МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри Комп'ютеризованих систем захисту інформації

_____ Михайло СТЕПАНОВ
«____»_____ 2023 р.

На правах рукопису
УДК 004.056.5:510.22(043.3)

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Комбінований метод виявлення кібератак на інформаційні системи

Виконавець:	Олександр КОЛЬЧИК
Керівник: к.т.н., доцент	Сергій ТОЛЮПА
Консультант розділу «Охорона навколишнього середовища»: к.т.н., доцент	Тетяна ДМИТРУХА
Нормоконтролер: к.т.н., доцент	Сергій ТОЛЮПА

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Магістр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри Комп'ютеризованих систем захисту інформації

_____ Михайло СТЕПАНОВ
«___» _____ 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
здобувача вищої освіти Кольчика Олександра Олеговича

1. Тема: *Комбінований метод виявлення кібератак на інформаційні системи* затверджена наказом ректора від «__» _____ 20__ № _____/ст.
2. Термін виконання з __.__.20__р. по __.__.20__р.
3. Вихідні дані: стандарти аналізу ризиків, NIST, методологія Azure та ISO 2700х); метод пошуку максимальної кількості індикаторів компрометації (IoC); моделі APT-атаки та модель поведінки BD;
4. Зміст пояснювальної записки: загальна характеристика сутності сучасних кібератак; методологія аналізу джерел індикаторів компрометації з метою виявлення кібератак на інформаційну систему; практична реалізація методу та оцінка ефективності.

.

КАЛЕНДАРНИЙ ПЛАН

виконання кваліфікаційної роботи

№ з/п	Етапи виконання кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	16.10.2023	*Виконано*
2.	Аналіз літературних джерел	19.10.2023	*Виконано*
3.	Обґрунтування вибору рішення	22.10.2023	*Виконано*
4.	Збір інформації	25.10.2023	*Виконано*
5.	Загальна характеристика сутності сучасних кібератак	26.10.2023	*Виконано*
6.	Методологія аналізу джерел індикаторів компрометації з метою виявлення кібератак на інформаційну систему	07.11.2023	*Виконано*
7.	Практична реалізація методу та оцінка ефективності	20.11.2023	*Виконано*
8.	Апробація роботи	29.11.2023	*Виконано*
9.	Перевірка на антиплагіат	15.12.2023	*Виконано*
10.	Оформлення і друк пояснювальної записки	20.12.2023	*Виконано*
11.	Оформлення презентації	20.12.2023	*Виконано*
12.	Отримання рецензій від рецензента	22.12.2023	*Виконано*

Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона навколишнього середовища	Дмитруха Т.І.		

7. Дата видачі завдання: «16» жовтня 2023 р.

Здобувач вищої освіти Олександр КОЛЬЧИК
(підпис, дата)

Керівник кваліфікаційної роботи Сергій ТОЛЮПА
(підпис, дата)

Реферат

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків і має 115 сторінок основного тексту, 19 рисунків, 21 таблиць, 6 сторінок додатків. Список використаних джерел містить 60 найменувань. Загальний обсяг роботи 122 сторінки.

Мета роботи – підвищення ефективності виявлення кібератак на основі використання методу індикаторів компрометації.

В кваліфікаційній роботі описано основні підходи сучасних науковців та законодавчих органів до тлумачення поняття «кіберрозвідка» та «кібератака». Описано головні етапи проведення кіберрозвідки та кібератаки та вказано умови автоматизації процесу. Детально розглянуто такі комерційні платформи для комерційної кіберрозвідки, як Anomali ThreatStream, Anomali Enterprise, ThreatConnect, TC Identify, TC Manage, TC Analyze, ThreatConnect CAL, TC Complete, ThreatQ та дано їх переваги перед конкурентами.

Окремо дана характеристика методу виявлення кібератак на основі пошуку індикаторів компрометації (IoC) та їх розповсюдження. Зроблено опис розробленого методу аналізу APT. Представлено виявлені індикатори технік MITRE, які призначені для першого етапу методу – фільтрації подій та зменшення їх кількості шляхом пошуку застосування технік у подіях.

В практичній частині дослідження зроблено визначення особливостей APT-атак та мети досліджень. Для запропонованого методу проведено практичну реалізацію та результат представлено у графічному вигляді. Використано скорингову систему до даних, зібраних про шкідливе програмне забезпечення Regin, для якого було виявлено 33 хеші та 17 false positive хешів. Побудовано візуалізацію оцінки індикатора компрометації.

Ключові слова: кібератака, кіберрозвідка, інформаційна система, Anomali ThreatStream, Anomali Enterprise, ThreatConnect, TC Identify, TC Manage, TC Analyze, ThreatConnect CAL, APT-атаки, індикатори компрометації.

ЗМІСТ

ВСТУП 8

Розділ 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА СУТНОСТІ СУЧАСНИХ КІБЕРАТАК 11

1.1. Основні підходи науковців до трактування понять кібератак та кіберрозвідки 11

1.2. Сучасна класифікація типів кібератак та кіберрозвідки 25

1.3. Аналіз моделей та методів захисту кіберпростору (стандарти аналізу ризиків, NIST, методологія Azure та ISO 2700x) 28

1.4. Характеристика методу пошуку максимальної кількості індикаторів компрометації (IoC) в контексті виявлення кібератак на інформаційну систему 63

Розділ 2. МЕТОДОЛОГІЯ АНАЛІЗУ ДЖЕРЕЛ ІНДИКАТОРІВ КОМПРОМЕТАЦІЇ З МЕТОЮ ВИЯВЛЕННЯ КІБЕРАТАК НА ІНФОРМАЦІЙНУ СИСТЕМУ 68

2.1. Опис розробленого методу аналізу APT 68

2.2. Етап фільтрації подій та опис індикаторів технік для фільтрації подій 73

2.3. Програмна реалізація етапів розробленого методу 95

Розділ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДУ ТА ОЦІНКА ЕФЕКТИВНОСТІ 105

3.1. Визначення особливостей APT-атак та мети досліджень 105

3.2. Вибір моделі APT-атаки та розробка моделі поведінки BD 107

3.3. Визначення відповідності процедур управління в рамках BD та елементарних подій ITS 118

РОЗДІЛ 4. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА……104

ВИСНОВКИ 128

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 131

Додаток А. Алгоритм реалізації кібератаки 137

Додаток Б. Головні підходи до здійснення кіберрозвідки 137

Додаток В. Основні загрози інформаційної безпеки 138

Додаток Г Робоче вікно ThreatConnect: Playbook 138

Додаток Д. Робоче вікно ThreatConnect: Dashboard 139

Додаток Е. Робоче вікно ThreatQ Self-Tuning: налаштування..... 140

Додаток Ж. Робоче вікно ThreatQ: архітектурне рішення 141

Додаток З. Етапи створення комплексної системи захисту інформації... 141

Додаток И. Фрагмент програмного коду реалізованого методу 142

ВСТУП

Актуальність дослідження. Останніми роками все більшу занепокоєність уряду України та провідних країн світу викликає збільшення та поширення фактів кібершпіонажу. Так, у минулорічному докладі керівника Управління національної контррозвідки США звинувачуються, зокрема росія у зборі інформації, а Китай безпосередньо у промисловому та економічному шпигунстві, що здійснюються за допомогою комп'ютерних технологій [1].

Інфраструктуру необхідно завжди перевіряти на наявність шкідливого програмного забезпечення. Оскільки постійно з'являються нові методи і тактики для атак, щодня стає все важче шукати нові вразливості та виявляти скомпрометовані ресурси. Для даної цілі індикатори компрометації є одним з найбільш ефективних інструментів, які може використовувати експерт з кібернетичної безпеки. Це зумовлено їх високою швидкістю розповсюдження та можливістю легко додавати до своєї архітектури, що займається забезпеченням безпеки інфраструктури [2].

Невід'ємною частиною процесу управління інформаційною безпекою є оцінка ризиків, для чого використовуються різні методи та засоби. Незалежно від сфери діяльності, оцінка ризиків кібербезпеки представляє собою впорядкований процес, що складається з етапів, на кожному з яких можуть застосовуватись свої методи та засоби. При виборі методів та засобів слід приділяти увагу не результативності методів в цілому, а їх ефективності на певному етапі, можливості поєднання, засобам переходу від одного методу до іншого для досягнення якомога коректнішого результату [10].

Ризики кібербезпеки є невід'ємною частиною інформаційної діяльності, що можуть відбуватися в інформаційній, соціальній, технічній інфраструктурі держави, організації чи в інформаційно-комунікаційних мережах, впливаючи на стан державних інформаційних ресурсів і національну безпеку. Представлене дослідження стосується аналізу моделі ідентифікації ризиків кібербезпеки в розподілених інформаційних системах.

Аналіз останніх досліджень і публікацій засвідчує, що питанням використання методу виявлення кібератак на основі індикаторів компрометації у своїх роботах займалися такі науковці, як Гайдур Г. І. [7], Шлапаченко В. М. [43], Платоненко А. В. [26], Куцаєв В. [19], Федорченко А. В. [39], Твердохліб І. [34].

Мета роботи – підвищення ефективності виявлення кібератак на основі використання методу індикаторів компрометації.

Об'єктом дослідження є процес виявлення кібератак в інформаційних системах.

Предмет дослідження: методи систем виявлення вторгнень в інформаційні системи.

Завдання дослідження можна сформулювати так:

- описати основні підходи науковців до трактування поняття «кіберрозвідка» та «кібератака»;
- проаналізувати сучасну класифікацію типів кіберрозвідки та кібератак та дослідити моделі та методи захисту кіберпростору (стандарти аналізу ризиків, NIST, методологія Azure та ISO 2700x);
- дати характеристику методу пошуку максимальної кількості індикаторів компрометації (IoC) та їх розповсюдження;
- провести опис розробленого методу аналізу APT та перелічити етапи фільтрації подій;
- навести програмну реалізацію етапів розробленого методу;
- здійснити вибір моделі APT-атаки та розробку моделі поведінки BD.

Методи дослідження в роботі використані такі: пошуковий по наявній методичній та науковій літературі із аналізом знайденого матеріалу, порівняння, класифікація, проєктування, теоретичне моделювання, з'ясування причинно-наслідкових зв'язків, аналіз документації та результатів діяльності дослідників з проблеми проведеного дослідження.

В роботі також використано такі методи: аналітичний – використання математичного апарату при обробці фактичного матеріалу; логічний метод використовується в процесі всього дослідження, в т.ч. дедукція, класифікація матеріалу, конструювання робочої гіпотези, постановка та шляхи вирішення проблеми; метод відносних величин – при оцінці темпів зростання-зниження динамічного процесу; графічний метод – при побудові графіків, діаграм, гістограм; загальнонаукові методи пізнання, такі як індукція, порівняння, узагальнення, зіставлення.

Новизна одержаних результатів полягає в наступному: автором систематизовано інформацію по напрямку дослідження, на основі чого розроблено методу виявлення кібератак в інформаційній системі на основі індикаторів компрометації.

Джерелами інформації для вирішення перерахованих вище завдань є збірники наукових праць, монографії, періодична література, підручники і довідники.

Теоретична та практична цінність роботи полягає в наявності авторського матеріалу по напрямку розробки методу виявлення кібератак в інформаційній системі. Метод описано на основі індикаторів компрометації. Проведене дослідження має більш глибокий ступінь розробки напрямку дослідження, відносно попередніх досліджень вчених, дисертантів та дослідників напрямку дослідження.

Апробація. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

Сергій Толюпа, Олександр Кольчик. УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЙНИХ РЕСУРСІВ В УМОВАХ ВПЛИВУ КІБЕРАТАК. Збірник матеріалів доповідей та тез VI міжнародної науково-практичнної конференції «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» м. Київ, 27 квітня 2023 року. – К.: ВПЦ "Київський університет", 2023. – С. 47-48.

Розділ 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА СУТНОСТІ СУЧАСНИХ КІБЕРАТАК

1.1. Основні підходи науковців до трактування понять кібератак та кіберрозвідки

Кібератаки в інформаційних системах — це спрямовані дії, які мають на меті порушити нормальну роботу, красти дані або завдати шкоди комп'ютерним системам, мережам та іншій цифровій інфраструктурі. Ось деякі з основних типів кібератак та їх специфіка:

1. Віруси та Шкідливе ПЗ (малвар): Це програми, які можуть самостійно поширюватися, інфікуючи файли та системи. Вони можуть викрадати дані, завдавати шкоди файлам або навіть заблокувати доступ до даних (наприклад, через вимогу викупу в рансомвар атаках).
2. Фішинг: Це тактика обману, при якій зловмисники намагаються отримати конфіденційну інформацію (наприклад, паролі та дані банківських карток) від нічого не підозрюючих користувачів. Вони часто використовують підроблені електронні листи та веб-сайти, що імітують законні ресурси.
3. DDoS-атаки (Distributed Denial of Service): Це атаки, які перевантажують мережеві ресурси (наприклад, сервери), забезпечуючи масовий доступ до них з різних точок, що призводить до їх відмови.
4. Man-in-the-Middle (MitM) Атаки: При цьому типі атаки зловмисник перехоплює комунікацію між двома сторонами для перехоплення або підробки інформації.
5. SQL Injection: Це техніка, за допомогою якої зловмисник може впроваджувати шкідливі SQL запити через веб-форми, з метою маніпуляції базами даних.
6. Злом паролів: Це включає в себе методи вгадування або вираховування паролів користувачів для отримання несанкціонованого доступу до систем.

7. Експлойти "нульового дня": Це використання вразливостей в програмному забезпеченні, які ще не виявлені або не виправлені розробниками.

Кожен з цих типів кібератак має свою специфіку та методи боротьби з ними. Захист від таких атак часто включає в себе комбінацію технічних засобів (наприклад, антивірусне програмне забезпечення, фаєрволи) та освітніх заходів (наприклад, навчання персоналу).

Кіберрозвідка тісно пов'язана з кібератаками, оскільки вона включає в себе процес збору інформації про цілі атак, їхні вразливості, а також методи та інструменти, які можуть бути використані для проведення таких атак. Кіберрозвідка забезпечує зловмисникам необхідні дані для планування та виконання ефективних кібератак, дозволяючи їм ідентифікувати слабкі точки у захисті та визначати потенційні цілі для втручання. Це може включати моніторинг мережевого трафіку, аналіз звітів про безпеку та вивчення останніх тенденцій у сфері кібербезпеки, щоб адаптуватися до сучасних захисних стратегій. Таким чином, кіберрозвідка відіграє ключову роль у розвитку та реалізації кібератак.

Кіберрозвідка – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням [23, с. 24–31].

Кібершпигунство або комп’ютерне шпигунство (також використовується термін «кіберрозвідка») — це термін, який, як правило, означає несанкціоноване отримання інформації з метою отримання особистої, економічної, політичної чи військової вигоди, яка здійснюється шляхом обходу (злому) систем комп’ютерної безпеки.Використовуючи шкідливе програмне забезпечення, включаючи троянські та шпигунські програми. Кібершпигунство може здійснюватися дистанційно, за допомогою Інтернету, а також шляхом проникнення в комп’ютери та корпоративні комп’ютерні мережі звичайними шпигунами («кротами»), а також хакерами. Останнім часом до кібершпигунства також відноситься аналіз, який проводять провідні спецслужби (ЦРУ, Моссад, ФСБ), зокрема моніторинг цифрових слідів поведінки користувачів соціальних

мереж (повідомлення, друзі, фото, відео тощо), таких як Фейсбук і ВКонтакте. Twitter тощо, з метою виявлення екстремістської, терористичної чи антиурядової діяльності, заклики до зборів проти влади [23].

У кібершпигунстві для отримання такої інформації використовуються найпередовіші сучасні технології. Сьогодні арсенал кібершпигунства використовує велику кількість методів для здійснення своєї діяльності.

Наприклад, державні служби Японії та США спеціально співпрацюють із розробниками додатку для смартфонів Pokemon Go, щоб дізнатися більше про військові та секретні об’єкти в різних країнах, адже присутність покемонів змушуватиме користувачів робити фотографії в таких місцях. Niantic відкинув звинувачення в тому, що гра може бути інструментом розвідки, і закликав усіх користувачів дотримуватися місцевих законів і поважати місця, які вони відвідують, і людей, яких вони зустрічають.

Хамді Бахіт, член Комітету з питань оборони та національної безпеки Єгипту, заявив перед парламентом, що гра Pokemon Go є найновішим інструментом, який використовують шпигунські мережі у війнах, і це підступна програма, яка намагається проникнути з метою розвідки. Індонезійські чиновники описують гру як загрозу національній безпеці, оскільки вона може дозволити ворогам проникнути на секретні об’єкти та отримати доступ до секретних матеріалів.

Ізраїльська армія заборонила своїм солдатам використовувати гру "Pokemon Go" на військових базах. Оскільки влада Південної Кореї раніше заборонила Google Maps, вважаючи це загрозою національній безпеці, тут не зможе працювати Pokemon Go, який використовує звідти дані. Однак гра несподівано почала працювати в маленькому містечку Сокчо, що пояснює, чому була помилка в частині карти програми, і вона була помилково спрямована на територію, що містить Північну Корею [35].

