його привілеї або блокувати сеанс (тобто *RA1*, *RA2* і *RA3*). Сервер додатків також може блокувати або блокувати сеанс. Після того, як система реактивного захисту виконала будь-яку з цих дій, людині може знадобитися проаналізувати, чи потрібно скасувати ці зміни (тобто розблокувати користувача).

Перенаправлення трафіку та обмеження швидкості (тобто *RA5* і *RA6*), які підтримуються деякими *IDS*, брандмауерами та серверами додатків, допомагають пом'якшити вторгнення, які збільшують швидкість мережі (тобто *I1*, *I2*, *I3* та *I4*). Це особливо важливо для *IAS*, оскільки на можливості реального часу може вплинути високий мережевий трафік у мережах на основі *Ethernet*.

Антивіруси, маршрутизатори, брандмауери, ідентифікатори мережі та системи керування подіями (*RA8*, *RA9* і *RA10*) як для корпоративної, так і для промислової мережі можуть надавати можливості аудиту та сканування, які допомагають більш детально аналізувати компоненти системи. Це особливо корисно за наявності зловмисного програмного забезпечення та атак грубої сили (*I5* і *I4*), щоб перевірити, чи вдалося вторгнення, і, якщо воно сталося,

перевірити, чи воно поширилося чи досягло своєї мети (тобто скомпрометовано компонент системи).

IDS промислової мережі також може надавати можливості для виконання резервного копіювання та відновлення конфігурацій (тобто *RA11*), специфічних для компонентів *IAS*. Це може допомогти видалити шкідливе програмне забезпечення (наприклад, *I5* і *I7*) або виправити неправильні конфігурації (тобто *I10*). Інші неправильні конфігурації на хост-пристрої *I10* можна виправити за допомогою програмного забезпечення самого хост-пристрою (наприклад, *RA14*) або за допомогою систем керування журналами та подіями (наприклад, *RA15*).

Нарешті, брандмауери та кінцеві точки *VPN* (тобто *RA4* та *RA7*) також здатні пом'якшувати вторгнення, пов'язані зі зв'язком (тобто *I1*, *I2*, *I3* та *I4*). Вони також здатні захищати компоненти *IAS* (тобто *I7* і *I8*), оскільки вони широко використовуються в промисловості (як спостерігається в Рис. 4).

3.4. Реалізація системи реактивного захисту інформації комп'ютерної мережі

Прототип системи реактивного захисту реалізовано в пристрої промислового *IoT Gateway* від *Bosch Rexroth AG* (Лор-на-Майні, БУ, Німеччина) [29]. Архітектура цього пристрою складається з дистрибутива *Linux* з відкритим вихідним кодом та інтегрованої віртуальної машини *Java (JVM)*, яка дозволяє розгортати програми *Java* через *Open Services Gateway Initiative (OSGi Framework)* [20].

Структура *OSGi* [21] дозволяє керувати та впроваджувати програми *Java*. Він забезпечує платформу з модульною архітектурою, яка дозволяє керувати додатками як незалежними компонентами, які називаються пакетами. Пакети можуть взаємодіяти один з одним завдяки *OSGi Framework* через публікацію та підписку на послуги, які вони надають. *OSGi Framework* також дозволяє керувати їхніми залежностями та версіями, що дозволяє контролювати

видимість їхніх служб і компонентів і зменшувати складність керування.

Отже, прототип був запрограмований на *Java* та розгорнутий у середовищі *OSGi*. Основними характеристиками прототипу реактивного захисту є наступні:

Можливість налаштування операційної політики та політики безпеки, а також статусу реактивної системи через графічний інтерфейс користувача.

Підтримуються такі політики безпеки: максимальна кількість спроб входу та аномальний мережевий трафік.

Підтримуються такі операційні політики: доступність зв'язку на основі певної *IP*-адреси або підмережі.

Підтримується наступна реактивна захисна дія: розірвання відкритих підключень до віртуальної приватної мережі (*VPN*) для захисту від виявлених вторгнень.

Зв'язок підтримує наступне: *Syslog* [10] за протоколом дейтаграм користувача (*UDP*), протоколом керування передачею (*TCP*) і безпекою транспортного рівня (*TLS*); та загальний формат подій (*CEF*) [17, 22].

Клієнт *VPN* належить до набору програм, наданих *Bosch Rexroth AG* у контексті свого *IoT Gateway*. Крім того, взаємодія між прототиповою системою реактивного захисту та клієнтом *VPN* можлива завдяки фреймворку *OSGi*.

3.5. Оцінка доцільності та застосовності Концепції реактивного захисту

Доцільність та застосовність представленої концепції оцінювалася двома способами. Спочатку представлено сценарій, який часто зустрічається в промислових системах, пов'язана з ним модель змагальності та особливості його емуляції. З цього сценарію виходить набір варіантів використання. Ці випадки використання демонструють застосовність представленої концепції, розглядаючи прототипну систему реактивного захисту та описуючи різні результати, які можна отримати на основі різних конфігурацій. Після цього виконання чотирьох вимог (тобто *R1–R4*), представлених у стРозділ

Зперевірено. Ця перевірка здійснюється шляхом виведення чотирьох гіпотез, які доводять доцільність представленої концепції. Обговорення цих гіпотез додатково обґрунтовується наведеними сценаріями використання.

3.5.1. Сценарій і модель змагальності

Щоб підтвердити представлену концепцію реактивного захисту, реальний сценарій, отриманий з еталонної архітектури IAS (Рис. 3.3) представлено. Цей сценарій показаний в Рис. 3.4. Він представляє спрощений приклад програми віддаленого обслуговування.

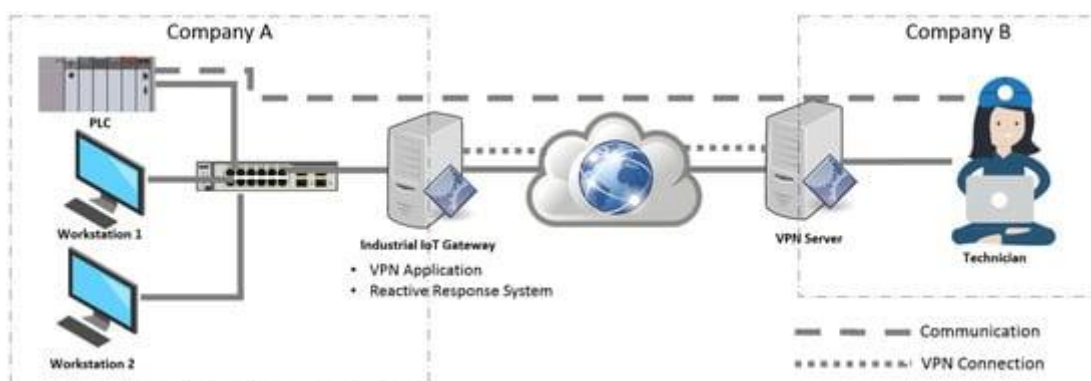


Рис. 3.4. Спрощений промисловий сценарій програми віддаленого обслуговування, отриманий на основі еталонної архітектури IAS

У представленому сценарії існують дві компанії: компанія А і компанія Б. Система автоматизації розташована на території компанії А; це представлено програмованим логічним контролером (ПЛК) і двома інженерними робочими станціями (Робота 1 і Робоча станція 2). Технік, розташований на сайті компанії В, бажає виконувати технічне обслуговування пристроїв, розташованих на території компанії А. Щоб виконувати технічне обслуговування безпечним способом, між цими двома сайтами встановлюється з'єднання віртуальної приватної мережі (VPN). Кінцева точка VPN на сайті компанії А представлена шлюзом *Bosch Rexroth IoT*. Як обговорювалося в попередньому розділі, Шлюз *IoT* містить програму-клієнт VPN, яка дозволяє йому встановлювати з'єднання з кінцевою точкою, розташованою на сайті Компанії Б, що дозволяє йому встановлювати пряме з'єднання з комп'ютером Технічного спеціаліста. З

іншого боку, кінцевою точкою на сайті компанії *B* може бути будь-який пристрій, який може надавати ті ж функції, що й сервер *VPN*.

Для цього випадку передбачається, що облікові дані, необхідні для налаштування *VPN*-з'єднання, вже надано. Також передбачається, що конфігурації *VPN* захищені від несанкціонованих змін.

Змагальна модель, яка розглядається для цього сценарію, складається із зовнішніх загроз, які можуть поширюватися через безпечне *VPN*-з'єднання до системи автоматизації, розташованої на сайті компанії *A* (наприклад, хробак *Slammer* [63]) або неправильне використання з боку Техніка.

3.5.2. Емуляція тестового сценарію

Емуляція вищезгаданого Сценарію здійснюється наступним чином. Визначено дві локальні мережі (*LAN*). У *LAN A* розташовані компоненти промислової автоматизації. Це представляє ПЛК та персональний комп'ютер (ПК). Пристрій *Industrial IoT Gateway* містить програму-клієнт *VPN*, а також систему реактивного захисту. Він також налаштований з двома різними *IP*-адресами, кожна з яких відповідає *LAN A* та *LAN B* відповідно. Крім того, події безпеки, які аналізуються системою реактивного захисту, генеруються на ПК. Цей ПК містить програму *Java*, розроблену з єдиною метою генерації повідомлень у загальному форматі подій. У реальному житті ці повідомлення про події будуть створюватися стороннім рішенням безпеки. однак, програма *Java* використовується для прототипу програми та її оцінки з метою спрощення процесу тестування.

Сервер *VPN* працює на *Raspberry Pi*, розташованому в *LAN B*. Двома сторонами *VPN*-з'єднання є промисловий шлюз *IoT* і *Raspberry Pi*. Через *VPN*-з'єднання можливе будь-яке спілкування (наприклад, завантаження програми *PLC*). Для цього тестового сценарію він представлений простим зв'язком між користувачем, розташованим у локальній мережі *B*, і ПЛК, розташованим у локальній мережі *A*. Огляд цього налаштування представлено в Рис. 3.5.

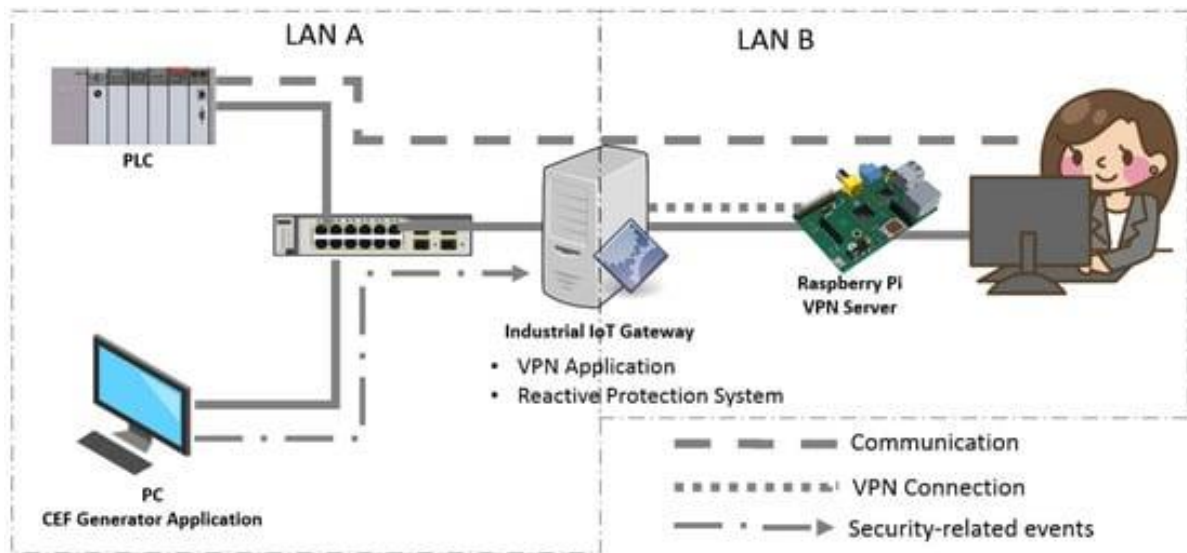


Рис. 3.5. Емуляція промислового сценарію програми віддаленого обслуговування *LAN*

3.5.3. Варіанти використання сценарію

З вищезгаданого сценарію впливають три варіанти використання. У кожному з цих трьох випадків використання порушується одна і та ж політика безпеки.

Політика безпеки, яку підтримує прототип системи реактивного захисту відноситься до перевищення максимальної кількості дозволених невдалих спроб входу (наприклад, користувач не вдається увійти до ПЛК кілька разів). Щоб запустити аналіз, проведений прототиповою системою реактивного захисту (див. Рис. 3.2 у розділі 3.2), програма генератора *CEF*, розташована на ПК, надсилає повідомлення *CEF*. Це повідомлення *CEF* містить інформацію, яка дозволяє системі реактивного захисту ідентифікувати політику безпеки, яка порушується.

Після того, як система реактивного захисту визначає, що *a*- і яка політика безпеки була порушена, вона перевіряє, чи можлива реактивна дія для протидії цьому порушенню політики. Для такого типу порушення політики система реактивного захисту підтримує припинення активних *VPN*-з'єднань. Виконання або відхилення такої дії залежить від операційної політики. Наведені нижче варіанти використання представляють різні альтернативи конфігурації для цих

операційних політик, що призводить до різних результатів для системи реактивного захисту. Для цілей цієї оцінки ініціюється VPN-з'єднання між LAN A та LAN B.

Випадок використання 1: У цьому випадку використання існує оперативна політика, яка визначає, що зв'язок між двома сторонами завжди має бути доступним. Ці сторони визначаються через їхні IP-адреси. Ці IP-адреси ідентифікуються як учасники відкритого VPN-з'єднання, і, отже, реактивна дія не виконується.

Випадок використання 2: Цей варіант використання подібний до варіанту використання 1. Однак у цьому випадку оперативна політика вказує на доступність зв'язку для певної підмережі, а не для певних IP-адрес. Під час перевірки операційних політик виявлено, що IP-адреса однієї зі сторін VPN-з'єднання знаходиться в цій підмережі, і, отже, реактивна дія не виконується.

Випадок використання 3: У цьому випадку використання не існує жодної з вищезгаданих політик, і, отже, виконується реактивна дія. Це означає, що активне VPN-з'єднання закрито. Якщо відсутність операційної політики була навмисною і відображає експлуатаційні вимоги системи автоматизації, то припинення VPN-з'єднання не впливає на роботу базової системи. Однак, якщо нехтування операційною політикою було ненавмисним, це могло б збільшити проблему доступності в системі, яка потенційно може призвести до збою в IAS.

3.6. Налаштування корпоративної мережі для розширеного захисту

Всі кінцеві точки та сервери в корпоративній мережі або підмережі, також як і мобільні пристрої, знаходяться на прицілі у кібер-злочинців, які розглядають їх як мету та засоби для досягнення інших цілей у атакованій компанії. Настійно рекомендуємо, щоб компанії застосовували максимальний захист кожної кінцевої точки (ПК, ноутбук або сервер) у своїй корпоративній мережі, включаючи всі підмережі та віддалені офіси. Це найкращий спосіб запобігти серйозним фінансовим і репутаційним збиткам, уникнути злому

систем і захистити компанію від будь-яких інших інцидентів, які негативно можуть вплинути на роботу компанії.