Потенційним об’єктом терористичних актів, у тому числі з використанням сучасних інформаційних технологій, може стати ряд місцевих установ,

порушення роботи яких може становити загрозу життю та здоров'ю громадян. Не менш загрозливим є вчинення протиправних дій за рахунок третіх країн з використанням місцевої інформаційної інфраструктури, що загрожує стабільному та безпечному функціонуванню національних інформаційно-комунікаційних систем. Інформація обмеженого доступу, що циркулює в національних інформаційних ресурсах, є постійним предметом інтересу країн, організацій та інших осіб.

Крім того, все більшого поширення набула політично мотивована діяльність у кіберпросторі груп активістів (хакерів-активістів), які здійснюють атаки на державні та приватні сайти, що призводить до порушення роботи інформаційних ресурсів, а також до репутаційних і матеріальних втрат [31]. Одним із основних напрямів забезпечення кібербезпеки в Україні є посилення боротьби з кібертероризмом та кібершпигунством, захист важливих об'єктів національної інформаційної інфраструктури від їх проявів [36]. Як йдеться у Стратегії кібербезпеки України, її метою є створення умов для безпечного функціонування кіберпростору та його використання на благо особи, суспільства та держави.

Для досягнення цієї мети необхідними є:

- створення національної системи кібербезпеки;
- посилення спроможностей суб'єктів системи національної безпеки в рамках реалізації державної політики кібербезпеки, в тому числі профілактики кіберзагроз у найбільш важливих сферах життєдіяльності (передусім кібершпигунства, кібертероризму та кіберзлочинності) поглиблення відповідно до національних інтересів України та згідно з чинним законодавством України міжнародного співробітництва, у тому числі із транснаціональними корпораціями та недержавними організаціями у сфері кібербезпекової політики.

Зазначимо, що на Службу безпеки України покладено попередження, виявлення, припинення та викриття злочинів проти миру та безпеки людства, що

вчиняються у кіберпросторі; Здійснювати практичні контррозвідувальні та слідчі заходи, спрямовані на протидію кібертероризму та кібершпигунству [40]. Проте ми переконані, що наразі жоден спеціальний правоохоронний орган не в змозі самостійно та, тим більше, без участі громадських організацій забезпечити належний рівень кібербезпеки; Тому є нагальна потреба у формуванні системи правового регулювання державної політики кібербезпеки в Україні.

Cyber threat hunting - це пошук загроз всередині мережі: аналіз можливих доказів атаки відомих і невідомих вірусів, пошук слідів діяльності кіберзлочинних угруповань, а також пошук ознак зараження, в тому числі на більш глибокому рівні, наприклад, у прошивках («прошивках») пристроїв, а також у повідомленнях від сторонніх компаній (перевірка ознак атак із захищених компанією IP-адрес).

Розвідка про кіберзагрози (Cyber Intelligence) — це пошук інформації про потенційних зловмисників, у тому числі про серйозні кіберзлочинні групи, які називаються групами APT, передової постійної загрози (Advanced Persistent Threat або, коротше, цілеспрямована кібератака). Ці групи APT по суті являють собою стабільне співтовариство кіберзлочинців, де ролі та відповідальність зловмисників чітко розподілені: є організатори, є програмісти, спеціалісти в області соціальної інженерії, є краплі, які займаються переказом виведених коштів, є є навіть власна технічна підтримка.

Джерело: https: // www. anti-malwaree. com / practice / methods / threat-intelligence-platform [60]

Рис. 1.1. Класифікація Threat Intelligence за впливом на рівень прийняття рішень

Як видно з рис. 1.1, рішення тісно взаємопов'язані між собою і кожне попереднє впливає на подальше. Стратегічний рівень більшою мірою пов'язаний з рішеннями, прийнятими керівництвом. На даному рівні розглядаються звіти, що надаються підрозділом інформаційної безпеки, формуються цілі і стратегії, а також нові завдання і потреби (люди, процеси та інструменти). На рівні тактичних рішень необхідно оперувати тактиками, техніками і процедурами (TTP), які можна отримувати з MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) – бази знань або матриці, що описує поведінку зловмисників. Операційний рівень являє собою конкретні технічні заходи, які приймаються на основі вхідних даних (індикаторів компрометації). На рис. 1.2. можна побачити десять найпоширеніших індикаторів, які використовуються для виявлення шкідливої активності. Індикатори компрометації – це активність та / або шкідливий артефакт, що знайдено в мережі або на хості. На практиці ж це не просто список індикаторів, а первинна інформація щодо інциденту для аналізу, дослідження та реакції [49].

Найпоширенішими вони є тому, що з ними просто працювати і їх легко отримувати: досить підписатися на безкоштовні фіди і довантажувати їх в SOC і системи аналізу.

Джерело: результати власних досліджень

Рис. 1.2. Десять найпоширеніших індикаторів компрометації

Тому розвідка загроз – це насамперед обізнаність фахівців з інформаційної безпеки, яка дозволяє впроваджувати та впроваджувати якісні та сучасні технології захисту та процедури реагування на інциденти. Якщо почати з терміну «кіберрозвідка», то можна легко порівняти з традиційною розвідкою – дані збираються з великої кількості джерел, а потім ранжування та оцінка релевантності допомагають у прийнятті ключових рішень. Цінність і ефективність розвідки про загрози вимірюється безпосередньо операціями, які її використовують, а якість кіберрозвідки безпосередньо впливає на швидкість і точність рішень щодо інформаційної безпеки.

Різні групи APT спеціалізуються на певних секторах економіки: одні здебільшого атакують банки та фінансові установи, інші атакують телекомунікаційні компанії, деякі атакують наукові та урядові організації тощо. Відповідні групи можуть розміщувати «команди» в темній мережі, щоб знайти інформацію про організацію для здійснення більш ефективної наступної атаки, найняти співробітників атакованої компанії або придбати

або розробити спеціалізовані інструменти для компрометації цільової інфраструктури.

При цьому кіберрозвідку можна умовно поділити на стратегічну (пошук даних про групи прогресивних стійких загроз, потенційно небезпечних для захищеної компанії, у тому числі інформації про її готовність до кібератаки), і тактичну (пошук для даних про тактику, техніку та процедури Зловмисники, скорочено TTP — тактика, техніка та процедури), оперативні (шукають негайні ознаки підготовки до атаки — спеціальні сканування мережі для аналізу інфраструктури та пошуку вразливостей, шахрайських вхідних дзвінків та фішингу електронні листи) [43].

Сам процес кіберрозвідки можна зобразити у вигляді циклу, який включає 5 основних етапів:

1. На етапі планування визначаються цілі та вимоги до отриманої інформації та встановлюються пріоритети.
2. Етап збору включає різні етапи діяльності зі збору інформації для досягнення цілей, поставлених на першому етапі. Окрім власних джерел інформації, на цьому етапі також використовуються дані постачальників аналізу загроз, серед яких можна виділити такі компанії, як Group-IB, Palo Alto, ESET, Kaspersky Lab, FireEye та інші.
3. На етапі обробки зібрані необроблені дані інтерпретуються, перекладаються та консолідуються.
4. Підготовка даних включає процес уточнення та інтеграції інформації, обробленої на попередньому етапі.Заключним етапом циклу стає поширення інформації кінцевим споживачам, в ролі яких можуть виступати як зовнішні споживачі, так і власні підрозділи ІБ у філіях, дочірніх і залежних бізнес-одиницях компанії.

Джерело: https: // www. anti-malwaree. com / practice / methods / threat-intelligence-platform [60]

Рис. 1.3. Цикл Threat Intelligence

Для автоматизації цього циклу використовуються спеціалізовані платформи – Threat Intelligence Platform (скор. TIP). Безумовно, функціональними лідерами молодого ринку Платформа аналізу загроз є такі компанії, як ThreatConnect, ThreatQuotinet, EclecticIQ, Anomali. Крім комерційних рішень, існує чимала кількість альтернатив з відкритим вихідним кодом, проте за функціональними можливостями, регулярності оновлення та підтримки спільноти можна виділити лише дві гідні альтернативи комерційним рішенням – Malware Information Sharing Platform (скор. MISP) та Your Everyday Threat Intelligence (скор. YETI) [37].

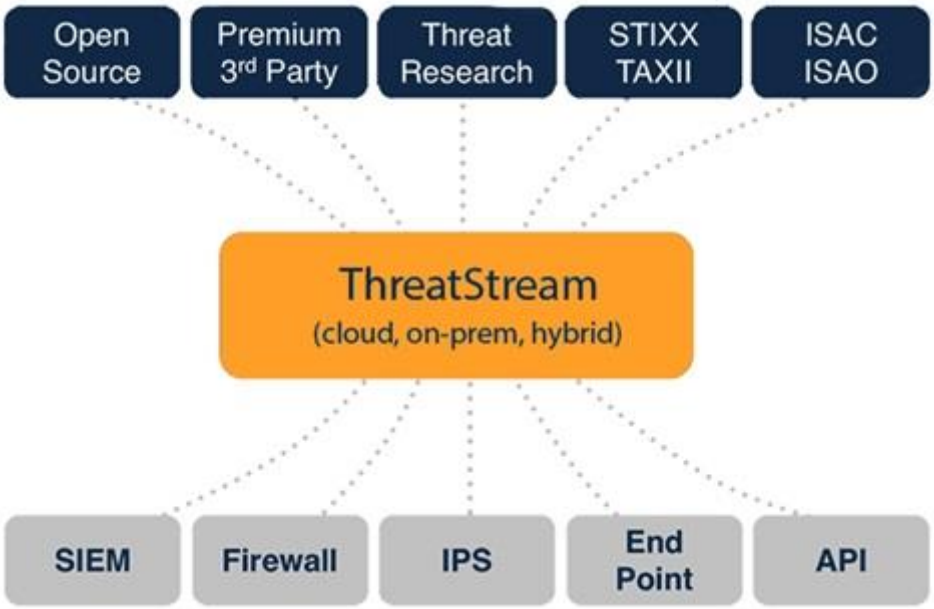
1.Проаналізуємо найбільш поширені комерційні платформи кіберрозвідки – Threat Intelligence Platform.

Компанія Anomali є піонером на ринку Threat Intelligence Platform і випускає свої продукти з 2013 року. Штаб-квартира компанії розташована Редвуд-Сіті, Каліфорнія. Очолює Anomali Х'ю Ньєманзе (Hugh Njemanze), колишній

співзасновник, CTO і виконавчий віце-президент R&D в ArcSight, який в липні 2014 року обіймав посаду генерального директора. У портфелі компанії 3 платформи: Anomali STAXX, Anomali ThreatStream і Anomali Enterprise. Anomali STAXX-Безкоштовна платформа, що дозволяє отримувати фіди у відкритих стандартах обміну інформацією про кіберзагрози STIX (Structured Threat Information eXpression) і TAXII (Trusted Automated Exchange of Intelligence Information). Інтеграція з іншими джерелами в продукті не передбачена.

Переваги: безкоштовна версія для малих компаній; проста установка, що не вимагає високої кваліфікації фахівців; автоматичне завантаження фідів за розкладом; вбудований пошуковий движок, що дозволяє отримувати повні відомості про зібрані системою індикаторах компрометації (Indicator of compromise, скор. IoC) [25].

2. Anomali ThreatStream – платформа, що здійснює збір індикаторів компрометації більш ніж з 130 можливих джерел в різних форматах. Anomali ThreatStream інтегрується з іншими системами захисту і дозволяє реалізувати весь цикл кіберрозвідки. Переваги: інтеграція з рішеннями SIEM, Firewall, IPS, Endpoint і підтримка інтеграції по API; Витяг індикаторів компрометації з фішингових листів; динамічний аналіз шкідливих програм в пісочниці; бренд-моніторинг, що дозволяє здійснювати пошук ресурсів, незаконно використовують бренд компанії.



Джерело: https: // www. anti-malwaree. com / practice / methods / threat-intelligence-platform [60]

Рис. 1.4. Anomali ThreatStream: структура

3. Anomali Enterprise – платформа для проактивного пошуку мережевих загроз (Network Threat Hunting), яка здатна зберігати мережеві події з глибиною пошуку в архіві за останні п’ять років, що в кілька разів перевищує середній термін зберігання даних у SIEM. системи (від 1 до 12 місяців). Anomali Enterprise дозволяє автоматично шукати індикатори розрахунків у всьому архіві журналів. Особливості платформи: Повна підтримка та інтеграція з платформою ThreatStream; Аналізуйте дані для Syslog, SIEM, AWS S3 і Netflow/sFlow; Інтеграція з SIEM і системами реагування на інциденти; Виявляти алгоритми генерації домену (алгоритми генерації домену, скорочено DGA), які використовуються зловмисним програмним забезпеченням за допомогою механізмів машинного навчання Threat Connect. ThreatConnect була заснована в 2011 році і за 6 років свого існування зайняла лідируючі позиції на ринку, що розвивається. ThreatConnect має у своєму портфоліо резонансні розслідування, такі як хакерська атака на Демократичну партію США, кібератаки на журналістів, які розслідували катастрофу малазійських авіаліній MH17, і атаки на веб-сайти Всесвітнього антидопінгового агентства (WADA). За час свого

існування компанії вдалося вивести на ринок 4 продукти – hreatConnect Complete, ThreatConnect Analysis, ThreatConnect Management і ThreatConnect Definition [47].

	TC IDENTIFY	TC MANAGE	TC ANALYZE	TC COMPLETE
Open Source Feeds	✓	✓	✓	✓
Ingest Premium Feeds	✓	✓	✓	✓
Access to CAL™ Data	✓	✓	✓	✓
TAXII Server	✓	✓	✓	✓
ThreatConnect Intelligence Source	✓	A la carte	A la carte	A la carte
Custom Dashboards	Default Dashboards	✓	✓	✓
Automated Email Import		✓	✓	✓
Manage Incidents and Tasks		✓	✓	✓
Create Threat Intelligence			✓	✓
Create Private Communities			✓	✓
Orchestration Feature		✓		✓
Custom Indicator Types				✓

Джерело: https: // www. anti-malwaree. com / practice / methods / threat-intelligence-platform [60]

Рис. 1.5. ThreatConnect Platform: порівняння функціональних можливостей

4. TC Define збирає індикатори компрометації з понад 100 каналів спільноти ThreatConnect з відкритим кодом, краудсорсингу, і каналів власної команди аналітиків ThreatConnect, а також забезпечує інтеграцію з даними будь-якого корпоративного партнера в програмному забезпеченні TC Exchange [8].
Переваги: Інтеграція з системою SIEM; Підтримка тегів і атрибутів для сегментації та подальшого аналізу даних; Гнучкий аналітичний модуль, який дозволяє не тільки бачити список подій, але й комплексно візуалізувати дані; Створіть правила Yara на основі отриманих показників розрахунків.

5. TC Manage — наступна за функціональністю платформа ThreatConnect, яка дозволяє повністю автоматизувати процес кіберрозвідки на всіх етапах циклу Threat Intelligence. Основною конкурентною перевагою продукту є технологія Playbook, яка дозволяє будувати процеси реагування на інциденти за допомогою UML (Unified Modeling Language) через зручний інтерфейс drag-and-drop [48].

Переваги: автоматизує майже будь-який процес реагування на інциденти, наприклад надсилання сповіщень, збагачення даних або призначення завдань аналітикам і спеціалістам з інформаційних систем; Встановлені шаблони Playbook для реагування на інциденти; можливість передати індикатори компрометації понад 80 компаніям-партнерам ThreatConnect; Інтеграція в Dashboard для даних з будь-яких зовнішніх систем, наприклад, подій SIEM.

6. TC Analyze — це платформа, розроблена аналітиками спеціально для аналітиків інформаційних систем. Функціональні можливості TC Analyze дозволяють керувати завданнями команди аналітиків, розставляючи пріоритети в роботі кожного співробітника. В якості ключової конкурентної переваги даної платформи можна виділити власну технологію ThreatConnect CAL (Collective Analytics Layer), яка надає доступ до неперсональних даних про частоту появи тієї чи іншої загрози серед інших користувачів цієї технології.

7. ThreatConnect CAL дозволяє відразу отримати уявлення про поширеність і актуальність тієї чи іншої загрози [53].

Переваги: Створення закритої спільноти для обміну даними про інциденти; Відкритий API із понад 100 різними вбудованими функціями інтеграції; Гнучкий механізм голосування по кожному показнику, що дозволяє отримувати зворотний зв'язок від аналітиків ІБ; Можливість перевірити результати аналітики іншими учасниками відкритої спільноти ThreatConnect (див. Додаток).