Така рекомендація заснована на нашому досвіді та знанні мотивів кібер-злочинців, першим завданням яких є пошук найбільш уразливого пристрою, який можна було б використовувати для доступу до інших комп'ютерів та серверів. Після установки в мережі, їх «твори» потай починають шукати слабку ланку компанії для доступу до робочих станцій і серверів – реальних цілей багатьох атак. Для цього вони здатні здійснити незліченну кількість ітерацій та прихованих дій, щоб виконати свої шкідливі дії та скомпрометувати потрібний сервер.

Єдиний спосіб захистити всі пристрої – це ретельний моніторинг та контроль кожної дії, що вживається на всіх робочих станціях та серверах, класифікуючи кожен запущений процес та виявляючи всі взаємозв'язки з іншими процесами, включаючи легітимні процеси, які можуть допомогти хакерам зламувати корпоративні програми, системи та здійснювати крадіжку /псування інформації.

Нижче наведемо деякі приклади реальних атак, які наочно ілюструють, чому безпосередній захист усіх мережевих ресурсів, включаючи сервери, офісні та віддалені робочі станції, – це єдиний ефективний захист від кібер-атак і, що особливо важливо, невідомих загроз.

3.6.1. Описання атак на корпоративні сервери

Кожен сервер у корпоративній мережі – це бажана мета для кожного кібер-злочинця через різні причини:

- вони мають відкриті порти та встановлюють з'єднання.
- Часто відсутній постійний моніторинг активності сервера. Тобто. як правило, контролюється тільки його продуктивність.
- Сервери не завжди мають всі встановлені патчі і не завжди, виявляється, повноцінно захищені через те, щоб виключити проблеми, викликані питаннями продуктивності, простоїв у роботі та ін.

- вони мають величезну кількість запущених процесів, тому більш

чутливі до наявних уразливостей, які можуть бути використані хакерами.

Сімейство рішень з функціями розширеного захисту *Adaptive Defense* надає можливість «з перших рук» спостерігати за техніками, які використовуються кібер-злочинцями для компрометації різних типів внутрішніх серверів, навіть тих, які не дивляться в Інтернет.

Важливо мати на увазі, що хакери зазвичай не запускають пряму атаку на свою мету, а підбираються до неї поступово і дуже тонко. Ось чому ми спостерігаємо зростання кількості атак, які не використовують будь-які шкідливі програми. Що хакери роблять - так це намагаються наблизитися до своєї мети, не викликаючи підозр, роблячи різні маневри, що відволікають, і побічні рухи. Найчастіше метою є саме сервери, т.к. вони, як правило, є тими ІТ-активами, де міститься найбільший обсяг конфіденційної інформації, і вони можуть використовуватися злочинцями для запуску атак на інші комп'ютери всередині мережі або за її межами.

Нижче ми розповімо про найпоширеніші атаки на сервери, які ми бачили в лабораторії *PandaLabs* останнім часом та які блокувалися рішенням *Adaptive Defense*.

3.6.2. Описання атак на сервери баз даних *SQL/MySQL*

Взагалі кажучи, перше, що помітите при такому типі атаки - це аномалія у трафіку, що входить до сервера з БД. Використовується хакерами для пошуку та використання вразливостей на сервері БД (який не завжди «пропатчений» через побоювання у простої тощо).

Як тільки знайдено необхідну вразливість, хакери змушують сервер генерувати шкідливі файли на жорсткому диску та запускати їх для того, щоб отримати повний контроль над системою. Завдяки розширеному захисту в *Adaptive Defense*, ми бачимо, як хакери створюють користувачів зі специфічними профілями для віддаленого доступу до серверів і використовують останні як стартові майданчики для кібер-атак на інші мережеві ресурси.

3.6.3. Описання атаки через віддалене підключення до робочого столу

Це поширений спосіб атаки на корпоративні сервери, і він став дуже популярним за останній рік з метою поширення шифрувальників. Він полягає в тому, щоб отримати доступ до цільового комп'ютера через Інтернет, щоб можна було віддалено ним керувати. Як тільки кібер-злочинці знаходять сервер із включеним *Remote Desktop Protocol*, вони запускають проти нього атаку типу *brute-force* для підбору реєстраційних даних (ім'я користувача та пароль). В антивірусній лабораторії *PandaLabs* за останні місяці виявили безліч прикладів подібних атак, наприклад:

- “*Crysis*” у всьому світі через віддалений робочий стіл;
- це не *ransomware*, але в будь-якому випадку може "захопити" ваш сервер;
- *RDPPatcher* продає доступ до вашого комп'ютера за низькою ціною.

3.6.4. Описання атак на доменні та файлові сервери

Незалежно від методу, який використовується хакером для проникнення в корпоративну мережу, добре відомо, що одна з головних цілей будь-якого вторгнення – це отримання користувача, який може використовуватись для виконання певних дій усередині ІТ-структури. Це робить сервери управління доменом первинною метою хакерів, т.к. такі сервери зберігають облікові записи адміністратора домену (потрібні для виконання цих «певних» дій) і мають доступ до всіх комп'ютерів у домені.

Аналіз постійних загроз підвищеної складності (*APT*) показав, що використання серверів управління доменами – це поширена практика для запуску атак у мережі. Наприклад, один з клієнтів *Adaptive Defense* використовував традиційний антивірусний захист на своїх серверах, у той час як на робочих станціях в домені поверх цього захисту був налаштований наш розширений захист. Якогось моменту на робочих станціях стала спрацьовувати розширений захист, т.к. вона почала ідентифікувати та блокувати атаки на них. Розслідування показало, що ці атаки були здійснені з корпоративних серверів – насправді вони були зламані.

Ризик зараження невідомим шифрувальником підключених мережових дисків. Мережові диски часто використовуються для спільного доступу до інформації з різних комп'ютерів, але також становлять серйозну небезпеку зараження.

Якщо комп'ютер із підключеними мережними дисками був заражений шифрувальником, то дії цієї шкідливої програми не обмежаться тільки зараженим комп'ютером, але вони будуть поширені і на спільні ресурси мережових дисків. Щоб знизити ризик, організаціям рекомендується впроваджувати обмежувальні заходи контролю доступу, видаляючи права на запис у мережі скрізь, де це можливо.

Для забезпечення належного захисту кожного комп'ютера в мережі ми рекомендуємо встановлювати рішення з функціями розширеного захисту *Adaptive Defense* або *Adaptive Defense 360* на кожний комп'ютер.

Одна з найпоширеніших помилок полягає в тому, що розширеного захисту достатньо для захисту лише тих комп'ютерів, які містять спільні ресурси, залишаючи інші комп'ютери без розширеного захисту. Однак при такому сценарії, якщо незахищений комп'ютер був заражений шифрувальником, цей зловред намагатиметься зашифрувати всі документи, які він знайде на доступних дисках в системі, включаючи мережні диски.

Щоб віддалено зашифрувати вміст мережних дисків, шифрувальник використовує віддалені виклики процедур (*RPC*). З точки зору комп'ютера, на якому фізично знаходяться ці мережові диски, йдеться про цілком легітимну операцію, що виконується легітимними процесами операційної системи (доступ та зміна файлів з даними). Тобто. легітимна поведінка не асоціюватиметься зі шкідливими діями.

Проте насправді запускається шкідливий процес на тому комп'ютері, звідки йде атака. Тому вона має бути ідентифікована та зупинена саме там. Саме тому необхідно, щоб розширений захист було впроваджено кожному комп'ютері.

3.6.5. Приклад налаштування розширеного захисту в *Adaptive Defense 360*

Adaptive Defense 360 – це хмарне SaaS-рішення інформаційної безпеки з функціями розширеного захисту. А у цій дипломній роботі на прикладі цього продукту давайте подивимося, наскільки трудомістко налаштовувати розширений захист від невідомих загроз.

За рахунок того, що функції розширеного захисту максимально автоматизовані, то налаштування займає досить мало часу.

Можна паралельно робити аналогічні дії у демо-консолі *Panda Adaptive Defense 360* (для роботи буде потрібно лише браузер – бажано *Chrome* або *Firefox*, нічого встановлювати не потрібно).

Увійшовши в консоль *Panda Cloud*, обираємо *Panda Adaptive Defense 360* і переходимо в консоль управління, після чого в основному меню виберіть розділ Налаштування (рис. 3.6).

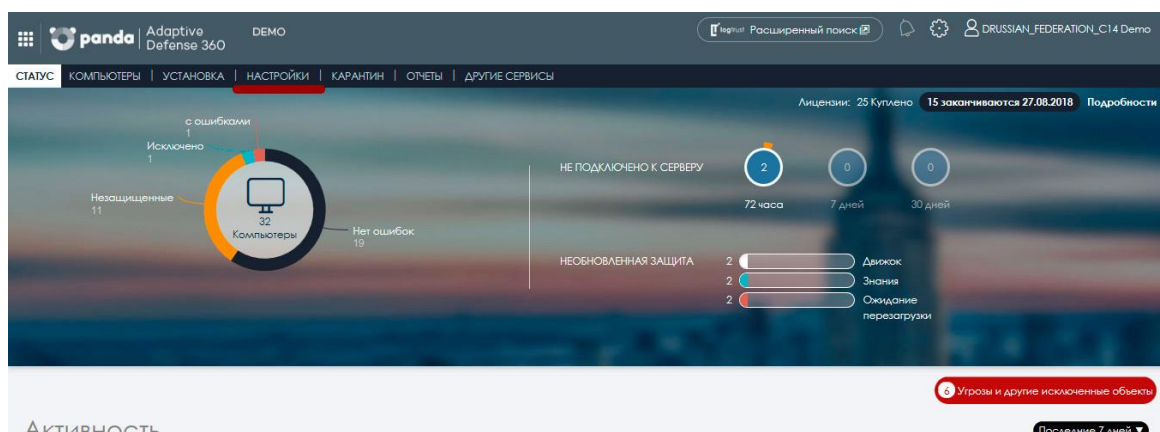


Рис. 3.6. Налаштування захисту комп'ютерної мережі засобами *Adaptive Defense 360*

У цьому розділі системи зліва представлені групи комп'ютерів, а праворуч – профілі безпеки (рис. 3.7). Управління розширеним захистом складає основі профілів. Тому потрібно вибрати потрібний профіль, в якому потрібно її налаштувати. Наприклад, візьмемо профіль *Default*:

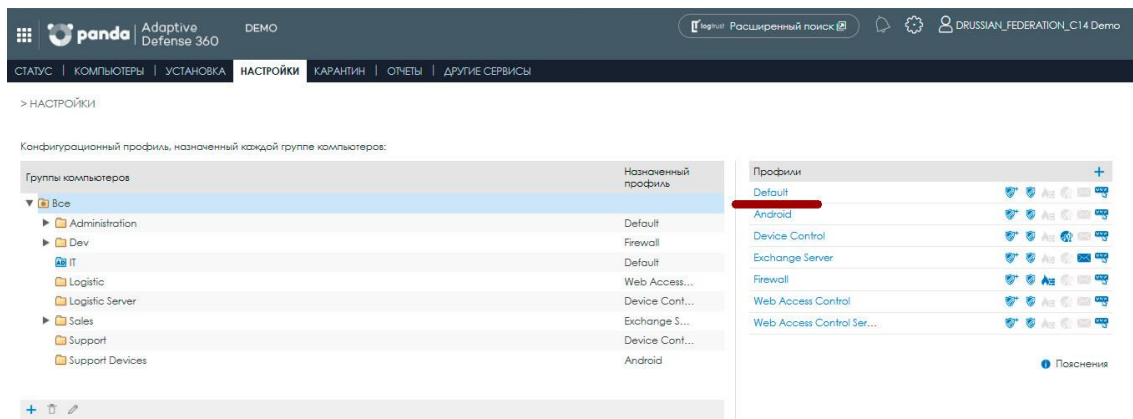


Рис. 3.7. Управління розширеним захистом у системі *Adaptive Defense 360*

У профілі, що відкрилося, в меню зліва виберемо розділ Розширений захист (рис. 3.8).

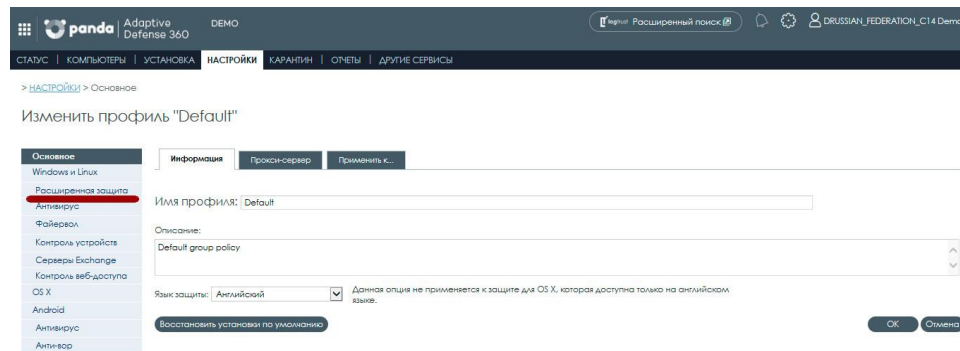


Рис. 3.8. Створення нового сценарію в системі *Adaptive Defense 360*

В результаті цього відкриється сторінка з налаштуваннями розширеного захисту (рис. 3.9).

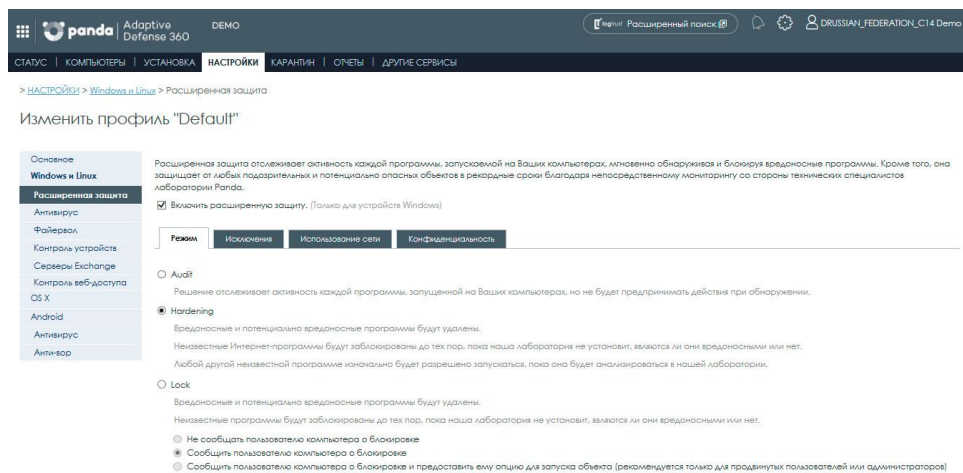


Рис. 3.9. Додаткові налаштування розширеного захисту у системі *Adaptive Defense 360*

Щоб увімкнути розширений захист для цього профілю, поставте галочку у опції Увімкнути розширений захист. Звертаємо Вашу увагу на те, що зараз цей функціонал пропонується лише для пристроїв із Windows.

Після цього Вам будуть доступні опції налаштування, розділені на чотири закладки: Режим, Винятки, Використання мережі та Конфіденційність. Розглянемо їх докладніше.

Режим – розширений захист дозволяє встановити різні режими безпеки для блокування невідомих шкідливих програм і захистити комп'ютери від сучасних загроз і постійних загроз підвищеної складності.