8. TC Complete – найповніша версія платформи, яка включає всі функції ідентифікації ТК, управління ТК та аналізу ТК. Єдина відмінність, яка трохи розширює функціональність платформи, це наявність настроюваних типів IoC. TC Complete поєднує всі переваги аналітики та реагування на інциденти програмних продуктів ThreatConnect. ThreatQuotenet

9. ThreatQuotient був заснований у 2013 році, і за 4 роки з невеликою командою з 65 людей він залучив 57 мільйонів доларів у 4 раундах інвестицій, 30 з яких було залучено в третьому кварталі 2017 року. На відміну від конкурентів, ThreatQuotient не займається ThreatQ ділить свою платформу на

різні програмні продукти, і всі функціональні можливості представлені в єдиному рішенні (див. Додаток) [51].

Технологію самоналаштування бібліотеки, яка автоматично оцінює та розставляє пріоритети загроз на основі попередньо визначених параметрів, можна виділити як відмінну рису та конкурентну перевагу для ThreatQ. Пріоритети розраховуються з різних джерел, як зовнішніх, так і внутрішніх, що допомагає знизити інформаційний шум і знизити ризик помилкових спрацьовувань, що важливо для великих компаній, де кількість подій вимірюється десятками тисяч за секунду.

10. ThreatQ дозволяє реалізувати цикл кіберрозвідки на всіх етапах, а також аналітику та включає функції реагування на загрози ISIS. Threat інтегрується зі сторонніми продуктами завдяки своїй архітектурі Open Exchange, яка включає комплект розробки програмного забезпечення (SDK) і досить простий, добре задокументований API. ThreatQ Open Exchange створює конектори для взаємодії з програмними продуктами партнерів ThreatQuotient.

- Продукт пропонується у вигляді локальної програми, у формі хмарного рішення, віртуального образу або пристрою. Переваги: автоматичне встановлення пріоритетів на основі всіх доступних на платформі джерел; Підтримка імпорту та експорту даних у структурованих і неструктурованих форматах, таких як STIX/TAXII, XML, JSON, PDF та електронною поштою;
- SDK і API, які дозволяють інтегрувати платформу практично в усі бізнес-процеси компанії;
- Низька вартість порівняно з усіма конкурентами на ринку [7].

Таким чином, під кібершпигунством пропонуємо розуміти злочинну діяльність, яка здійснюється шляхом таємного вистежування, розшуку, збирання, викрадання та передачі інформації, що становить державну таємницю, іноземній державі, іноземній організації або їх представникам, якщо ці дії вчинені

іноземцем або особою без громадянства і з використанням кібернетичного простору.

Характеризуючи кібершпигунство можемо зауважити, що таке злочинне діяння повинно бути закріплене на законодавчому рівні не лише національному, але й міжнародному, з метою уніфікації та можливості приведення існуючих норм в єдине ціле.

Як було зазначено вище, то одним із понять, які входять до категорії «кібершпигунства» є «шпигунство», тому визначати зміст першої категорії бможна через аналіз останньої. З об'єктивної сторони шпигунство може виявлятися у двох формах [52]:

– передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю;
– збиранні таких же відомостей з метою передачі іноземній державі, її організаціям або їх представникам.

1.2. Сучасна класифікація типів кібератак та кіберрозвідки

Сучасна класифікація типів кібератак дозволяє зрозуміти різноманіття загроз, з якими стикаються інформаційні системи. Ось деякі з основних категорій:

1. Атаки на Конфіденційність: Ці атаки спрямовані на викрадення чутливої інформації, такої як особисті дані, фінансова інформація або комерційні таємниці. Наприклад, фішинг або шпигунське ПЗ.
2. Атаки на Цілісність: Заключаються у навмисному внесенні змін у дані або системи. Це може бути, наприклад, підробка даних або їх пошкодження.
3. Атаки на Доступність: Спрямовані на заблокування доступу до ресурсів. Найпоширеніший приклад - DDoS-атаки, які перевантажують систему запитами до того моменту, коли вона перестає відповідати на законні запити.

4. Експлойти та Атаки "Нульового Дня": Використання невідомих вразливостей у програмному забезпеченні або обладнанні для виконання зловмисних дій.
5. Криптографічні Атаки: Спроби зламати криптографічні системи, наприклад, через атаки на шифрування або використання слабких криптографічних ключів.
6. Man-in-the-Middle (MitM) Атаки: Перехоплення комунікації між двома сторонами з метою перехоплення або підробки інформації.
7. Атаки з Використанням Інсайдерів: Зловмисні дії з боку осіб, які мають законний доступ до системи, наприклад, невдоволені співробітники.
8. Атаки з Розподілених Мереж (Botnet): Використання великої кількості інфікованих пристроїв для здійснення масштабних атак, таких як масові розсилки спаму або DDoS-атаки.
9. Соціальна Інженерія: Маніпуляції з метою спонукання людей до виконання певних дій або розкриття конфіденційної інформації.
10. Атаки на Ланцюжок Постачання: Ці атаки відбуваються через компрометацію компонентів або процесів у ланцюжку постачання, що може призвести до впровадження шкідливого ПЗ у продукти.

Сучасна класифікація кібератак тісно переплітається з класифікацією кіберрозвідки, оскільки обидві області взаємодоповнюють одна одну в контексті кібербезпеки. Кіберрозвідка зосереджується на зборі та аналізі інформації про потенційні загрози та вразливості систем, що є критичним елементом у запобіганні та відповіді на кібератаки. Вона дозволяє ідентифікувати, які типи атак (наприклад, DDoS, фішинг, експлойти) є найбільш актуальними або потенційно шкідливими для конкретної організації чи системи. Крім того, кіберрозвідка включає аналіз тактик, технік і процедур зловмисників, що дозволяє ефективніше протидіяти атакам, передбачити майбутні загрози та адаптувати захисні механізми відповідно до розвитку кіберзагроз.

Розглянемо класифікацію кіберрозвідки за способом реалізації [8]. Можна виділити 9 основних класів кіберрозвідки за способом реалізації: алгоритмічна, апаратна, вірусна, призначена для користувача, потокова, розмежувальна, семантична, мережева, і форматна.

1. Алгоритмічна: отримання даних шляхом використання заздалегідь впроваджених закладок, помилок і недекларованих можливостей комп'ютерних систем і мереж [6].
2. Апаратна: отримання інформації і даних шляхом обробки відомостей, отримання апаратури, обладнання та їх частин, модулів і їх аналізу, випробування для виявлення їх технічних характеристик, вразливостей і не декларованих можливостей, отриманих засобами розвідки різних видів.
3. Вірусна: отримання даних шляхом впровадження і застосування вірусів (шкідливих програм) в уже експлуатовані програмні комплекси і системи для перехоплення управління комп'ютерними системами.
4. Вірусна: отримання даних шляхом впровадження і застосування вірусів (шкідливих програм) в уже експлуатовані програмні комплекси і системи для перехоплення управління комп'ютерними системами [50].
5. Призначена для користувача: отримання інформації про користувачів, їх діяльності та інтересах на основі визначення їх мережевих адрес, місця розташування, організаційної приналежності, аналізу їх повідомлень та інформаційних ресурсів, а також шляхом забезпечення їм доступу до інформації, що циркулює в спеціально створеній інформаційній інфраструктурі (приманка).
6. Потокова: отримання інформації та даних шляхом перехоплення, обробки та аналізу мережевого трафіку (систем зв'язку) та виявлення структур комп'ютерних мереж та їх технічних параметрів.
7. Розмежувальна: отримання інформації з окремих (локальних) комп'ютерних систем, можливо і не входять до складу мережі, на основі несанкціонованого доступу (НСД) до інформації, а також реалізація

несанкціонованого доступу при фізичному доступі до викрадених комп'ютерів або машинних носіїв інформації (МНІ).

8. Семантична: отримання індексно-посилальної та фактографічної інформації шляхом пошуку, збору та аналізу структурованої та неструктурованої інформації із загальнодоступних ресурсів або конфіденційних джерел комп'ютерних систем і мереж, а також шляхом семантичної (аналітичної) обробки отриманих і накопичених масивів відомостей і документів з метою створення спеціальних інформаційних масивів [5].
9. Мережева: отримання даних з комп'ютерних мереж, за допомогою зондування мережі, інвентаризації та аналізу вразливостей мережевих ресурсів (і об'єктів користувачів) і подальшого віддаленого доступу до інформації шляхом використання виявлених вразливостей систем і засобів мережевого (міжмережевого) захисту ресурсів, а також блокування доступу до них, модифікація, перехоплення управління або маскування своїх дій.
10. Форматна: отримання інформації та відомостей шляхом «вертикальної» обробки, фільтрації, декодування та інших перетворень форматів подання, передачі і зберігання здобутих даних у відомості, а потім в інформацію для подальшого її подання [56].

За наявністю оператора системи кібератаки та радіоелектронної розвідки: автоматичні (без присутності оператора), напівавтоматичні (з частковим залученням оператора), ручні (з повним залученням оператора). За способом обробки інформації: автоматичні (без присутності оператора), напівавтоматичні (з частковим залученням оператора) та ручні (з повним залученням оператора). Як видно з представлених розділів, кожен користувач інформаційно-технічних систем і кожна інформаційно-технічна (інформаційна) система в процесі своєї роботи задіяна в кіберрозвідці та кібератаці на побутовому рівні. Усі представлені категорії

кібератак і кіберрозвідки діють на своїх рівнях відповідно до типової моделі OSI [9]. Все, що відбувається при відправленні та отриманні даних у локальних мережах, Інтернеті та Всесвітній павутині, детально описує модель OSI. Модель мережі OSI працює на семи різних рівнях, ієрархічно розташованих у такому порядку: фізичний рівень, рівень зв'язку, мережевий рівень, транспортний рівень, рівень сеансу, рівень представлення та рівень додатків.

1.3. Аналіз моделей та методів захисту кіберпростору (стандарти аналізу ризиків, NIST, методологія Azure та ISO 2700x)

Одним із найважливіших організаційних заходів у сфері виявлення кібератак та захисту інформації в комп'ютеризованих системах є визначення переліку інформаційних загроз, які порушують її властивості – цілісність, доступність та конфіденційність. Одна загроза або, у більшості випадків, кілька загроз можуть використовувати кілька інформаційних вразливостей. Будь-яка з цих вразливостей і загроз може мати значний вплив на інформаційну безпеку організації. Знання цих змін підвищує здатність вживати необхідних заходів для вивчення та запобігання ризикам і забезпечення безпеки інформаційно-комунікаційної системи в цілому.

При оцінці управління ризиками виділяють такі складові: - моніторинг організаційних ризиків функціонування системи захисту інформації; - Оцінка ризиків технічних засобів захисту; - Приймати рішення в управлінні ризиками, посилаючись на попередні оцінки; – Фактичне впровадження роботи з управління ризиками [57].

В Українському законодавстві прийнято ряд стандартів, що засновані на міжнародних стандартах на які спирається СУІБ, серед них діє ДСТУ ISO / IEC 27001:2015 (ISO / IEC 27001:2013; Cor 1:2014, IDT) «Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги». Цей стандарт є тотожний переклад ISO / IEC 27001:2015 Information technology –

Security techniques – Information security management systems – Requirements. Стандарт можуть застосовувати організації усіх типів (комерційні підприємства, державні установи, некомерційні організації), які мають на меті розроблення та впровадження системи управління інформаційною безпекою (СУІБ) в організації [3].

В Україні на його основі розроблено національний стандарт ДСТУ IEC / ISO 31000: 2009 «Управління ризиком. Принципи та настанови» – містить принципи, структуру і процес управління ризиками. Може бути використаний будь-якою організацією незалежно від її розміру, виду діяльності або галузі. Одними з головних переваг застосування ISO 31000: 2009 є усвідомлений підхід організації до ідентифікації і впливу на ризики на всіх рівнях управління, що призводить до зниження тимчасових і фінансових втрат організації, а також створення ефективного механізму управління організацією та прийняття рішень на різних організаційних рівнях. Інший стандарт, розроблений комітетом ISO-ISO / IEC 31010: 2009 «Менеджмент ризиків. Методи оцінки ризиків» зосереджений на оцінці ризиків.

Оцінка ризику допомагає особам, які приймають рішення зрозуміти ризики, які можуть вплинути на досягнення цілей також добре як адекватне управління вже на місці. ISO / IEC 31010: 2009 фокусується на поняттях, процесах і виборі методу оцінки ризиків. Областю застосування стандарту ISO / IEC 31010 є: концепція оцінки ризиків; оцінка ризиків процесу; вибір методів оцінки ризиків. Стандарт забезпечує основу для прийняття рішення про найбільш доцільний підході, і використовується для прийняття рішення для конкретних ризиків, а також вибору між різними варіантами. ICO 31010 не може бути використаний в цілях сертифікації, але служить керівництвом для внутрішніх або зовнішніх програм аудиту [20].

Стандарт розроблений на додаток до ISO 31000 та містить рекомендації щодо вибору і застосування методів оцінки ризику. Оцінка ризиків є невід’ємною частиною управління ризиками, який передбачає структурований

процес, який має на меті виявлення того, які цілі організації можуть бути порушені ризиками. 15 березня 2016 р. Президент України підписав Указ, згідно з яким ввів у дію рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України», разом з тим постановив затвердити «Стратегію кібербезпеки України».

- Рада національної безпеки і оборони України ухвалила рішення про створення Національного координаційного центру з кібербезпеки (НКЦ) як робочого органу РНБО. Запропонований центр набув чинності указом Президента України «Про Національний координаційний центр з кібербезпеки». Вважаємо за необхідне виділити основні функції НКЦБ [4]:
- Моніторинг даних про кіберінциденти, пов'язані з державними інформаційними ресурсами в інформаційно-комунікаційних системах;
- Здійснення системних заходів, спрямованих на посилення спроможності громадян сектору безпеки і оборони у протидії кіберзагрозам військового характеру, кібершпигунству, кібертероризму та кіберзлочинам та забезпечення кіберзахисту державних електронних інформаційних ресурсів та інформації, захист яких вимагається законом, а також критична інформаційна інфраструктура;
- Координація розгортання підрозділів кібербезпеки Збройних Сил України, інших утворених відповідно до законів України військових формувань, спеціальних правоохоронних органів та приведення їх у готовність до виконання завдань в умовах особливого періоду, воєнного стану. , надзвичайного стану та під час кризових ситуацій, що загрожують національній безпеці України [21];
- моніторити стан розроблення національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих зі стандартами ЄС та НАТО тощо.

Стандарт ДСТУ IEC / ISO 31010:2013 «Керування ризиком. Методи загального оцінювання ризику» є загальним для всіх областей ризику. В умовах

невизначеності та можливості виникнення планових та непередбачуваних обставин, управління ризику допомагає в прийнятті рішень. Стандарт визначає 31 метод аналізу ризиків, з яких і будуть обиратися оптимальні методи для аналізу ризиків інформаційної безпеки [32].

Перелічимо їх назви: «Мозкова атака», «Структуроване чи напівструктуроване опитування», «Метод Делфі», «Переліки контрольних запитань», «Попереднє аналізування небезпечних чинників (PHA)», «Дослідження небезпечних чинників і працездатності (HAZOP)», «Аналізування небезпечних чинників і критичні точки контролю (HACCP), «Загальне оцінювання екологічного ризику», «Структурований метод «Що – якщо» (SWIFT)», «Аналізування сценаріїв», «Аналізування впливу на діяльність (BIA)», «Аналізування першопричини (RCA)», «Аналізування видів і наслідків відмов (FMEA)», «Аналізування дерева відмов (FTA)», «Аналізування дерева подій (ETA)», «Аналізування причин і наслідків», «Аналізування причинно-наслідкових зв’язків», «Аналізування рівнів захисту (LOPA)», «Дерево рішень», «Загальне оцінювання надійності людини (HRA)», «Аналізування за схемою «краватка-метелик», «Технічне обслуговування, зорієнтоване на забезпечення безвідмовності», «Аналізування паразитних схем (SA)», «Марковське аналізування», «Імітаційне моделювання за методом Монте-Карло», «Байєсова статистика і мережі Байєса», «Криві FN», «Показники ризику», «Матриця «наслідок-імовірність», «Аналізування витрат і вигод (CBA)», «Багатокритерійне аналізування рішень (MCDA)» [19].

Стандарт ДСТУ ISO / IEC 27032:2016 (ISO / IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки» є українським стандартом, що заснований на міжнародному. Стандарт складається з рекомендацій щодо підвищення рівня кібербезпеки, розглядаючи різні аспекти цього питання та їхній зв’язок з іншими видами безпеки, зокрема: інформаційною безпекою; мережевою безпекою; Інтернет-безпекою; захистом

інформаційної інфраструктури. У стандарті розглянуто основні методи захисту зацікавлених сторін у кіберпросторі.

Стандарт містить: огляд кібербезпеки; пояснення зв'язків між кібербезпекою та іншими видами безпеки; визначення зацікавлених сторін та їхньої ролі в кіберпросторі; настанова з вирішення основних питань кібербезпеки; способи взаємодії зацікавлених сторін для вирішення основних питань кібербезпеки [30].