Аудит – цей режим призначений лише для моніторингу невідомих загроз. У такому режимі роботи рішення нічого не блокує, а лише відстежує всі запуснені процеси та взаємозв'язки між ними і надає результати моніторингу у вигляді експертної інформації. До речі, цей режим рекомендується використовувати в перші 2-3 тижні з моменту впровадження *Adaptive Defense*, щоб рішення могло «познайомитися» з ПЗ, що використовується в компанії, і адаптуватися під його специфіку.

Hardening – у цьому режимі рішення дозволяє запуск некласифікованих програм, які вже встановлені на комп'ютерах користувачів. При цьому рішення буде відслідковувати всі процеси, породжені такими програмами, щоб запобігти шкідливим та підозрілим з них, а також кожна з таких програм приблизно протягом доби буде проаналізована в антивірусній лабораторії *PandaLabs* для класифікації.

Також в даному режимі рішення блокуватиме всі невідомі програми, які надходять на комп'ютер із зовнішніх джерел (Інтернет, електронна пошта, флешки та ін.), доки воно не буде класифіковано. У свою чергу, програми, класифіковані як шкідливі, будуть переміщені до централізованого карантину.

Lock – цей режим дозволяє заблокувати запуск усіх невідомих (некласифікованих у *PandaLabs*) програм, доки вони не будуть класифіковані. Цей режим має досить серйозні обмеження на використання невідомого ПЗ, однак у переважній більшості випадків кожна така невідома програма буде

класифікована протягом доби. Крім того, адміністратор завжди має можливість зробити виняток із блокування для кожної конкретної невідомої програми.

Якщо вибрано цей режим, можна настроїти такі опції:

- не повідомляти користувачеві комп'ютера про блокування;
- локальний агент не буде показувати будь-які повідомлення при блокуванні невідомої програми;
- надати опцію для запуску об'єкта – у цьому випадку кінцевому користувачеві протягом 1 хвилини відображається повідомлення, де він може вибрати варіант запуску заблокованої програми під свою відповідальність. Такі винятки є постійними, доки адміністратор не змінить конфігурацію в консолі керування.

Винятки – на цій закладці можна настроїти об'єкти на комп'ютерах, які не перевірятимуться рішенням *Adaptive Defense*. Дані налаштування будуть актуальні як для розширеного захисту, так і антивірусного захисту теж (рис. 3.10). На цій закладці можна вказати розширення, папки або файли, які потрібно виключити з контролю.

Основное
Windows и Linux
Расширенная защита
Антивирус
Файрвол
Контроль устройств
Серверы Exchange
Контроль веб-доступа
OS X
Android
Антивирус
Анти-вор

Расширенная защита отслеживает активность каждой программы, запускаемой на ваших компьютерах, мгновенно обнаруживая и блокируя вредоносные программы. Кроме того, она защищает от любых подозрительных и потенциально опасных объектов в рекордные сроки благодаря непосредственному мониторингу со стороны технических специалистов лаборатории Panda.

☒ Включить расширенную защиту. (Только для устройств Windows)

Режим | Исключения | Использование сети | Конфиденциальность

Изменение этих параметров позволит снизить уровень безопасности
Каждый раз, когда вы исключаете файл или папку из сканирования, существует шанс, что вредоносная программа запустится на вашем компьютере, и Adaptive Defense 360 не сможет обнаружить ее.

Эти параметры влияют одновременно на антивирусную защиту и расширенную защиту.

Расширения для исключения:

.CER
.SAFE

Добавить
Удалить
Очистить

Папки для исключения:

C:\INACCESSIBLE_FOLDER
C:\SAFE_FILES

Добавить
Удалить
Очистить

Файлы для исключения:

C:\CHECKED_AND_SAFE.EXE
C:\UTILS\VACINED.EXE

Добавить
Удалить
Очистить

Рис. 3.10. Налаштування винятків у розширеному захисті

Використання мережі – кожен некласифікований в *PandaLabs* файл, який виконується, який намагається запуснитися на комп'ютері користувача, відправляється агентом на наш сервер для ретельного аналізу. Ця функція налаштована таким чином, щоб не впливати на продуктивність комп'ютерної мережі. У зв'язку з цим за замовчуванням опція Максимальна кількість МБ, яка може бути передана за годину, має значення 50 МБ.

Можна вказати в даній опції необхідне значення в МБ або поставити значення 0, якщо не хочемо обмежувати обсяг файлів, що передаються (рис. 3.11).

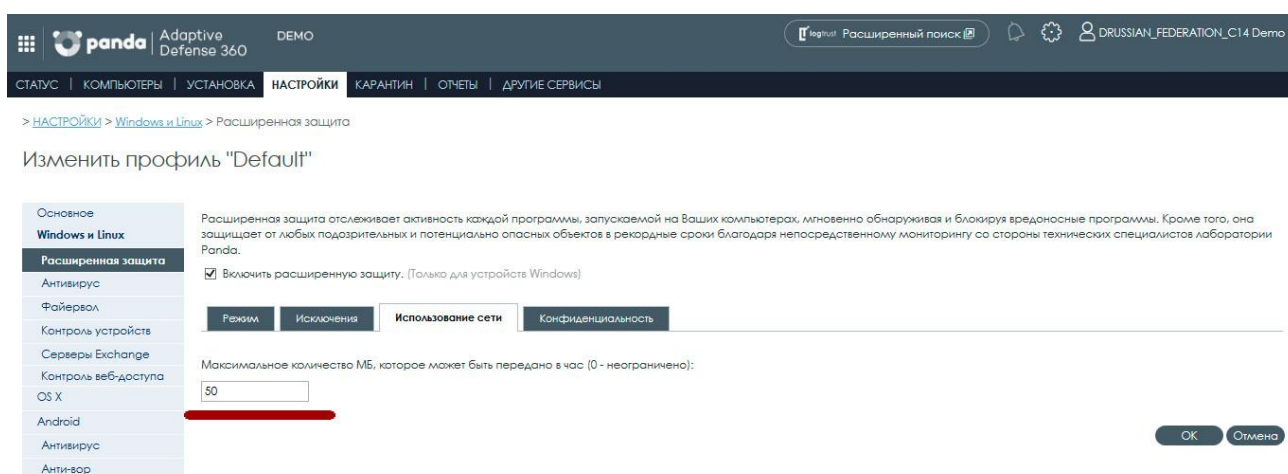


Рис. 3.11. Налаштування обмеження розміру файлів

Невідомі файли відправляються лише один раз серед усіх користувачів у світі, які використовують *Adaptive Defense*, тому якщо даний невідомий файл вже надсилався агентом будь-якого користувача, то з комп'ютера іншого користувача він вже не надсилатиметься. Крім того, у рішенні використовуються спеціальні механізми, які дозволяють оптимізувати використання мережевих ресурсів і максимально знизити навантаження на корпоративну мережу.

Конфіденційність – на цій закладці Ви можете налаштувати кілька опцій конфіденційності:

– якщо вибрати першу опцію, то рішення збиратиме і показуватиме адміністратору в консолі управління (і звітах) назву та повний шлях файлів з

даними, до яких зверталися шкідливі програми / процеси;

— якщо вибрати другу опцію, то адміністратор зможе побачити в консолі управління (і звітах) дані щодо користувача, який був авторизований у системі в момент виявлення загрози на комп'ютері.