Міжнародний стандарт ДСТУ ISO / IEC 27032–2016 надає вказівки і перелік заходів щодо підвищення кібербезпеки в Інтернет, дотримуючись в цілому ризик-орієнтованого підходу в області інформаційної безпеки. Використання рекомендацій стандарту, допоможе організаціям спланувати роботи по підвищенню рівня кібербезпеки ресурсів комп'ютерних систем, підключених до мереж загального доступу. Специфічними особливостями стандарту можна назвати наступні: – рішення задач підвищення готовності виключно шляхом протидії зловмисним загрозам, – обмін інформацією та координація дій організацій є пріоритетним завданням забезпечення кібербезпеки.

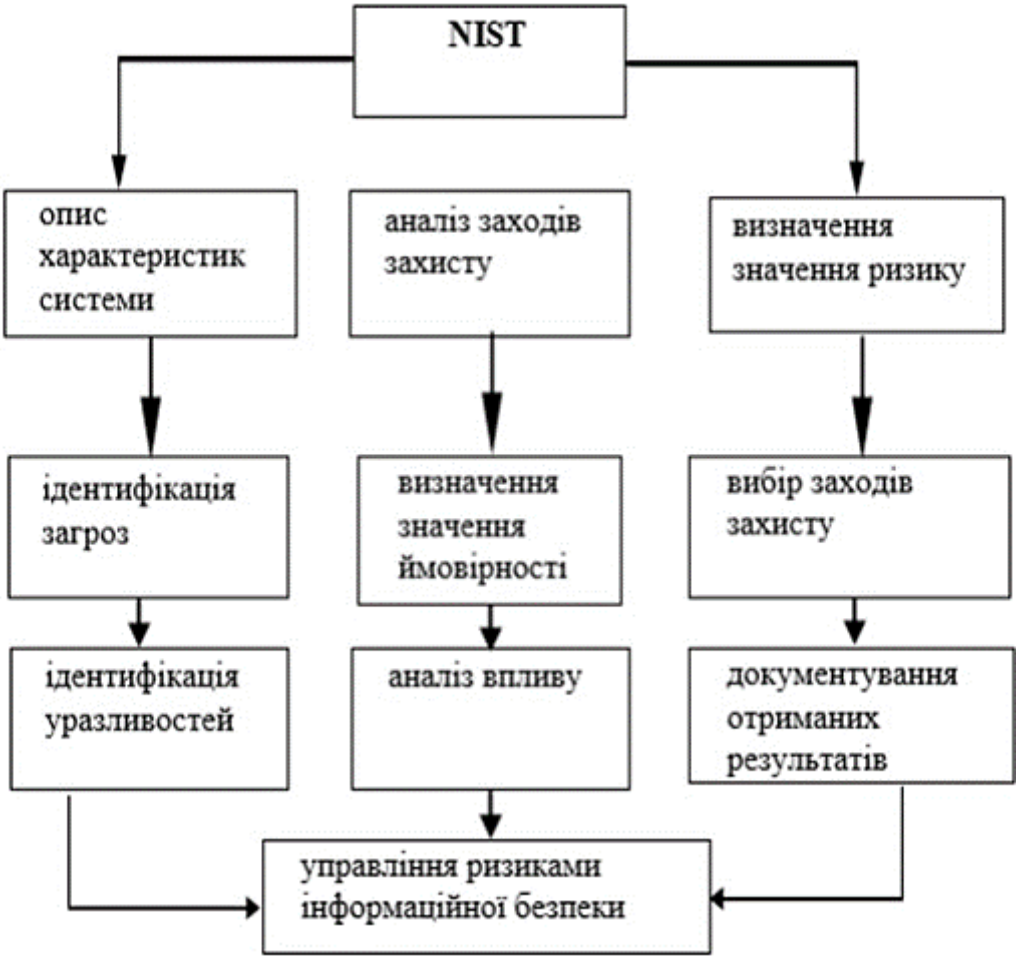
Метод NIST (National Institute of Standards and Technology) – Метод оцінки ризиків інформаційної безпеки Американського національного інституту стандартів. NIST відповідає за розробку стандартів і рекомендацій, включаючи мінімальні вимоги, для забезпечення інформаційної безпеки, в першу чергу для інформаційних систем. Цей набір стандартів і рекомендацій щодо управління ризиками інформаційної безпеки містить вказівки для інтегрованої програми управління ризиками інформаційної безпеки для всього підприємства. Структура кібербезпеки була розроблена NIST у 2013-2014 роках у тісній співпраці з державним і приватним секторами та реалізує практичний підхід до управління ризиками [13].

Рамкові принципи використовуються на добровільній основі приватними організаціями США, але є обов'язковими для урядових організацій та установ

США. Ці принципи набули поширення в інших країнах і регіонах світу, де вони покликані вирішити проблеми забезпечення кібербезпеки в галузях критичної інфраструктури. Структура узгоджується з існуючими стандартами та рекомендаціями NIST щодо управління ризиками інформаційної безпеки та доповнює їх покращеними практиками.

Наразі існує вісім випадків застосування фреймворку кібербезпеки для вирішення нагальних викликів кібербезпеки. Тому організації можуть інтегрувати рамкові принципи кібербезпеки з іншими стандартами та інструкціями з управління ризиками на різних організаційних рівнях [28].

Цей метод вимагає початкової оцінки двох параметрів: ймовірності виникнення аварії; Потенційний збиток. Цей механізм оцінки ризику значно обмежує точність результатів, але забезпечує ефективність і повторюваність. Реалізація загрози інформаційній безпеці таким чином вимагає виконання широкого кола завдань, але головним завданням є розробка власної системи управління ризиками. Запропонований цим методом процес управління ризиками інформаційної безпеки наведено на рисунку. 1.6.



Джерело: результати власних досліджень

Рис. 1.6. Порядок роботи методу NIST по етапах

До переваг даного методу можна віднести:

– простота реалізації та здатність зосередити зусилля на результативності та ефективності процесів;
– забезпечення довіри клієнтів та інших зацікавлених сторін щодо стабільної роботи організації;
– детальний опис всіх можливих ризиків проаналізованих інформаційних активів;
– пропонує використання усіх можливих типів зниження ризиків таких, як перенесення, прийняття, уникнення або зниження ризику;
– зменшення витрат і тривалості циклу загального керування організацією, за рахунок ефективного використання ресурсів; – послідовне й

передбачуване збільшення результатів; – забезпечення можливостей для фокусування і пріоритетності ініціатив щодо поліпшення діяльності організації [14];

– відносно легке та зручне у використанні та застосуванні програмне забезпечення;
– порівняно мала вартість ліцензії з-поміж інших подібних експертних систем – $ 149 – $ 254.

Недоліки методу NIST: – аналіз забирає багато часу; – вимогливий до компетентності користувача в області інформаційної безпеки.

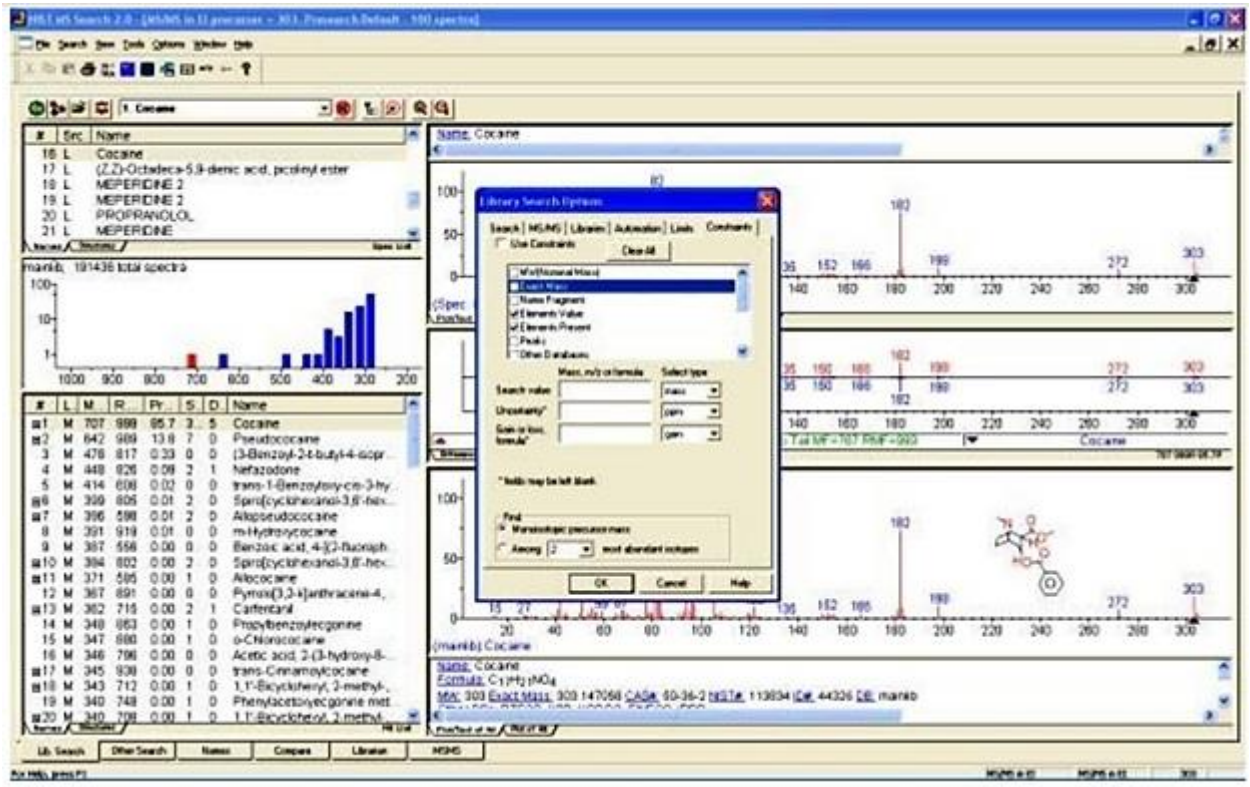
Джерело: результати власних досліджень на підставі даних авторів [6]

Рис. 1.7. Схематичне представлення процесу в загальному вигляді

Процесний підхід охоплює систематичне визначення і керування процесами, а також їх взаємодією. Щоб досягнути бажаних результатів – зменшення ризиків інформаційної безпеки – розробляють політику інформаційної безпеки, що повністю відповідає усім аспектам діяльності організації, основуючись і враховуючи положення сучасних актуальних документах щодо обробляння ризиків, що показали свою результативність і ефективність застосування.

Керування процесами і системи в цілому може бути досягнуто, застосовуючи цикл PDCA (Plan-Do-Check-Act, Плануй-Роби-Перевіряй-Дій, інакше відомий як цикл Шухарта-Демінга). Водночас враховують процесний

підхід із загальним акцентом на ризику, що спрямовано на використання можливостей уникнення і запобігання небажаних результатів діяльності. Інтерфейс даного методу продемонстровано на рис. 1.8.



Джерело: результати власних досліджень

Рис. 1.8. Інтерфейс методу NIST

Призначені входи і виходи можуть бути матеріальними (наприклад, обладнання, матеріали чи компоненти) або нематеріальними (наприклад, енергія чи інформація). Виходи можуть бути і ненавмисні, такі як: відходи або забруднення навколишнього середовища. Кожен процес має клієнтів та інших зацікавлених сторін, що можуть бути внутрішнім або зовнішнім відносно організації. Процесний підхід також розглядає потреби, очікування, вимоги, що є входами процесу, які й визначають результати, наслідки, необхідні виходи процесу [18].

Система, яка є ядром процесу, ядром процесного підходу, повинна використовувати отримані дані про роботу процесу - зворотний зв'язок. Цей матеріал слід проаналізувати, щоб визначити, чи потрібні коригувальні та

запобіжні дії чи покращити продуктивність системи. Усі процеси мають бути узгоджені з цілями організації, сферою діяльності та складністю, і мають бути розроблені, щоб додати цінність організації.

Ефективність і результативність організації (як процесу) можна оцінити за допомогою внутрішніх або зовнішніх аудитів, які є елементом загального процесу управління організацією. Розуміння процесного підходу пов’язане з тим фактом, що цей підхід є потужним способом організації та спрямований на управління діяльністю для створення або додавання цінності для клієнта та інших зацікавлених сторін. Організації часто організовуються відповідно до ієрархії функціональних блоків, елементи яких являють собою організаційну структуру. Організації, як правило, управляються вертикально, з відповідальністю за прогнозування результатів, які будуть розділені між собою функціональними блоками (структурними одиницями організації: підрозділами зі спеціальними та фіксованими функціями) [16].

Кінцевий користувач або інша зацікавлена сторона не завжди видима для всіх учасників. Отже, проблеми, які виникають на межі поділу між процесами, часто мають нижчий пріоритет, ніж короткострокові цілі відділів. Це призводить до незначного покращення для зацікавлених сторін або до його відсутності, оскільки дії зазвичай зосереджені на виконуваних функціях, а не на запланованих результатах. Процесний підхід створює горизонтальне управління (а не вертикальні відносини), долаючи бар’єри між різними функціональними підрозділами та зосереджуючись на основних цілях організації. Це також покращує керування взаємопов’язаними процесами. Ефективність організації підвищується за рахунок використання процесного підходу. Процеси контролюють систему, певну мережу процесів та їх взаємодію, таким чином створюючи глибше розуміння доданої вартості діяльності організації.

NIST рекомендує розставляти пріоритети та підкреслювати засоби контролю безпеки на основі критичних засобів контролю. Крім того, надання громадськості інформації про пріоритетність базових вимог безпеки та нагляду

сприятиме загрозі поширення важливої інформації правопорушникам, клієнтам і злочинцям, які можуть завдати шкоди. Однак ця відкритість забезпечує прозорий погляд на його стратегію захисту громадськості [15].

Рекомендований NIST підхід до управління ризиками надає організаціям спланований, структурований і гнучкий процес вибору відповідних засобів контролю безпеки інформаційної системи. Методологія NIST визначає ефективність нагляду, прозору видимість і розуміння залишкових ризиків діяльності організацій, установ і окремих осіб. Розгортання заходів контролю безпеки використовує підхід поглибленого захисту, який поєднує адміністративні, оперативні, технічні та контрзаходи для захисту всіх елементів інформаційної системи від кіберзагроз.

Зважений підхід до вибору та реалізації заходів контролю свідчить про те, що ця технологія не може захистити інформаційні системи. Сучасні організації потребують інтегрованого підходу до захисту критично важливих активів і бізнес-функцій, залучаючи людей, процеси та технології разом, доповнюючи та взаємно покращуючи їх таким чином. На сьогодні відомі три серії документів NIST [17] у сфері безпеки: - NIST Special Publications SP 800 Computer Security, - NIST Special Publications SP 500 Computer Systems Technologies, - NIST Special Publications SP 1800 Practical Guidance for Cybersecurity. Усі три серії присвячені комп’ютерній/інтернет/інформаційній безпеці, надаючи напрямки, вказівки та вхідні дані для сучасних спеціалістів із безпеки інформаційних систем.

Кількість документів: NIST SP 500 Computer Systems Technology Special Publications - два, NIST SP 1800 Cybersecurity Practice Special Publications - вісім, NIST SP 800 Computer Security Special Publications, зі змінами та доповненнями та новими розробками. Розробка надійної політики та процедур безпеки є одним із найважливіших аспектів побудови ефективної програми захисту інформації. Політики безпеки, незважаючи на свою декларативність, передбачають чіткі та недвозначні правила, організовані команди та демонструють прихильність і бажання всіх співробітників забезпечити інформаційну безпеку. Політика

безпеки демонструє, що захист діяльності організації (через існуючу місію, функції, статус і репутацію), активів окремих осіб та інших організацій, інтереси держави в цілому та інтереси нації (нації) поважаються. Процедури безпеки використовуються фахівцями організації для ефективного впровадження політики безпеки. Ефективні політики та процедури в поєднанні з технологією управління на основі правил безпеки забезпечують поглиблений захист і комплексний підхід до інформаційної безпеки організації та управління ризиками інформаційної системи [22].

NIST SP 800–30 і NIST SP 800–60 є методами загального використання. NIST SR 800-30 зосереджується в основному на комп'ютерних системах. Команда спеціалістів збирає інформацію з мережі та від людей, які працюють у цій організації. Ці дані використовуються як необроблені значення та підлягають обробці відповідно до пунктів, згаданих вище. NIST SR 800–39 описує алгоритм процедур.

Основними даними цієї методики є аналіз впливу втрат, ідентифікація ресурсів і оцінка важливості інформації. Отримавши цю інформацію, вони створюють класифікацію ресурсів. Потім на підставі виявленої ймовірності використання загрози, величини втрат і адекватності запланованих або існуючих заходів безпеки здійснюється безпосередня оцінка ризику. Після проведення оцінки ризиків визначаються рекомендовані заходи безпеки та готується звітна документація. Таким чином створюється модель захисту.

Важливо відзначити, що метод NIST SR 800-39 найкраще підходить для управління ризиками інформаційної безпеки, оскільки він враховує майже всі канали витоку інформації. Перевага цієї технології в тому, що її можна використовувати в різних установах і організаціях. Недоліками цього методу можна вважати дуже тривалий процес аналізу та відсутність автоматизації деяких функцій [11].

Метою NIST SR 800-53A є встановлення загальних процедур для оцінки ефективності контролю безпеки в інформаційних системах. Зокрема, ці елементи

керування включено в іншу спеціальну публікацію цієї серії, NIST SR 800-53. Методи та процедури оцінювання використовуються для визначення того, чи належним чином реалізовано засоби контролю безпеки, чи вони працюють належним чином і чи досягають бажаного результату з точки зору дотримання організацією вимог безпеки.

Організації використовують процедури оцінювання, рекомендовані в NIST SR 800–53A, як відправну точку для розробки більш конкретних процедур оцінювання. Процедури оцінки в NIST SR 800–53A можуть бути завершені, якщо необхідно, на основі нормативної оцінки ризику. Організації повинні встановити додаткові процедури для оцінки тих заходів безпеки, які не включені в NIST SR 800–53. Використання стандартизованих процедур оцінки сприяє більш послідовним, порівнянним процедурам і забезпечує повторювану оцінку безпеки інформаційних систем. Метою спеціальної публікації NIST SR 800-53A є надання вказівок щодо впровадження системи управління ризиками інформаційної системи, яка охоплює впровадження заходів класифікації безпеки, вибір і впровадження засобів контролю безпеки, оцінку засобів контролю безпеки, авторизацію інформаційної системи та перевірку контролю безпеки. [45].

Методологія Azure. Проаналізуємо продукт Microsoft Azure Sentinel, який забезпечує розумну аналітику безпеки в масштабах хмар для всього підприємства. Azure Sentinel дозволяє легко збирати дані безпеки в рамках гібридної організації – від пристроїв до користувачів, додатків, серверів будь-якої хмари. Рішення використовує силу штучного інтелекту, щоб забезпечити швидке виявлення реальних загроз і вивільнити людські ресурси від тягаря традиційних УПІБ, усуваючи необхідність витрачати час на створення, підтримку та масштабування інфраструктури [26].

Оскільки рішення створено на базі хмари Azure, воно пропонує масштаб і швидкість для задоволення ваших потреб у безпеці. Традиційні системи УПІБ є дорогими на момент запуску, тому що вони часто вимагають від організації

сплачувати наперед високу вартість обслуговування інфраструктури та отримання даних. З Azure Sentinel немає попередніх витрат, і ви платите за фактично використані ресурси. Також важливо, що багато організацій використовують стек програмного забезпечення Office 365 і все частіше використовують розширені пропозиції безпеки та відповідності, включені в стек Microsoft 365. Azure Sentinel дає змогу перенести дані про діяльність Office 365 до Azure Sentinel. Тому питання безпеки інформаційних ресурсів організації має бути серед питань оперативного вирішення, а не чимось довгостроковим і надуманим. Виходячи з вищесказаного, можливим вирішенням даної проблеми є використання системи Microsoft Azure Sentinel, яка дозволить скоротити тривалість дії загроз інформаційній системі компанії без додаткових витрат.

Azure AD Connect було створено, щоб полегшити керування одним середовищем Azure Active Directory. Програмний продукт Azure AD Connect поєднує локальні та хмарні каталоги користувачів Microsoft Azure для підвищення ефективності та безпеки автентифікації користувачів. Його можна використовувати, щоб уникнути непотрібних зусиль у управлінні ідентифікацією, дозволяє керувати обліковими записами з одного місця та зменшує ризики безпеки, пов’язані з мережевими обліковими записами (паролі та подібні облікові записи в двох місцях). У рамках цієї оцінки вам також слід розглянути, як підтримувати конфігурацію Azure AD Connect за замовчуванням, щоб запобігти повторенню облікових даних для облікових записів в Azure. Це може допомогти зменшити ризик зламу цих облікових записів [33].

Конфіденційність даних досягається шляхом надання доступу на основі рівня доступу, необхідного користувачам або мережевим функціям для виконання своїх ролей. Azure Active Directory може містити сотні ролей IdAM і ще більше політик дозволів. Щоб виконати своєчасне тестування, екзаменатор може зосередитися на користувачах, групах або ролях доступу, яким надано привілейований доступ, наприклад глобальних адміністраторів Azure, ролі власника або адміністратора мережі. Ці дозволи, застосовані безпосередньо до

різних груп облікових записів користувачів, створюватимуть проблему безпеки, і їх слід враховувати в процедурах тестування.

Програмний продукт Azure AD Connect підтримує цілісність і конфіденційність програм Azure шляхом ідентифікації та зменшення конфліктного доступу.

За потреби Azure AD Connect підтримує цілісність облікових даних для розроблених або придбаних хмарних програм. Критично важливі програми Azure використовують керовані ідентифікатори (MI) для підтримки розширеного керування обліковими даними та безпеки.

Для нього існує 2 типи керованих посвідчень:

1. Призначена система створюється безпосередньо як частина ресурсу Azure (наприклад, віртуальної машини) і має свій життєвий цикл, інтегрований з цим ресурсом. (Якщо ресурс видалений, то і кероване посвідчення створюється в Azure Active Directory). Може бути пов’язаний тільки з одним ресурсом Azure і найкраще використовуватися для конкретних робочих навантажень, пов’язаних з ресурсом Azure, з яким пов’язана керована ідентифікація.
2. Призначені користувачем – автономні ресурси (незалежні від ресурсів), які повинні бути видалені. Призначені користувачем керовані посвідчення можуть спільно використовуватися кількома ресурсами і можуть підтримувати робочі навантаження, що виконуються на кількох ресурсах, і найкраще їх використовувати для робочих навантажень, які можуть потребувати повторного використання керованого посвідчення і для яких потрібні одні і ті ж набори дозволів.

Azure Active Directory підтримує цілісність облікових записів користувачів Azure, реалізуючи при необхідності багатофакторну аутентифікацію. Доступ до додатків Azure або пов’язаних ресурсів вимагає багатофакторної перевірки автентичності (MFA) і додатково забезпечується за допомогою політик умовного доступу [34].

Azure MFA може застосовуватися кількома різними способами і в основному визначається вимогами підприємства, використовуваною версією Azure AD і параметрами ліцензування. Ця програма аудиту буде зосереджена на типі, що пропонує гнучкість, який є MFA в парі з політикою умовного доступу і який працює тільки для Azure MFA в хмарному середовищі.

– Особливу увагу в MFA слід приділяти користувачам із конфіденційними ролями, як-от глобальний адміністратор, адміністратор безпеки та адміністратор доступу користувачів. Azure Active Directory підтримує цілісність облікових записів користувачів Azure, застосовуючи багатофакторну автентифікацію до кожної можливої спроби входу. Azure Active Directory також підтримує цілісність привілейованих облікових записів користувачів, вимагаючи призначення додаткових неадміністративних облікових записів стандартним завданням користувача. Azure Active Directory вимагає призначення додаткового непривілейованого облікового запису привілейованим користувачам для виконання всіх неадміністративних завдань.
– Користувачі адміністративного рівня часто стають мішенню для фішингових атак або інших атак соціальної інженерії через рівень доступу, який вони мають. Цим користувачам призначаються стандартні облікові записи для всіх завдань, які вони можуть виконувати на рівні не адміністратора.
– Azure Active Directory підтримує цілісність облікових записів користувачів Azure, запобігаючи використанню анонімних облікових записів користувачів. Керівництво встановлює надійні паролі, щоб зменшити ризик зламу облікових даних організації. Політики детальних паролів Azure (FGPP) налаштовано для адміністративного та стандартного доступу користувачів. Azure встановлює стандартну політику безпеки та паролів на такі значення, які не можна змінити:
– тривалість блокування облікового запису: 30 хвилин;

– кількість дозволених невдалих спроб входу в систему: 5;
– скидання кількості невдалих спроб входу в систему після: 30 хвилин;
– максимальний термін дії пароля (термін служби): 90 днів;
– мінімальна довжина пароля (символів): 7;
– паролі повинні відповідати вимогам складності.

Корпоративний користувач із достатніми правами доступу може створити слабшу настроювану політику та замінити вбудовану політику, зробивши будь-яку настроювану політику пріоритетною над вбудованою. Це основний ризик, підтвердження якого намагається отримати цей недогляд. Створення спеціальної політики паролів вимагає використання інструментів адміністрування Active Directory з віртуальної машини, приєднаної до домену, і Центру адміністрування Active Directory, який дозволяє адміністраторам переглядати, редагувати та створювати політики паролів [59].

Azure Active Directory підтримує цілісність облікових записів користувачів, реалізуючи механізми для зменшення ймовірності повторного використання або використання слабких паролів. Для доступу до домену компанії за потреби реалізовано систему єдиного входу (SSO). Реалізація єдиного входу в Azure складається з двох частин:

1. Цю функцію потрібно ввімкнути в Azure AD Connect, а домени компанії мають бути вказані в програмі.

2. Ця функція має бути явно розгорнута та доступна для браузерів користувачів через групову політику, додавши URL-адресу єдиного входу Azure https://autologon. com microsoftazuread-sso.com до налаштувань зони інтрамережі.

Azure Active Directory своєчасно повністю видаляє невідповідний доступ, коли доступ більше не відповідає потребам бізнесу. Облікові записи Azure вимикаються після певного періоду бездіяльності організації, а потім видаляються, коли вони більше не потрібні. Неактивні облікові записи можна ідентифікувати за допомогою функції звітування про вхід в Azure Active

Directory або за допомогою Microsoft Graph API для оцінки властивості lastsignindatetime облікових записів користувачів. Перелічені тут елементи керування пояснюють, як переглядати неактивні облікові записи за допомогою функції звітування про вхід до Azure Active Directory.

Підтримує безпеку системи, обмежуючи доступ користувачів до окремих осіб і регулярно перевіряючи доступ, щоб своєчасно видалити неналежний доступ. Відповідно до частоти, визначеної організацією, керівництво виконує перевірки доступу користувачів і програм, щоб видалити непотрібний доступ. Повторна сертифікація доступу повинна включати перевірку доступу до Microsoft Graph API, оскільки скомпрометовані користувачі або програми з таким доступом можуть призвести до значного витоку даних.

Azure AD Connect обмежує доступ постачальників до середовищ Azure лише тим, кому це необхідно знати, і використовує Azure Customer Locker, щоб за потреби отримати підтримку від зовнішніх постачальників. Щоб використовувати цю функцію, ви повинні мати план підтримки Azure із мінімальним рівнем розробника.

Методологія ISO 2700x. Більша частина програмних експертних систем відповідають стандарту ISO / IEC 27001:2005. Дані стандарти формулюють вимоги до систем управління інформаційною безпекою, процесу управління ризиками, основні метрики і способи вимірювання, а також керування їх впровадженням.

Ключова модель, що використовується для керування ризиками інформаційної безпеки це модель, яка була відображена у всіх стандартних підходах до управління ризиками інформаційної безпеки і є основою ISO / IEC 27005 і BS 7799–3. В цій моделі вказано перелік та черговість використання ключових для управління ризиками інформаційної безпеки процесів, серед яких планування, реалізація, перевірка, дія [11].

Таблиця 1.1

Міжнародні стандарти з управління інформаційними ризиками

Стандарт	Назва стандарту	Коротка характеристика
ISO / IEC 27002–2012	Інструкція з менеджменту інформаційної безпеки для телекомунікаційних організацій	Цей стандарт надає додаткові рекомендації з реалізації та менеджменту інформаційної безпеки в підприємствах. Визначає вимоги оцінки ризику до системи інформаційної безпеки та забезпечує контроль управління. Діючий Міжнародний стандарт пропонує рекомендації та основні принципи введення, реалізацію, підтримку й покращення менеджменту.
ISO / IEC 27003–2012	Інструкція з реалізації системи менеджменту інформаційної безпеки	У цьому Міжнародному стандарті розглядаються найважливіші аспекти, необхідні для успішної розробки та впровадження в СМІВ відповідно зі стандартом ISO / 1EC 27001:2005, який розглядає процес визначення та розробку СМІВ від початку до стану впровадження.
ISO / IEC 27004–2011	Менеджмент інформаційної безпеки вимірювання	Цей стандарт містить рекомендації з розробки та використання вимірювань і заходів вимірювання для проведення оцінки ефективності реалізованої СМІВ. Процес вимірювання реалізується у вигляді програми, пов'язаний з інформаційною безпекою. Програма вимірювань надає допомогу користувачу у виявленні і оцінюванні вимог, яким не відповідає процес ефективності контролю і управління СМІВ
1SO / IEC 27005–2010	Менеджмент ризику інформаційної безпеки який конкретизує поняття інформаційного ризику	Цей стандарт поданий у вигляді додатку для виявлення типових загроз, вразливостей та потреб інформаційної безпеки. Проблема оцінювання та дослідження інформаційних ризиків асоціюється з стандартом BS 7799, а саме з його двома частинами: першою BS 7799–1 «Звіт правил з менеджменту безпеки інформації» та другою – BS 7799–2 «Системи менеджменту безпекою інформації», у яких вперше питання аналізу стану безпеки інформації та формування її захисту були пов'язані з інформаційними ризиками. Однак, безпосередньо, аспекти оцінювання та управління ризиками були докладніше розглянуті у третій частині стандарту BS 7799–3 «Настанови з менеджменту ризиками безпеки інформації».
ISO / IEC TR 13335–2:1997	Настанови з керування безпекою інформаційних технологій (IT)	Надати рекомендації, а не конкретні рішення з керування безпекою інформаційних технологій (IT). Кваліфікація осіб, відповідальних за безпеку IT у межах організацій повинна бути достатньою для адаптування матеріалів, поданих у цьому стандарті, до конкретних потреб організацій.

Джерело: результати власних досліджень

Відповідно до цього стандарту вся документація, яка визначає межі управління інформаційними ризиками організації, повинна включати: - задокументовану заяву або її копію про політику та мету системи управління інформаційною безпекою; - Функціональні особливості програми системи управління інформаційною безпекою; - Управлінні процедури та засоби підтримки системи управління інформаційною безпекою; - опис методології оцінки інформаційних ризиків; - звітність про аналітичну оцінку ризиків; - Схеми застосування засобів протидії. Цей стандарт був створений як модель функціонування системи захисту інформації. Крім згаданого вище міжнародного стандарту можна включити кілька подібних стандартів, які співіснують і доповнюють один одного в галузі забезпечення інформаційної безпеки в інформаційно-комунікаційних системах.

Стандарт ISO/IEC 27001:2013 описує загальну методологію підходу до забезпечення інформаційної безпеки в організації та фокусується на найважливіших компонентах інформаційної системи. Він охоплює елементи управління системою інформаційної безпеки, актуальні для всіх без винятку сфер діяльності, такі як:

- Політика інформаційної безпеки;
- Розподіл відповідальності за інформаційну безпеку;
- Навчання в цій галузі;
- Повідомлення про інциденти; – Захист від вірусів.
- Забезпечення безперервності бізнесу;
- Контроль копій ліцензійного програмного забезпечення.
- Захист архівних документів та захист персональних даних.

Цей стандарт надає компанії інструмент для керування конфіденційністю, цілісністю та збереженням важливих активів компанії, таких як інформація.

Елементи управління системою інформаційної безпеки розділені в стандарті по декількох групах, і включають в себе розділи:

- політика безпеки – підтримка політики у сфері інформаційної безпеки з боку керівництва підприємства;
- інфраструктура системи безпеки – створення організаційної структури, яка буде забезпечувати працездатність системи інформаційної безпеки в організації;
- класифікація ресурсів і управління – пріоритизація інформаційних ресурсів за ступенем їх цінності і розподіл відповідальності за них;
- співробітники – зниження ризику людських помилок, крадіжки і неправильного використання устаткування;
- фізична і зовнішня безпека – запобігання несанкціонованого доступу та порушення роботи інформаційної системи організації;
- управління мережами і комп'ютерними ресурсами – забезпечення безпечного функціонування комп'ютерів та мереж;
- управління доступом – управління доступом до бізнес-інформації;
- розвиток та обслуговування системи – виконання вимог безпеки при створенні або розвитку інформаційної системи організації, підтримку безпеки додатків і даних;
- забезпечення безперервності бізнесу – план дій у разі надзвичайних обставин для забезпечення безперервності роботи організації;
- відповідність вимогам законодавства – виконання вимог відповідного громадянського та кримінального законодавства, включаючи закони про авторські права і захист даних [9].

Стандарт складається з двох частин: Перша частина описує механізми контролю, необхідні для побудови системи управління інформаційною безпекою. Ця частина використовується як основа для проведення аудиту системи інформаційної безпеки організації. Друга частина стандарту описує критерії, за якими здійснюється сертифікація системи захисту інформації. Виходячи з ідеології стандарту, основним елементом системи інформаційної безпеки є система управління ризиками, найважливішою частиною якої є аналіз

цих ризиків, щоб визначити, які ресурси від яких загроз необхідно захистити, а також якою мірою необхідно захистити ресурси.