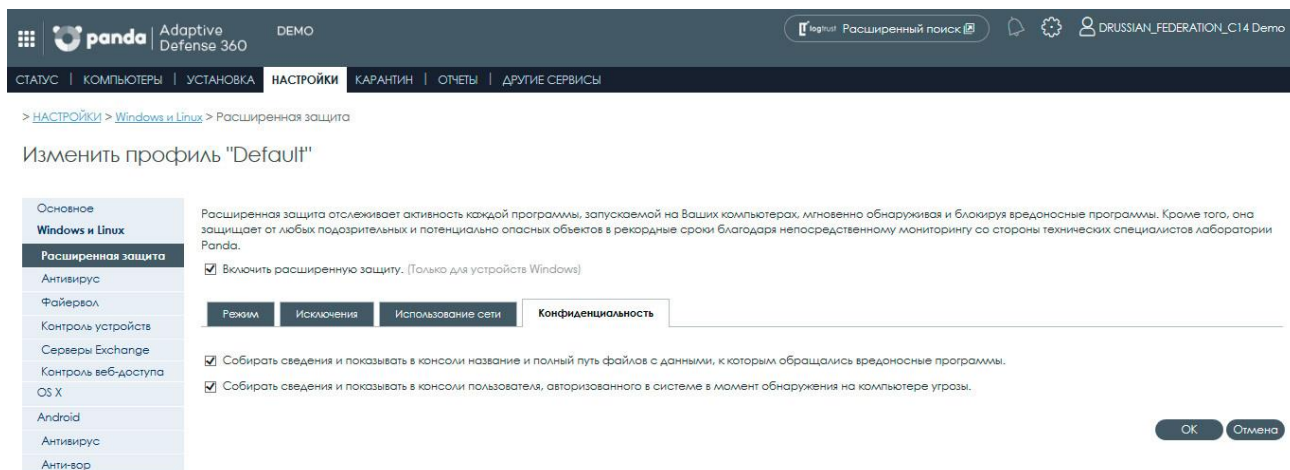


Рис. 3.10. Налаштування конфедційності розширеного захисту у системі
Adaptive Defense 360

На цьому налаштування розширеного захисту в цьому профілі закінчено. Приблизно через 15 хвилин усі настройки будуть синхронізовані та набудуть чинності. З цього моменту на тих комп'ютерах, які належать даному профілю, розширений захист працюватиме відповідно до ваших настройок.

Після того як налаштували опції розширеного захисту, давайте подивимося, як поводитиметься рішення залежно від сценарію. У таблиці нижче наведено номер сценарію для *Adaptive Defense* та *Adaptive Defense 360* залежно від режиму роботи та характеристики виявленого об'єкта, а нижче під таблицею вже представлені докладні описи кожного сценарію.

Adaptive Defense – спрощена версія продукту без перманентного захисту. Вона містить лише модуль розширеного захисту. Ця версія може працювати паралельно з будь-яким поточним корпоративним антивірусом, надаючи додатковий рівень захисту від невідомих загроз.

Adaptive Defense 360 – це повна версія продукту, яка, крім розширеного захисту, містить також і всі модулі перманентного захисту (антивірус, фаєрвол,

контроль пристроїв, *URL*-фільтрація, захист *Exchange* і т.д.).

За сценарієм 0, ніяких дій не вживається (лікування, видалення, блокування, ...).

Сповіщення:

– на комп'ютері кінцевого користувача не відображається жодних спливаючих вікон• Активність шкідливих програм та ПНП реєструється та відображається в консолі керування (панелі Шкідливі програми та Потенційно небажані програми);

– активність підозрілих та невідомих об'єктів не реєструється та не відображається в консолі керування (панель Заблоковані клас);

– якщо у розділі Параметри увімкнені та налаштовані поштові повідомлення, вони будуть надсилатися у разі виявлення шкідливих програм

За сценарієм 1, вживається дія блокування.

Сповіщення: після цього дані об'єкти не будуть реєструватися в панелі Заблоковані некласифіковані об'єкти, якщо у розділі Параметри увімкнені та налаштовані поштові повідомлення, вони будуть надсилатися у разі виявлення шкідливих програм та підозрілих об'єктів. Але вони не вирушатимуть у випадку з ПНП.

За сценарієм 2, вживається дія блокування та надсилання на карантин, лікування або видалення.

Сповіщення:

– на комп'ютері кінцевого користувача відображається спливаюче вікно з повідомленням

– активність шкідливих програм та ПНП реєструється та відображається в консолі управління (панелі Шкідливі програми та Потенційно небажані програми)• Активність підозрілих та невідомих об'єктів реєструється та показується у консолі управління (панель Заблоковані некласифіковані об'єкти). Після того, як ці об'єкти будуть класифіковані, вони реєструватися та відображатися у відповідній панелі (Шкідливі програми або Потенційно небажані програми), за винятком випадків, коли ці об'єкти в кінцевому

підсумку будуть класифіковані як нешкідливі програми (*goodware*). Після цього дані об'єкти не будуть реєструватися в панелі Заблоковані некласифіковані об'єкти;

– якщо у розділі Параметри увімкнені та налаштовані поштові повідомлення, то вони будуть відправлятися у разі виявлення шкідливих програм та підозрілих об'єктів. Але вони не вирушатимуть у випадку з ПНП.

За сценарієм 3, вживається блокування всіх невідомих об'єктів.

Сповіщення:

– на комп'ютері кінцевого користувача відображається спливаюче вікно з повідомленням. Після того, як ці об'єкти будуть класифіковані, вони будуть реєструватися і показуватись у відповідній панелі (Шкідливі програми або Потенційно небажані програми), за винятком випадків, коли ці об'єкти в кінцевому підсумку будуть класифіковані як нешкідливі програми (*goodware*). Після цього дані об'єкти не будуть більше реєструватися в панелі Заблоковані некласифіковані об'єкти;

– ніякі поштові повідомлення не надсилаються у разі виявлення невідомих об'єктів.

За сценарієм 4, вживається блокування всіх невідомих об'єктів, які відповідають логіці правил, встановлених для режиму розширеного захисту *Hardening*.

Сповіщення:

– на комп'ютері кінцевого користувача відображається спливаюче вікно з повідомленням. Після того, як ці об'єкти будуть класифіковані, вони будуть реєструватися і показуватись у відповідній панелі (Шкідливі програми або Потенційно небажані програми), за винятком випадків, коли ці об'єкти в кінцевому підсумку будуть класифіковані як нешкідливі програми (*goodware*). Після цього дані об'єкти не будуть більше реєструватися в панелі Заблоковані некласифіковані об'єкти

– ніякі поштові повідомлення не надсилаються у разі виявлення невідомих об'єктів.

Висновки за розділом

Пасивні реакції при наявності вторгнень переважають у сфері рішень безпеки для IAS через побоювання, що реактивні реакції можуть негативно вплинути на роботу системи автоматизації. Це часто вимагає, щоб будь-які реактивні контрзаходи були здійснені людиною, що призводить до затримки відповідей. Це збільшує вразливість системи та створює вікно можливостей для успішного вторгнення і, отже, негативного впливу на систему.

Adaptive Defense 360 пропонує автоматизований розширений захист від невідомих загроз, APT, спрямованих атак, шифрувальників та інших загроз нульового дня. Цей захист, використовуючи всю міць хмарних великих даних та штучного інтелекту, дозволяє аналізувати кожен процес безпосередньо в контексті всього «великого процесу», що дозволяє більш точно розуміти його характер та кінцеві цілі. А це, у свою чергу, дозволяє більш точно класифікувати кожен програму та процес, забезпечуючи високий рівень захисту від невідомих загроз.

ВИСНОВКИ

В дипломній роботі було досліджено методики захисту передачі інформації в локальній мережі

Концепція системи реактивного захисту забезпечує гнучкість, щоб інтегрувати нові політики та реактивні дії. Його також можна адаптувати для роботи з іншими рішеннями безпеки, які є в *IAS*, щоб розширити ці функції. Ця гнучкість і адаптивність дозволяють автоматично виконувати реактивні дії.

На жаль, важливо мати на увазі, що автоматичне виконання реактивних дій, передбачене цією концепцією, пов'язане з компромісом між настроюваністю та автоматизацією реактивних дій. Це означає, що чим детальніша конфігурація системи, тим ефективніше її автоматичне реагування. Хоча це вимагає великих зусиль перед розгортанням системи, важливо враховувати, що *IAS* має тривалий термін служби, і, отже, їх реконфігурація та обслуговування відбувається нечасто. Аналіз і вибір цього компромісу слід виконувати між системними інтеграторами та експертами з безпеки, щоб знайти відповідний баланс.

Для того щоб довести доцільність представленої концепції, виконання вимог було висунуто чотири гіпотези. Далі представлені ці гіпотези. Умови, необхідні для задоволення експлуатаційних вимог (висока продуктивність, доступність і можливості в режимі реального часу) системи автоматизації, можна визначити як операційну політику.

У другому розділі було проаналізовано технології реактивного захисту *EDR* та *XDR*.

XDR повинен будуватися на сильному *EDR*, який сам по собі в рамках кінцевих точок повинен охоплювати велику кількість джерел даних: ПК, ноутбуки, віртуальні машини, мобільні пристрої плюс різні операційні системи (*Windows*, *Linux*, *MacOS*, *Android*, *iOS*, ін.).

XDR не те ж саме, що *EDR*. *XDR* базується на розширенні технології *EDR*.

Літера “X” на початку скороченого варіанта назви “XDR” означає кількість джерел/продуктів, що підключаються, які беруть участь у процесі виявлення, розслідування та реагування. Кількість «X», що підключаються, залежить від потреб замовника, від вже впроваджених рішень від одного вендора, а також від обраного постачальника XDR, тобто від його підтримуваних джерел (класів продуктів).

Політику часто називають правилами, умовами чи обмеженнями, які необхідно дотримуватися. Отже, операційні вимоги також можна визначити як політику. У представленій концепції ці операційні політики були визначені шляхом визначення критичних активів, які становлять систему автоматизації. На основі цих активів була отримана класифікація операційної політики. Такий висновок був досягнутий шляхом аналізу випадків або умов, пов’язаних із цими критично важливими активами, у яких можуть негативно вплинути основні операційні вимоги IAS (тобто висока продуктивність, доступність та можливості реального часу). Кожен із класів, визначених у цій класифікації, детально описує інформацію, яку можуть містити такі політики. Крім того, наведено кілька прикладів (розділ 3).

Застосовність цих політик оцінювалася за вищезгаданим сценарієм. Крім того, виводячи ці політики з критичних активів, пов’язаних з операційними вимогами в IAS, гарантується, що, враховуючи ці політики, ці вимоги будуть виконані, а отже виконання R3, визначеного в другому розділі. Отже, гіпотеза про те, що експлуатаційні вимоги системи автоматизації можна визначити як операційну політику, може бути визначена як вірна.

У цій роботі представлена концепція системи, яка дозволяє реактивно й автоматично реагувати на вторгнення. Ця концепція вирішує вищезгадані проблеми, що призводить до підходящої та здійсненої альтернативи реактивного захисту для IAS.

Ця концепція вперше була розроблена шляхом визначення чотирьох вимог, пов’язаних з рішеннями для запобігання вторгненням та іншими архітектурними тенденціями та тенденціями безпеки для промислових систем.

З цих вимог було закладено основу для представленої концепції. Ця основа складається з безпеки та операційної політики, а також реактивних дій, які потенційно можуть протидіяти вторгненням.

Система, що є результатом цієї концепції, здатна аналізувати події безпеки, отримані від інших компонентів системи (наприклад, сторонніх рішень безпеки). Ці події аналізуються з метою виявлення порушень політики безпеки. Після виявлення порушення політики вибирається відповідна реакція. Перед виконанням або ініціюванням такої дії операційні політики перевіряються. Це гарантує, що виконуються лише реактивні дії, які не порушують операційну політику базової системи автоматизації. Це означає, що до тих пір, поки визначена політика безпеки та операційна політика представляє справжні вимоги та обмеження системи автоматизації, реактивні дії не матимуть на неї негативного впливу. Крім того, Важливо підкреслити, що обсяг захисту, передбачений представленою концепцією, дозволяє захистити систему автоматизації та її компоненти на рівні сегмента мережі. Це відповідає сучасним тенденціям архітектури та безпеки IAS. Крім того, представлена концепція передбачала вказівки, яким можна слідувати, щоб визначити політики безпеки, реактивні дії та компоненти для виконання цих дій.

Застосування цих вказівок і концепції було проілюстровано за допомогою еталонної архітектури та програми IAS, а також набору прикладів політики безпеки та реактивних дій, які підкреслили потенціал представленої концепції. Крім того, оцінка представленої концепції була проведена наступним чином. Спочатку була впроваджена прототипна система реактивного захисту. Щоб перевірити його доцільність та застосовність, було визначено реальний сценарій, на основі якого були отримані варіанти використання. Ці сценарії використання були емульовані за допомогою тестової установки, де був розгорнутий прототип. Після цього, щоб додатково підтвердити оцінку доцільності, було виведено та доведено чотири гіпотези. Результати цих оцінок показали, що представлена концепція є придатною та здійсненою для IAS.

Майбутня робота буде зосереджена на вдосконаленні прототипної

реалізації. Це включає розширення можливостей, дозволяючи віддалену конфігурацію системи реактивного захисту та збагачуючи базу знань політик безпеки та операційної політики.

Іншим важливим аспектом є подальше покращення сумісності з іншими рішеннями безпеки, що дозволить додати підтримку більш реактивних дій захисту (наприклад, додати нові правила брандмауера). Крім того, будуть досліджені альтернативи для покращення зручності використання конфігурації для безпеки та операційної політики.

На даний момент конфігурація політики безпеки та операційної політики повинна виконуватися вручну людиною-оператором, що володіє знаннями щодо роботи системи автоматизації та її безпеки. Хоча це може вимагати значних зусиль щодо конфігурації (залежно від складності системи та її політик), представлена концепція забезпечує можливу та відповідну альтернативу для активного захисту від вторгнень. Компроміс між зусиллями щодо конфігурації та автоматичним захистом слід додатково обговорити між зацікавленими сторонами системи.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Weyer, S.; Schmitt, M.; Ohmer, M.; Gorecky, D. *Towards Industry 4.0-Standardization as the crucial challenge for highly modular, multi-vendor production systems. IFAC-PapersOnLine* 2015, 48, 579-584.
2. Koutepas, G.; Giannopoulos, G.; Mitsiara, A. *Cyber Security Trends and Their Implications in ICS: Mid-Year Report 2016*. Available online: <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC103512/lbna28187enn.pdf> (accessed on 22 September 2018).
3. Kaspersky Lab ICS CERT. *Threat Landscape for Industrial Automation Systems: H1 2018*. Available online: https://ics-cert.kaspersky.com/media/H1_2018_ICS_REPORT_ENG.pdf (accessed on 1 October 2018).
4. *Security Requirements for Cryptographic Modules: FIPS PUB 140-2: Federal Information Processing Standards Publication*. 2001. Available online: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf> (accessed on 1 October 2018).
5. Schneider, F.B. *Enforceable security policies*. *ACM Trans. Inf. Syst. Secur.* 2000, 3, 30-50. [Green Version]
6. Kissel, R. *Glossary of Key Information Security Terms: NISTIR 7298*; Diane Publishing: Collingdale, PA, USA, 2011. [Google Scholar]
7. Scarfone, K.; Mell, P. *Intrusion Detection and Prevention Systems*. In *Handbook of Information and Communication Security*; Stavroulakis, P., Stamp, M., Eds.; Springer Berlin Heidelberg: Berlin/Heidelberg, Germany, 2010; pp. 177-192. [Google Scholar]
8. Karnouskos, S.; Colombo, A.W.; Bangemann, T. *Trends and Challenges for Cloud-Based Industrial Cyber-Physical Systems*. In *Industrial Cloud-Based Cyber-Physical Systems: The IMC-AESOP Approach*; Colombo, A.W., Bangemann, T.,

Karnouskos, S., Delsing, J., Stluka, P., Harrison, R., Jammes, F., Lastra, J.L., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 231-240. [Google Scholar]

9. Jazdi, N. Cyber physical systems in the context of Industry 4.0. In *Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR)*, Cluj-Napoca, Romania, 22-24 May 2014; pp. 1-4.