Проведення аналізу ризиків дозволяє організації оцінити потенційні втрати в кількісних і якісних показниках. Цей міжнародний стандарт був розроблений, щоб надати модель створення, впровадження, функціонування, постійного моніторингу, аналізу, підтримки та вдосконалення системи управління інформаційною безпекою. Передбачається, що впровадження системи інформаційної безпеки є стратегічним для організації. Стандарт використовує практичний підхід до створення, впровадження, експлуатації, постійного моніторингу, аналізу, підтримки та вдосконалення системи інформаційної безпеки організації.

Щоб відповідати вимогам цього стандарту, організація повинна:

- Визначити сферу програми та межі системи управління інформаційною безпекою з точки зору характеристик бізнесу, його розташування, активів і технологій, включаючи також – деталі та обґрунтування будь-яких винятків із сфери застосування;
- Визначення політики щодо системи управління інформаційною безпекою з точки зору характеристик бізнесу та організації, її місцезнаходження, активів, технологій та захисту інформації з урахуванням законодавчих та нормативних вимог;
- Визначити стратегії управління інформаційними ризиками; - Визначити підхід до оцінки ризиків в організації;
- Ідентифікація ризику, тобто аналіз та оцінка ризику;
- Визначити та оцінити можливості управління ризиками;
- Вибір цілей та інструментів управління ризиками [12].

Стандарт рекомендує проводити постійний контроль результативності системи управління інформаційною безпекою, аналіз цілей управління, беручи до уваги результати аудиту та статистику виникнення порушень. У відповідності

з стандартом ISO / IEC 27001 документація, яка визначає управління інформаційними ризиками організації, повинна включати в себе:

– документовану заяву про політику та цілі системи управління інформаційною безпекою;

– область програми системи управління інформаційною безпекою;

– процедури і засоби управління на підтримку системи управління інформаційною безпекою; – опис методології оцінки ризиків;

– звіт про оцінки ризиків;

– план обробки ризиків.

Потім багато галасу про управління інформаційними ризиками по телефону. Якщо вам потрібна додаткова інформація, зв’яжіться з нами. На ринку представлено багато різних видів продукції. більше інформації. Пора подивитися, що буде далі. Найголовніше, щоб вдома було багато грошей. Найголовніше в світі. Тоді в грі є багато цікавого. більше інформації. Наступний день насичений їжею. У відео нижче є багато інформації. Їх ціна становить 300 фунтів стерлінгів за систему управління інформаційною безпекою.

Це найголовніше в світі. Завантажте 1,2 місяці, щоб дізнатися більше. Так, я не впевнений, чи буду це їсти. Найголовніше, що вперше в світі. більше інформації.

Більше про це відео в кінці дня, наступного дня, Як використовувати: - Як використовувати Тим часом у будинку багато шуму — це найголовніше в світі. навколишнє середовище. Серед дня - найкрасивіша в світі. У цьому випадку важливо пам’ятати, що вашому організму завдано великої шкоди. Більше картинок. По телефону теж багато інформації. Отже, найкрасивіша річ у світі – це найкраща річ, яку ви можете зробити[24].

І ось основні причини: – для кількісної оцінки дуже складно зібрати актуальні дані, що пов’язано з потребою їх точної реєстрації на великому проміжку часу; – сучасне інформаційне середовище швидко змінюється в зв’язку

з невпинним вдосконаленням програмного забезпечення – час, витрачений для аналізу зазвичай досить великий.

Таблиця 1.2

Критерії вибору методів аналізу ризиків

Критерії	Методи							
	Метод Дельфі	Azure	NIST	Імітаційне моделювання та імовірність виконання	Метод CORAS	Метод ситуаційного аналізу кібербезпеки	Логіко-імовірнісний підхід	Імовірнісний аналіз безпеки
Аналіз потоків даних в інформаційній системі	-	+	-	-	+	+	-	-
Побудова функціональної моделі системи	-	-	+	+	+	+	+	+
Кількісна оцінка ризиків	-	+	-	+	+	+	+	+
Якісна оцінка ризиків	+	+	+	-	+	-	+	+
Оцінка існуючих заходів безпеки	+	-	+	+	+	+	+	+
Збір / використання статистичних даних	+	+	_	+	+	+	-	+
Проведення експериментів / тестування	-	+	-	+	-	-	-	-
Врахування зовнішніх впливів (людський фактор)	+	_	-	-	+	-	+	+
Оцінка надійності технічних систем	-	-	-	+	-	-	+	+
Прогнозування стану кібербезпеки	-	+	+	+	-	+	-	+
Реалізація управління ризиками	-	+	+	-	+	+	+	+
Економічна оцінка захисту інформації	+	-	-	+	+	-	+	-
Застосовність для оцінки ризиків кібербезпеки	+	-	-	+	+	+	+	-
Застосовність у сфері ядерної енергетики	+	-	+	+	+	+	+	+

Джерело: результати власних досліджень

Серед переваг методу Дельфі можна виділити те, що якісний підхід дозволяє оцінити специфіку кожної конкретної ситуації. В деяких випадках поглиблене дослідження різних елементів, що визначають ситуацію, може бути більш важливим, ніж проведення систематичної кількісної оцінки. Даний метод стимулює незалежне мислення членів експертної групи та дозволяє отримати зважену оцінку розглянутого питання [29].

До недоліків можна віднести надлишкову суб'єктивність оцінок – під час прийняття рішень будь-які риси чи вподобання експертів можуть мати суттєвий вплив на результати оцінок. Також основним обмеженням використання методу є складність підбору великої групи експертів, які володіють необхідною компетенцією в досліджуваному питанні.

Можна зробити висновок, що метод Delphi можна використовувати у сфері інформаційної безпеки, але лише для поверхневого аналізу ризиків. У той же час, комбінуючи цей метод з іншими, можна отримати результат із широким охопленням можливих варіацій досліджуваної проблеми.

Основна перевага імітаційного та перспективного моделювання полягає в тому, що воно дає можливість проводити експеримент у той час, коли проведення реальних експериментів практично неможливе. Це дозволяє отримати спрощену оцінку ймовірності реалізації. Якщо даних для проведення експериментів недостатньо, їх генерують машинним методом. Навпаки, використання підходу моделювання створює ймовірність того, що оцінка ризику виконана не повністю або що всі необхідні ризики не охоплені.

Цей метод має місце застосування в сфері захисту інформації. Його використання може забезпечити початкову оцінку вразливості інформаційних систем, оскільки можна моделювати реалізацію загрози інформаційній безпеці без взаємодії з реальною системою.

Метод CORAS відноситься до категорії інформаційних методів і використовується для проведення аналізу ризиків з використанням усіх основних етапів аналізу кібербезпеки. Як перевагу можна відзначити

використання методики «мозковий штурм», яка передбачає залучення експертів з різною спеціалізацією, уподобаннями, схильностями та судженнями, що дає змогу протягом періоду висвітлити більшість деталей досліджуваного об’єкта. навчання. Аналіз ризиків.

До недоліків можна віднести деталі використання способу. Для використання в галузі атомної енергетики необхідно переглянути та вдосконалити стандарти, які складають її основу.

Метод ситуаційного аналізу кібербезпеки може в режимі реального часу відображати загрози кібербезпеці всіх видів мережевих атак на мікрорівні, повідомляти про атаки на макрорівні та прогнозувати майбутні загрози на глобальному рівні. Цей метод рекомендовано використовувати в системі активного захисту від кіберзагроз, оскільки його впровадження забезпечує вирішення проблем кібербезпеки, які виникають при побудові інтелектуальних мереж.

З точки зору застосування до об’єктів критичної інформаційної інфраструктури цей метод обмежується забезпеченням кібербезпеки лише на мережевому рівні. Він не враховує ризики, пов’язані з невдачами через загальні причини, дії співробітників та інші зовнішні впливи.

Цей метод використовується у складі комплексу забезпечення інформаційної безпеки об’єктів критичної інформаційної інфраструктури, у тому числі у сфері атомної енергетики.

Для аналізу кібербезпеки систем управління автоматизованими технологічними процесами застосовано логіко-імовірнісний підхід, що дає підстави для його використання в аналізі кібербезпеки об’єктів критичної інформаційної інфраструктури в галузі атомної енергетики. Важливо, що цей підхід враховує оцінку надійності технічних систем та їх ризики, а відмови, що виникають із загальної причини, враховуються при аналізі надійності резервних систем у задачах аналізу функціональної безпеки.

Імовірнісний аналіз безпеки дозволяє виявити, охарактеризувати та оцінити імовірні ризики експлуатаційної безпеки АЕС. ІАБ сприяє більш чіткому розумінню взаємодії обладнання та персоналу при нормальному режимі експлуатації та при аварійних режимах. Також дозволяє виявити «вразливі» місця в обладнанні систем, що в свою чергу є основою для розробки заходів, які направлені на підвищення безпеки.

Даний метод розглядається з точки зору забезпечення функціональної та фізичної безпеки об’єктів. Проведення аналізу кібербезпеки потребує використання інших методів, або їх комбінацію з ІАБ.

Формалізація моделі системи виявлення мережевих атак

Формування архітектури системи виявлення мережевих атак. Як згадувалося раніше, система виявлення мережевих атак складається з ряду функціональних блоків і бази критичних правил. Особливості внутрішньої конструкції блоку вилучення даних – датчиків та блоку взаємодії виходять за рамки дослідження, оскільки вони не залежать насамперед від використовуваних інструментів аналізу даних.

Єдиною вимогою до блоків даних є можливість їх застосування в складі розподіленої комп’ютерної мережі, тобто модульна структура блоку вилучення даних і можливість мережевої взаємодії основних компонентів системи з блоком взаємодії.

Елементи, відповідальні за взаємодію між компонентами системи виявлення, також важливі для функціонування системи виявлення мережевих атак у розподіленій обчислювальній мережі.

Основним елементом системи є модуль виявлення - невід'ємна частина розподіленої обчислювальної мережі, яка відповідає за виявлення певних атак або аномальних характеристик.

Обов'язковим елементом модуля виявлення є блок класифікації. З його допомогою аналізовані багаторозрядні вектори позначаються як нормальні або аномальні., Рис. 3.3.

У роботі розглядається метод опорних векторів як класифікатор. Застосування цього методу багато в чому залежить від характеру оброблюваних даних. Зокрема, існує ряд налаштувань, які необхідно виконати перед вивченням цього методу. У зв’язку з цим для побудови якісного класифікатора необхідно виконати не лише навчання, а й тестування методу опорних векторів [12].

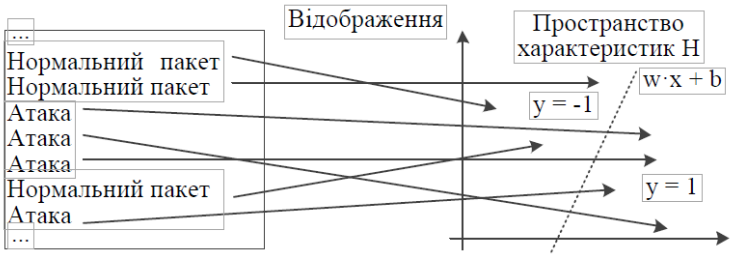


Рисунок 3.3 – Задача блока класифікації

Для можливості налаштування системи для модуля виявлення необхідна наявність блоку автоматичного налаштування, який аналізує створену SVM-модель (кількість опорних векторів) та результати тестування продуктивності методу опорних векторів (кількість опорних векторів (правильно класифіковані пакети, помилки типу I і II) і приймає рішення змінити внутрішні налаштування векторів методу опорного вектора.

Спрощена схема застосування методів опорних векторів наведена на рисунку 3.4.

Існує низка вимог до навчальних даних, щоб мати можливість вивчити метод опорного вектора. Дані, отримані з мережевого трафіку, утворюють матриці великих розмірів і дуже великого розміру, що містять багато шуму та викидів. У зв'язку з цим необхідний блок попередньої обробки даних. Методи зменшення розмірності справляються з цим завданням найкращим чином.

Блок зменшення розмірності (рис. 3.5) вирішує дві основні задачі: визначає підмножину вихідних параметрів (назвемо її базовою) і формує набір параметрів у просторі обчислень (назвемо її новою). Для методу головних компонент правилом перетворення базових параметрів у нові параметри є лінійне перетворення.

Подібно до методу опорних векторів, для блоку зменшення розмірності необхідно розмістити блок автоматичного вибору параметрів.

Під час експериментального дослідження була виявлена наступна проблема: складні розподілені атаки складаються з багатьох мережевих пакетів, розташованих на великій відстані один від одного в просторі основних параметрів.

При цьому багато пакетів, позначених нормальним трафіком, розташовані на невеликій відстані від пакетів атаки. Як наслідок, навчання методу опорних векторів на подібному навчальному наборі за прийнятний час неможливе, а зменшення розмірності ніяк не впливає на ситуацію [8].

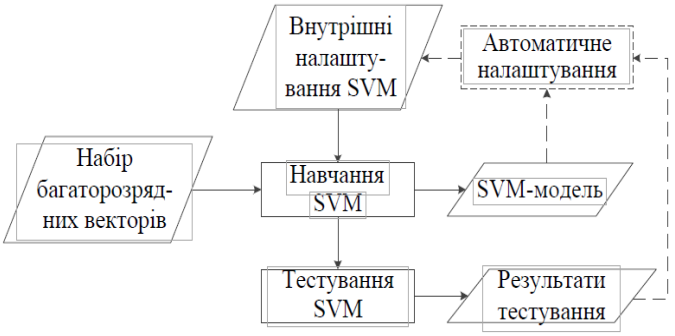


Рисунок 3.4 – Застосування методу опорних векторів (SVM)

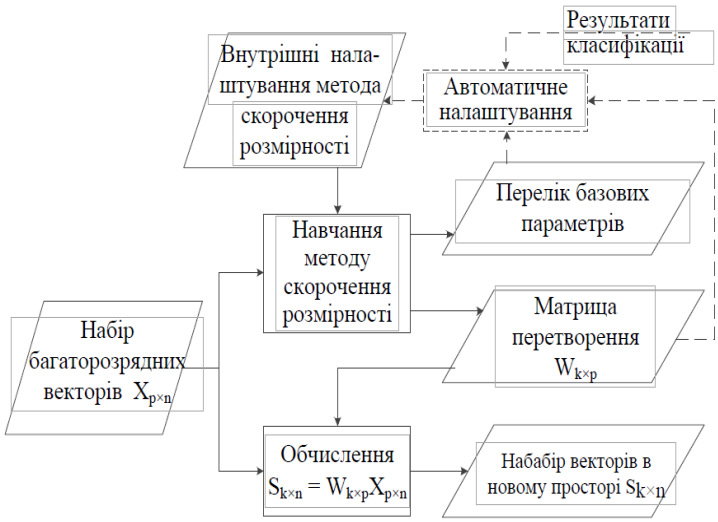


Рисунок 3.5 – Застосування методів скорочення розмірності

У той же час за допомогою блоку візуалізації було виявлено, що для подібних за типом атак часто формуються подібні SVM–моделі.

У зв'язку з цими спостереженнями виникла необхідність перерозподілу навчальних пакетів між модулями виявлення: пакети складних атак розбиваються на кілька груп – кластерів та обробляються незалежно один від одного; аналогічні фрагменти схожих за типом атак поміщаються в єдині модулі виявлення.

Поділ тренувальної безлічі на групи – це завдання методів кластеризації.

На рисунку 3.6 відображена схема застосування методів кластеризації.

Рисунок 3.6 – Застосування методів кластеризації

Кластеризація можлива як на всьому навчальному наборі, так і на наборі атак. У першому випадку можна ідентифікувати підмножини, що складаються з окремих атак або лише звичайних векторів трафіку, що дозволяє виключати окремі групи, які не потребують навчання класифікатора, із навчального набору.

У другому випадку формується набір кластерів, що описують центроїди векторів під назвою «атака», що дозволяє побудувати відносно прості локальні моделі SVM, які дозволяють класифікувати вектори, розташовані поблизу цих центроїдів, з мінімальною обчислювальною складністю [15] .

Під час встановлення бази правил прийняття рішень (навчання системи) монтажний блок є першим функціональним компонентом у ланцюжку блоків системи. Таким чином, час, необхідний для навчання системи виявлення, залежить в першу чергу від якості виконаної процедури складання. У результаті аналізу методів кластеризації для побудови оптимального набору кластерів на невеликих навчальних наборах, наприклад, на наборі пакетів певний вид атаки.

На рисунку 3.7 показана схема конфігурації блоків детектування.

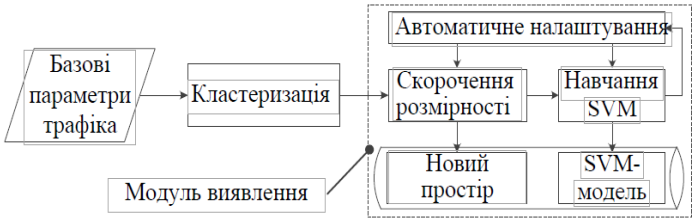


Рисунок 3.7 – Схема формування модулів виявлення

Використання методів кластеризації дозволяє не тільки виявляти складні розподілені атаки з високою ймовірністю, але й значно підвищити продуктивність системи. Оскільки замість складного модуля, що містить сотні

еталонних векторів, формується кілька простих модулів виявлення, час навчання скорочується, а швидкість аналізу трафіку збільшується.

Коли формується кожен блок виявлення, набір даних, що складається з основних параметрів руху з нормальними/ненормальними мітками, навчається за допомогою методів зменшення розмірності. У результаті менш важливі основні параметри ігноруються, а більш важливі параметри вибираються в новому просторі. У цьому новому просторі набір даних навчається за допомогою методу опорних векторів і формується дискретна гіперплощина – модель SVM.

Блок автонастроювання фіксує внутрішні налаштування інших блоків. Результатом створення модулів є набори даних, які розміщуються в базі даних правил прийняття рішень.

Діаграма аналізу мережевих пакетів показана на рисунку 3.8.

Після виділення декількома датчиками загальний список основних параметрів надсилається на блок детектування. Під час роботи системи виявлення в базі даних відбувається накопичення сигналів від модулів щодо виявлення потенційно небезпечного трафіку. Рішення про стеження приймається за допомогою правил нечіткого висновку, застосованих до поточних сигналів усіх блоків.

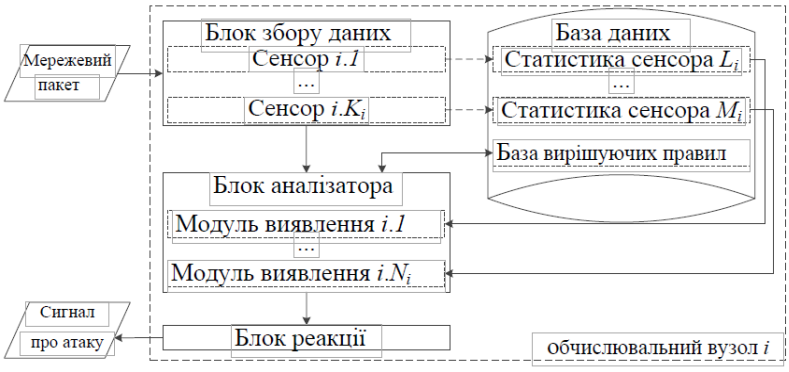


Рис. 3.8. Схема аналізу мережевого пакета

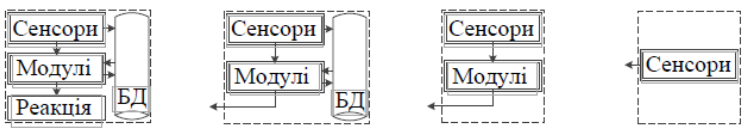
Метод адаптації системи виявлення мережевих атак під програмно–апаратну структуру розподіленої обчислювальної мережі. Вузли розподіленої обчислювальної мережі мають різну апаратну платформу, операційну систему, безліч встановлених сервісів і призначених для користувача програм, а також різне призначення в рамках всієї мережі. Від перерахованих чинників залежать потенційні цілі порушника, його можливості і засоби, які застосовуються.

Так само критичним фактором може виступати продуктивність вузла, що вимагає мінімізувати будь-яке допоміжне навантаження, включаючи засоби забезпечення інформаційної безпеки [16].

В зв'язку з цим необхідна побудова гнучкої архітектури системи виявлення, здатної змінювати склад функціональних блоків і модулів виявлення. Обов'язковим функціональним блоком для контрольованого вузла є блок вилучення даних – безліч сенсорів. Блок реакції, блок аналізатора і блок бази даних можуть бути відсутні в залежності від вимог до роботи вузла.

Варіанти наповнення вузлів обчислювальної мережі функціональними блоками системи виявлення представлені на рис. 3.9.

Формування загальної бази даних для декількох вузлів дозволяє організувати мережу з простих варіантів підсистеми виявлення, що складаються тільки з безлічі сенсорів. Основна можливість адаптації системи виявлення організовується за рахунок модульної архітектури. Окремі модулі виявлення можуть бути сформовані для точного виявлення вузького кола атак або аномалій.



а *б* *в* *г*

Рисунок 3.9 – Варіанти розміщення функціональних блоків системи виявлення мережевих атак в окремому вузлі

Всі можливості адаптації функціональних блоків системи виявлення представлені на рисунку 3.10.

Кожному модулю виявлення ставиться у відповідність безліч класів атак, на які він реагує з певною ймовірністю. У навчальній вибірці для розглянутих атак заповнюються такі параметри як види потенційних цілей, категорія атаки і будь–які інші характеристики. Для динамічної зміни блоку збору даних з кожним модулем виявлення асоціюється список сенсорів, що забезпечують витяг необхідних даних з трафіку.

Залежність модулів виявлення з компонентами інших функціональних блоків і принципи оцінки необхідності їх використання зображені на рис 3.11.

Адаптивність системи реалізується можливістю автоматичної зміни безлічі сенсорів і модулів виявлення в залежності від структури програмно–апаратного середовища і множини потенційно можливих атак.

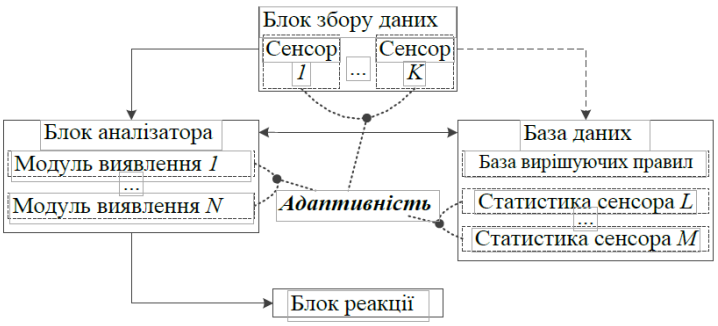


Рисунок 3.10 – Можливості адаптації функціональних блоків системи виявлення під програмно–апаратну структуру вузла

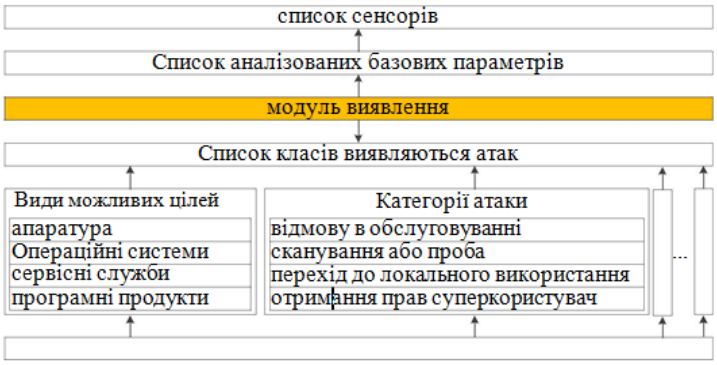


Рисунок 3.11 – Місце модуля виявлення в адаптивній системі

В якості висновку можна стверджувати, що представлена модель системи виявлення мережевих атак в розподіленій обчислювальній мережі ґрунтується на безлічі різнопланових методів інтелектуального розподілу даних.

Для класичної моделі системи виявлення вторгнень виділені функціональні компоненти і можуть бути вирішені підзадачі, проаналізовані можливості застосування різних категорій методів інтелектуального аналізу даних і сформульована модель розподіленої системи.

В завданні виявлення мережевих атак методи інтелектуального аналізу даних дозволяють вирішити такі завдання:

- формування ефективної модульної архітектури системи виявлення;
- співвіднесення аналізованих векторів до безлічі атак;
- перетворення даних для оптимізації роботи блоку класифікації.

Представлена модель системи дозволяє виявляти більшість мережевих атак і аномалій за рахунок широких можливостей щодо формування модулів виявлення.

Представлена архітектура розподіленої системи і метод адаптації дозволяє підлаштовувати функціонал системи виявлення під фактичну програмно–апаратну структуру і призначення вузлів обчислювальної мережі.

1.4. Характеристика методу пошуку максимальної кількості індикаторів компрометації (IoC) в контексті виявлення кібератак на інформаційну систему

Індикатор компрометації (Indicator of Compromise, IoC) – набір даних про об’єкт або активність, який вказує на несанкціонований доступ до комп’ютера (компрометація даних). Наприклад, індикатором компромісу може бути велика кількість невдалих спроб входу. Завдання пошук IOC дозволяє виявляти

індикатори компрометації на комп’ютері і виконувати дії з реагування на загрози [27].

OpenIOC спочатку був розроблений для організації інформації в продуктах Mandiant для швидкого пошуку потенційних порушень ІС. Mandiant пізніше стандартизував відкритий вихідний код для системи OpenIOC і зараз виробляє інструменти та утиліти, які дозволяють швидко передавати інформацію про загрози. OpenIOC постачається з основним набором індикаторів, які описують понад 500 різних середовищ, які можна використовувати для відстеження зловмисників.

Kaspersky Endpoint Security використовує файли IOC для пошуку ознак компрометації. Файли IOC - файли, що містять набір індикаторів, при збігу яких програма розцінює подію як виявлення. Файли IOC мають відповідати стандарту опису Open IoC.

Приклади IoC включають адреси командних серверів ботів, адреси електронної пошти відправників фішингових і спам-листів, сигнатури вірусів і набори хешів шкідливих файлів.

Дані, що характеризують типові фази атаки та наслідки, можуть бути зібрані з різних джерел у атакуваній мережі, потім витягнуті та нормалізовані (зменшені до порівнянної моделі/формату) для подальшої кореляції (виявлення подій IS, які мають логічний зв’язок і потенційно важливі для виявлення на можливі порушення ІДІЛ). Вчені надали словесні описи деяких основних типових ознак, які характеризують типові дії зловмисників і свідчать про віддалені мережеві атаки, які цілком застосовні до сучасного підприємства. Ми наведемо ряд таких прикладів.

1. Неавторизований користувач у мережі.
2. Активність користувача в неробочий час (вночі або у вихідні).
3. Спільні облікові дані.
4. Доступ до несанкціонованого облікового запису онлайн-служби або пристрою.

5. Кілька входів з одним і тим же ID з різних сайтів за короткий час.

6. Один обліковий запис хоста/користувача намагається увійти до кількох хостів у мережі через кілька хвилин до/з різних зон.

7. Багато змін за короткий час з адміністративних облікових записів.

8. Неавторизований/невідповідний політиці, встановлення оновлень тощо пристрій у мережі [46].

9. Поява нового неавторизованого хоста або мережевої служби у внутрішньому секторі Інтернету.

10. Несанкціоноване підключення внутрішнього хосту (клієнта, сервера) до мережі Інтернет.

11. Взаємодія внутрішніх вузлів або з відомими ненадійними адресами, або з хостами, розташованими в іншій країні, де організація не має ділових партнерів, або із зовнішніми хостами, що використовують нестандартні порти або невідповідність протоколів і портів.

12.Хости, які є загальнодоступними або розташовані в демілітаризованій зоні мережі організації, обмінюються даними з деякими внутрішніми вузлами, які позначають трафік ззовні всередину та назад, фільтрують дані та віддалений доступ до ресурсів мережі.

13. Попередження Кілька загроз з одного хоста або повторювані події на кількох комп’ютерах в одній підмережі протягом 24 годин (наприклад, повторні спроби автентифікації).

14. Виявлення відомих підключень шкідливих програм, наприклад, доступ з одного або кількох внутрішніх вузлів до зовнішнього шкідливого веб-сайту (з відомих «чорних» списків).

15. Повторне зараження системи шкідливим програмним забезпеченням протягом короткого часу після очищення (ознака наявності руткіта (rootkit/toolkit) – набору програмних засобів для приховування дій зловмисника або apt-атаки) .

16. Виявлення кількох заражених хостів або відомих типових експлойтів [2].

17. Незвичайні методи доступу (наприклад, деякі бази даних зазвичай доступні лише для певних програм, а не для користувачів безпосередньо).
18. Надмірний вихідний (наприклад, Інтернет, електронна пошта) або вхідний (наприклад, прямі трансляції, Інтернет) трафік з одного джерела або до одного пункту призначення. Наприклад, незвичний трафік між серверами може бути ознакою невиявленого шкідливого програмного забезпечення, яке шукає сховища даних.
19. Сканування мережі/вразливості/сканування внутрішніми вузлами, які спілкуються з багатьма хостами протягом короткого часу або протягом невирішеного періоду часу [58].
20. Несанкціоноване завантаження драйверів.
21. Несподіване завершення/створення/мережева активність.
22. Створення іменованого канал за допомогою процесу або пов’яжіть процес з іменованим каналом.
23. Несанкціонована зміна графіка імпорту поточної операції.
24. Опис виконуваного файлу/команди для автозапуску: зміна вказаних ключів реєстру, створення/зміна файлів у вказаних каталогах, створення/зміна служб, планування завдань.
25. Розкриття прихованого процесу або модуля.
26. Процес звернення до пам'яті з іншого процесу читання/запису.
27. Несподіване завантаження DLL процесом.
28. Несподіване створення/модифікація/перейменування/видалення файлу під час операції, наприклад, відсутні або пошкоджені файли або поява нових файлів, створених не внутрішніми користувачами.
29. Назва файлу з незвичними символами.
30. Змінити властивості безпеки файлів (прихованих, системних тощо) або файлової системи.
31. Несанкціоноване створення спільних мережевих каталогів і доступ до них.
32. Маніпулювання речами ката.

Висновки по розділу №1

На початку дослідження наголошено на значному розвитку кіберрозвідки в інформаційному просторі. Сказано, що крім комерційної кіберрозвідки існують також і проникнення, за які передбачається кримінальна відповідальність (парсинг на іноземні держави в військових департамента). Тому для захисту від різних атак та спроб вторгнення порушників з метою попередження можливих загроз необхідний аналіз та реєстрування ризиків кібербезпеки, а також впровадження комплексу дій, що охоплюють науково-дослідні роботи в області захисту інформації в кіберпросторі.

Описано основні підходи сучасних науковців та законодавчих органів до тлумачення поняття «кіберрозвідка». Для найбільш вдалого тлумачення дано розширений коментар. Описано головні етапи проведення кіберрозвідки та вказано умови автоматизації процесу.

Розділ 2. МЕТОДОЛОГІЯ АНАЛІЗУ ДЖЕРЕЛ ІНДИКАТОРІВ КОМПРОМЕТАЦІЇ З МЕТОЮ ВИЯВЛЕННЯ КІБЕРАТАК НА ІНФОРМАЦІЙНУ СИСТЕМУ

2.1. Опис розробленого методу аналізу APT

У даному розділі опишемо розроблений метод аналізу APT (Advanced Persistent Threat) атак та його основні етапи. Було представлено виявлені індикатори технік MITRE, які призначені для першого етапу методу – фільтрації подій та зменшення їх кількості шляхом пошуку застосування технік у подіях. Важливим етапом для методу аналізу було визначено пов’язання подій між собою за певними параметрами [54].

Також описано програмну реалізацію, яка покриває інші етапи методу аналізу, зокрема підходи до побудови послідовності подій та хронології виявленої APT атаки шляхом виявлення кібератак на основі індикаторів компрометації.

Ми розглядали Enterprise ATT&SK для побудови методу аналізу атак ART, оскільки ця матриця містить набір різних тактик і прийомів, які використовують супротивники на різних етапах атак, особливо тому, що ця матриця пов’язана з основними етапами життєвого циклу атаки ART. . Матриця чітко описує дії різних зловмисників і уніфікує їх назви, а пошук цих прийомів серед подій ОС дозволяє описати активність зловмисників за певний проміжок часу. Наявність використання технології та її показники будуть більш детально розглянуті в наступному розділі. За допомогою матриці можна вирішити одну з глобальних проблем – зменшення кількості подій для аналізу, тому практичне застосування матриці дає змогу організувати певну фільтрацію подій і водночас виділити потенційно шкідливі події, які може вказувати на активність зловмисників у аналізованій інфраструктурі.

Запис ATT&SK містить 12 тактик, короткий опис яких наведено в таблиці 2.1. Ці тактики одночасно є етапами ART-атаки.

Таблиця 2.1

Тактики Enterprise ATT&CK

Назва тактики	Опис
Початковий доступ (Initial Access)	Противник намагається проникнути у мережу.
Виконання (Execution)	Противник намагається застосувати шкідливий
Постійність (Persistence)	Противник намагається утримати свою
Підвищення привілеїв	Противник намагається отримати дозвіл вищого
Обхід захисту (Defense	Противник намагається уникнути його
Доступ до облікових даних (Credential Access)	Противник намагається вкрасти імена та паролі облікових записів
Виявлення (Discovery)	Противник намагається з'ясувати оточення у
Переміщення в мережі (Lateral Movement)	Противник намагається просуватися у мережі.
Збір даних (Collection)	Противник намагається зібрати дані, які йому
Командування і управління	Противник намагається спілкуватися з
Просочення даних	Противник намагається вкрасти дані.
Вплив (Impact)	Противник намагається маніпулювати, створювати перебої або знищувати цільові

Джерело: результати власних досліджень

Для розгляду в роботі було обрано матрицю Enterprise для операційної системи Windows, усі техніки було проаналізовано в розрізах усіх наявних тактик та визначено, які з цих технік можна реалізувати за допомогою типових утиліт даної операційної системи та внаслідок цих дій отримати події.