10. Karnouskos, S. Stuxnet Worm Impact on Industrial Cyber-Physical System Security. In *Proceedings of the IECON 2011-37th Annual Conference of IEEE Industrial Electronics*, Melbourne, Australia, 7-10 November 2011; pp. 4490-4494.

11. Nasser, M.; Ahmad, R.; Yassin, W.; Hassan, A.; Zainal, Z.; Salih, N.; Hameed, K. Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems. *Int. J. Adv. Comput. Sci. Appl.* 2018, 9. [Green Version]

12. Yang, Y.; McLaughlin, K.; Sezer, S.; Littler, T.; Im, E.G.; Pranggono, B.; Wang, H.F. Multiattribute SCADA-Specific Intrusion Detection System for Power Networks. *IEEE Trans. Power Deliv.* 2014, 29, 1092-1102. [Green Version]

13. Kim, B.K.; Kang, D.H.; Na, J.C.; Chung, T.M. Abnormal traffic filtering mechanism for protecting ICS networks. In *Proceedings of the 2016 18th International Conference on Advanced Communication Technology (ICACT)*, Pyeongchang, Korea, 31 January-3 February 2016; pp. 436-440.

14. Y?ksel, ?.; den Hartog, J.; Etalle, S. Reading Between the Fields: Practical, Effective Intrusion Detection for Industrial Control Systems. In *Proceedings of the 31st Annual ACM Symposium on Applied Computing*, Pisa, Italy, 4-8 April 2016; Ossowski, S., Ed.; ACM: New York, NY, USA, 2016; pp. 2063-2070.

15. ICS CERT. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. Available online: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf (accessed on 12 November 2018).

16. Sauter, T.; Soucek, S.; Kastner, W.; Dietrich, D. The Evolution of Factory

and Building Automation. IEEE Ind. Electron. Mag. 2011, 5, 35-48.

17. Scholten, B. *The Road to Integration: A Guide to Applying the ISA-95 Standard in Manufacturing*; ISA: Research Triangle Park, NC, USA, 2007. [Google Scholar]

18. Ab Rahman, N.H.; Choo, K.K.R. A survey of information security incident handling in the cloud. *Comput. Secur.* 2015, 49, 45-69.

19. Schneider Electric. *Industrial Defender: Security, Compliance, and Change Management Solution*. Available online: <https://www.schneider-electric.com/en/product-range-download/61675-industrial-defender/> (accessed on 29 November 2018).

20. Stouffer, K.; Falco, J.; Scarfone, K. *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC): Recommendations of the National Institute of Standards and Technology, Computer Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011. [Google Scholar]

21. Stouffer, K.K.; Falco, J. *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*; Department of Homeland Security, Control systems security Program, National Cyber Security Division: Washington, DC, USA, 2016. [Google Scholar]

22. Foo, B.; Glause, M.W.; Howard, G.M.; Wu, Y.S.; Bagchi, S.; Spafford, E.H. *Intrusion Response Systems: A Survey*. In *Information Assurance*; Qian, Y., Ed.; The Morgan Kaufmann Series in Computer Security; Elsevier: Amsterdam, The Netherlands; Morgan Kaufmann: Boston, MA, USA, 2008; pp. 377-412. [Google Scholar]

23. Piggin, R. *Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security*. In *Proceedings of the IET Conference on Control and Automation 2013: Uniting Problems and Solutions*,

Birmingham, UK, 4-5 June 2013; pp. 1-6.

24. Knowles, W.; Such, J.M.; Gouglidis, A.; Misra, G.; Rashid, A. Assurance Techniques for Industrial Control Systems (ICS). In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy*, Denver, CO, USA, 16 October 2015; Ray, I., Thomas, R., Cardenas, A.A., Eds.; ACM: New York, NY, USA, 2015; pp. 101-112. [Green Version]

25. Garitano, I.; Uribeetxeberria, R.; Zurutuza, U. A Review of SCADA Anomaly Detection Systems. In *Soft Computing Models in Industrial and Environmental Applications*, 6th International Conference SOCO 2011; Corchado, E., Snasel, V., Sedano, J., Hassanien, A.E., Calvo, J.L., Slezak, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 357-366. [Google Scholar]

26. Zhu, B.; Sastry, S. SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy. In *Proceedings of the 1st Workshop on Secure Control Systems (SCS)*, Stockholm, Sweden, 12 April 2010; Volume 11, p. 7. [Google Scholar]

27. Kagermann, H. Change Through Digitization-Value Creation in the Age of Industry 4.0. In *Management of Permanent Change*; Albach, H., Meffert, H., Pinkwart, A., Reichwald, R., Eds.; Springer Fachmedien: Wiesbaden, Germany, 2015; pp. 23-45. [Google Scholar]

28. Blowers, M.; Iribarne, J.; Colbert, E.J.M.; Kott, A. In Conclusion: The Future Internet of Things and Security of Its Control Systems. In *Cyber-security of SCADA and Other Industrial Control Systems*; Colbert, E.J.M., Kott, A., Eds.; Springer International Publishing: Cham, Switzerland, 2016; pp. 323-355. [Google Scholar]

29. Mitchell, R.; Chen, I.R. A Survey of Intrusion Detection Techniques for Cyber-Physical Systems. *ACM Comput. Surv.* 2014, 46, 1-29.

30. Goldenberg, N.; Wool, A. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. *Int. J. Crit. Infrastruct. Prot.* 2013, 6, 63-75.

31. Cruz, T.; Maglaras, L.A.; Jiang, J. Integrated OCSVM mechanism for intrusion detection in SCADA systems. *Electron. Lett.* 2014, 50, 1935-1936.

32. Maglaras, L.A.; Jiang, J. *Intrusion detection in SCADA systems using Machine Learning Techniques*. In *Proceedings of the 2014 Science and Information Conference (SAI)*, London, UK, 27-29 August 2014; pp. 626-631.

33. Ponomarev, S.; Atkison, T. *Industrial Control System Network Intrusion Detection by Telemetry Analysis*. *IEEE Trans. Dependable Secur. Comput.* 2016, 13, 252-260.

34. Nurjahan; Nizam, F.; Chaki, S.; Al Mamun, S.; Kaiser, M.S. *Attack detection and prevention in the Cyber Physical System*. In *Proceedings of the 2016 International Conference on Computer Communication and Informatics, Coimbatore, India*, 7-9 January 2016; pp. 1-6.

35. *Security Matters. Phoenix Contact's mGuard Integration with Silent Defense*. Available online: https://www.secmatters.com/hubfs/Security_Matters-March2017/PDF/Solution-Brief-SecurityMatters-and-Phoenix-Contact.pdf (accessed on 1 October 2018).

36. ДСТУ 3008-95. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення. – 39 с.

37. Комп'ютерна інженерія: методичні рекомендації до виконання дипломних проектів для студентів освітньо-дипломного рівня “Бакалавр” напрямку підготовки 6.050102 “Комп'ютерна інженерія” / Уклад.: І.А. Жуков, М.М. Проценко – К.: НАУ, 2015. – 36 с.

38. Юдін О.К. *Захист інформації в мережах передачі даних* / О.К. Юдін, Г.Ф. Конахович, О.Г. Корченко / Підручник МОН України. – К.: Видавництво *DIRECTLINE*, 2009. – 714 с.