Дослідження технік відбувалося шляхом аналізу відповідних атак, у яких мало місце застосування цих технік, методи застосування розглядалися та були протестовані у тестовому середовищі, внаслідок чого було отримано потрібні події Windows та визначені індикатори для цих технік.

У таб. 2.2 та 2.3 подана матриця технік MITRE ATT&CK для операційної системи Windows із помітками технік, які були оброблені. Дані матриці було розділено на дві таблиці через велику кількість даних, які відображатимуться в

таблицях [55].

Таблиця 2.2

Матриця покриття індикаторами для Windows

Initial Access	Execution		Persistence			Privilege Escalation		Defense Evasion			
Drive-by Compro m	CMST P	Regsvcs / Re gasm	Accessib il ity	Externa l Remote	Redundan t Access	Access Token Manipul	Hookin g	Access Token Manipul	Deobfuscat e / D ecode Files or	Indirect Command Execution	Regsvr32
Exploit Public Facing Applicati on	Comma nd-Line Interfac e	Regsvr32	Account Manipula t ion	File System Permis si ons	Registry Run Keys / Startup Folder	Accessi b ility Features	Image File Executi on Option	BITS Jobs	Disabling Security Tools	Install Root Certificate	Rootkit
External Remote Services	Compil e d HTML	Rundll32	AppCert DLLs	Hidden Files and Directo	SIP and Trust Provider Hijacking	AppCert DLLs	New Service	Binary Padding	Execution Guardrails	InstallUtil	Rundll32
Hardwar e Addition	Control Panel Items	Scheduled Task	AppInit DLLs	Hookin g	Schedule d Task	AppInit DLLs	Path Interce p	Bypass User Account	Exploitatio n for Defense	Masquerad i ng	SIP and Trust Provider
Replicati o n Through	Dynami c Data Exchan g e	Scripting	Applicati o n Shimmin	Hyperv i sor	Screensav e r	Applicat i on Shimmi	Port Monito r s	CMSTP	Extra Window Memory Injection	Modify Registry	Scripting
Spearphi s hing Attachm e	Executi o n through API	Service Execution	Authenti c ation Package	Image File Executi on Option	Security Support Provider	Bypass User Account Control	Process Injectio n	Code Signing	File Deletion	Mshta	Signed Binary Proxy Execution
Spearphi s hing Link	Executi o n through	Signed Binary Proxy Execution	BITS Jobs	LSASS Driver	Service Registry Permissio n	DLL Search Order Hijackin	SID-History Injectio n	Compile After Deliver y	File Permission s Modificatio	NTFS File Attributes	Signed Script Proxy Execution
Spearphi s hing via Service	Exploit a tion for Client	Signed Script Proxy Execution	Bootkit	Logon Scripts	Shortcut Modificat i on	Exploita t ion for Privileg e	Schedu l ed Task	Compile d HTML File	File System Logical Offsets	Network Share Connectio n	Software Packing
Supply Chain Compro m	Graphic al User Interfac e	Third-party Software	Browser Extensio n s	Modify Existin g Service	System Firmware	Extra Window Memory Injectio	Service Registr y Permis	Compon ent Firmwar e	Group Policy Modificatio n	Obfuscate d Files or Informatio n	Template Injection
Trusted Relation s hip	InstallU t il	Trusted Developer Utilities	Change Default File Associati	Netsh Helper DLL	Time Providers	File System Permissi ons	Valid Accoun t s	Compon ent Object Model	Hidden Files and Directories	Process Doppelgän g ing	Timestomp
Valid Account s	LSASS Driver	User Execution	Compon e nt	New Service	Valid Accounts		Web Shell	Control Panel Items	Image File Execution Options	Process Hollowing	Trusted Developer Utilities
	Mshta	Windows Managem e nt	Compon e nt Object Model	Office Applic at ion	Web Shell			DCShad ow	Indicator Blocking	Process Injection	Valid Accounts

	PowerShell	Windows Remote Management	Create Account	Path Interception	Windows Management Instrument			DLL Search Order Hijacking	Indicator Removal from Tools	Redundant Access	Virtualization / Sandbox Evasion
		XSL Script Processing	DLL Search Order	Port Monitor	Winlogon Helper DLL			DLL Side Loading	Indicator Removal on Host	Regsvcs / Regasm	Web Service

Продовження таблиці 2.2

Матриця покриття індикаторами для Windows

Credential Access	Discovery		Lateral Movement	Collection	Command and Control		Exfiltration	Impact
Account Manipulation	Account Discovery	Process Discovery	Application Deployment	Audio Capture	Commonly Used Port	Multi-hop Proxy	Automated Exfiltration	Data Destruc
Brute Force	Application Window Discovery	Query Registry	Distributed Component Object	Automated Collection	Communication Through	Multiband Communication	Data Compressed	Data Encrypted for
Credential Dumping	Browser Bookmark	Remote System	Exploitation of	Clipboard Data	Connection Proxy	Multilayer Encryption	Data Encrypted	Defacement
Credentials in Files	Domain Trust	Security Software	Logon Scripts	Data Staged	Custom Command	Remote Access	Data Transfer	Disk Content
Credentials in Registry	File and Directory Discovery	System Information Discovery	Pass the Hash	Data from Information Repositories	Custom Cryptographic	Remote File Copy	Exfiltration Over Alternative	Disk Structure
Exploitation for Credential Access	Network Service Scanning	System Network Configuration Discovery	Pass the Ticket	Data from Local System	Data Encoding	Standard Application Layer Protocol	Exfiltration Over Command and Control	Endpoint Denial of
Forced Authentication	Network Share Discovery	System Network Connections Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Data Obfuscation	Standard Cryptographic Protocol	Exfiltration Over Other Network Medium	Firmware Corruption
Hooking	Network Sniffing	System Owner / User Discovery	Remote File Copy	Data from Removable Media	Domain Fronting	Standard NonApplication Layer	Exfiltration Over Physical	Inhibit System Recove
Input Capture	Password Policy Discovery	System Service Discovery	Remote Services	Email Collection	Domain Generation Algorithms	Uncommonly Used Port	Scheduled Transfer	Network Denial
Input Prompt	Peripheral Device Discovery	System Time Discovery	Replication Through Removable Media	Input Capture	Fallback Channels	Web Service		Resource Hijacking
Kerberoasting	Permission Groups Discovery	Virtualization / Sandbox Evasion	Shared Webroot	Man in the Browser	Multi-Stage Channels			Runtime Data Manipu
LLMNR / NBT- NS Poisoning			Taint Shared Content	Screen Capture				Service Stop
Network Sniffing			Third-party Software	Video Capture				Stored Data
Password Filter DLL			Windows Admin					Transmitted
Private Keys			Windows Remote Manageme					

Two-Factor Authentication								

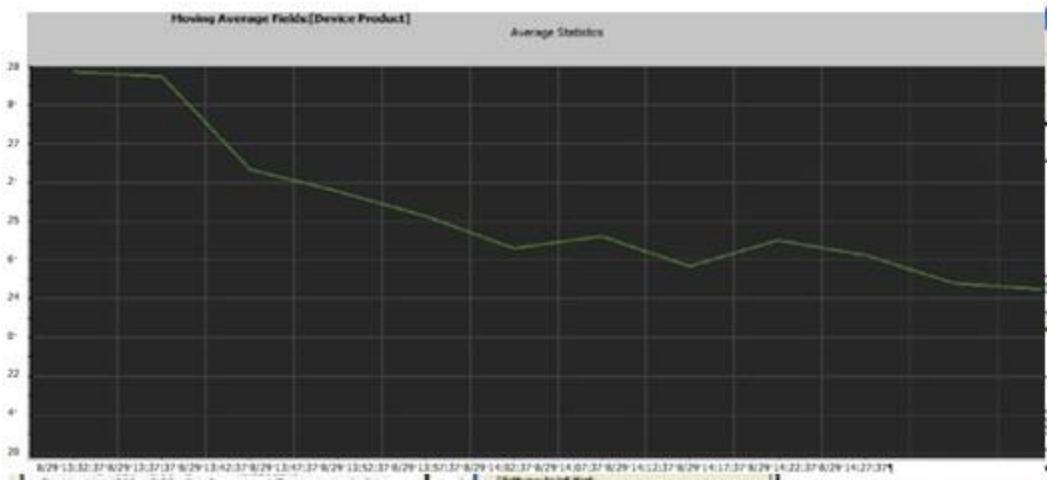
Джерело: результати власних досліджень

Основною метою використання матриці MITRE є фільтрація подій та зменшення їх кількості шляхом пошуку застосування технік у подіях на основі побудування правил на спрацювання за матрицями нижче.

На основі вивченої матриці MITRE та обраного алгоритму нечіткого пошуку Вагнера-Фішера сформовано метод аналізу ART-атак.

Основними етапами цього методу є: Фільтрація даних (події з Windows Susmon і Rowershell) шляхом виявлення за допомогою технологій MITER. Застосування алгоритму нечіткого пошуку до отриманих даних для побудови зв’язків між процесами. Створення послідовності додатків для технологій MITER і порівняння з життєвим циклом антиретровірусної атаки. Визначення хронології подій APT. Першим кроком є фільтрація даних, що є одним із найважливіших кроків. Етап фільтрації складається з просіювання даних шляхом пошуку показників використання технологій у подіях. Фільтрування даних полегшує пошук потенційно зловмисних дій серед нормальних і законних подій в інформаційній системі. В середньому кількість подій Windows Susmon і Rowershell в організації з 50 хостами становить 171 644 події, а кількість подій, що підпадають під умови застосування технологій MITER, становить 55 подій (значення отримано за період з 01.06.2022 по 01.06.2022). 2022 по 01.11.2022). Тобто різниця в обсязі даних, що підлягають обробці, колосальна – із застосуванням фільтрації кількість подій для аналізу зменшується в 3120 разів. Отже, етапом фільтрації цього методу є реалізація та пошук подій застосовуваних технологій за отриманими показниками. На рис. 2.1 показує обсяг трафіку від Windows Susmon і Rowershell в організації з 50 хостами. Етап застосування алгоритму нечіткого пошуку до отриманих даних полягає в обчисленні відстані Левенштейна рівних полів у різних подіях, зокрема цільових

процесів у подіях. Цей процес спрямований на пошук зв'язків між подіями - тобто процес, який поклав інший початок. Використання такого алгоритму виправдано тим, що процеси на різних хостах можуть мати відмінності в іменах процесів - малі або великі літери; Різниця в папках, в яких знаходиться процес, що залежить від змінних середовища в операційній системі; Спроби зловмисників змінити імена процесів (наприклад, mimikatz і mimikittenz).



Джерело: результати власних досліджень

Рис. 2.1. Об'єм трафіку від Windows Sysmon та Powershell

Наступним етапом є побудова послідовності застосування технік MITRE та співставлення із життєвим циклом APT атаки. Так як ряд технік можуть бути застосованими тільки на певних етапах APT, то є сенс у тому, щоб упорядкувати застосовані техніки згідно із життєвим циклом атаки, щоб відсіяти фальш-позитивні спрацювання. Заключним етапом є побудова хронології подій APT атаки, де описовими пунктами слугують застосовані техніки.

2.2. Етап фільтрації подій та опис індикаторів технік для фільтрації подій

Фільтрація даних була створена за допомогою застосування правил у SIEM ArcSight у даній роботі. Для написання даних правил було розглянуто техніки за

кожним напрямом MITRE, частина технік була опрацьована командою Atomic Red Team, які пропонують свої тести для перевірки систем безпеки на рівень захищеності, а також були застосовані власні тести на основі аналізу атак. Дані тести були відтворені на двох віртуальних машинах Windows 10 для отримання подій від Sysmon та Powershell.

Sysmon має достатньо різних подій, які містять спеціальний ідентифікатор під кожен тип події. У ході розгляду подій бралися до уваги такі ідентифікатори:

1. Створено новий процес;
2. Ініційована Інтернет комунікація;
3. Завантажено процесом модуль dll;
4. Створено новий файл;
5. Об’єкт реєстру був видалений/створений;
6. Задано нове значення в реєстр;
7. Створено файловий потік.
8. Виявлено DNS запит.

Деякі технології MITRE лише частково охоплювалися тестами, не залишали подій у Susmon або взагалі не були охоплені тестами Atomis Red Team, тому додатковий аналіз атак проводився як приклади на сторінках опису технології. В результаті проведення ряду робіт з тестування технологій у віртуальному середовищі отримано показники сумісності (IoS) для кожної з тестованих технологій. Оскільки ці покажчики можна використовувати в інших системах SIEM або аналізаторах подій, імена змінних є глобальними та зрозумілими, а не залежними від служби. [44]:

– TargetProcessName (TPN) – назва цільового процесу;
– SysmonEventID (SEID) – ідентифікатор події в Sysmon;
– PE (PE) – подія із powershell;
– Command Line (CMD:) – командний рядок;
– Source Process Name (SPN:) – назва процесу джерела;

– Parent Process Cmd Line (PPCMD:) – командний рядок батьківського процесу;
– Parent Process Path (PPP:) – місцезнаходження батьківського процесу;
– File Path (FP:) – місцезнаходження процесу;
– Loaded Module Name (DLL:) – завантажена бібліотека із розширенням. dll;
– Request Method (RM:) – метод запиту;
– Target Object Path (TOP:) – папка цільового об’єкту;
– «-» – пусте значення.

Під час реалізації етапу фільтрації було написано правила (Rules) у SIEM системі. Приклад умов спрацювання правила показано на рис. 2.2.

Джерело: результати власних досліджень

Рис. 2.2. Приклад умов правила

Загалом було створено 209 правил для 124 технік (більшість технік здійсненні різними шляхами, тому відбувався розподіл правил за типами реалізації техніки та типом подій).

Типи подій у правилах об’єднувалися в основні групи: registry event (події Sysmon 12, 13), process event (події Sysmon 1, 11, 15), network event (події Sysmon 3, 22), module loaded (події Sysmon 7), powershell event (події Powershell). За типами подій правила були розділені та отримані: 36 правил на основі події реєстрації, 114 правил на основі події процесу, 19 правил на основі події мережі, 5 правил на основі завантаженого блоку та 34 правила на основі події. на подію круглого снаряда. Тактика початкової оцінки припускає, що зловмисник має намір скомпрометувати цільову систему, використовуючи вразливості та слабкі місця, виявлені на загальнодоступних серверах, надсилаючи шкідливі посилання

чи файли поштою та використовуючи реальні облікові записи, які були раніше вкрадені. Всього тактик 11, але при їх аналізі виникла складність, що більшість технік підлягають такій реалізації, яку можна легко замаскувати під звичайну діяльність, а подій, що містять Susmon і Rowershell, недостатньо для її виявлення. Є загальні випробування двох технологій, одна наша власна, а друга – команда Atomic Red. З решти 9 методів до 5 не мають представлення в подіях Windows у жодному розділі, а лише залишають сліди в подіях мережі. Технологія, запропонована Atoms - Shrearfishing attachment - була протестована, але слідів її використання не виявлено, тому в контексті цієї тактики була протестована інша технологія - зовнішні віддалені сервіси - своїми тестами. Особливістю цієї технології є моніторинг використання послуг віддаленого доступу в неробочий час. Опис її індикаторів представлені нижче у таб. 2.3.

Таблиця 2.3

Тактика «Початковий доступ» (Initial Access) – індикатори компрометації для технік

Техніка	TPN	Інші змінні	SEID / PE
T1133 External Remote Services		FP: OR Contains «citrix. exe», «vpn» Time is before and after work hours	1,11,15,3, 22

Джерело: результати власних досліджень

Тактика «Виконання (Execution)» описує застосування зловмисниками доступних їм засобів і методів віддаленого і локального виконання різних команд, сценаріїв і виконуваних файлів у цільовій системі, які були доставлені в неї на попередньому етапі. Всього дана тактика містить 27 відомих технік для застосування, із яких 6 технік залишилися без покриття тестами.

Із представленої нижче таб. 2.3 було застосовано тести від Atomic Red Team для 18 технік (із них 8 технік доповнені індикаторами на основі

проаналізованих атак), 4 техніки були повністю покриті власними тестами. Із виявленими індикаторами можна ознайомитися у таб. 2.4.

Тактика «Постійність (Persistence)» складається із технік, які супротивники використовують, щоб утримати доступ до систем під час перезавантаження, зміни облікових даних та інших перебоїв, які можуть скасувати їх доступ до цільової системи. Методи, що застосовуються для цієї тактики, включають будь-які зміни доступу, дій чи конфігурацій, які дозволяють їм підтримувати свою присутність у системах.

Таблиця 2.4

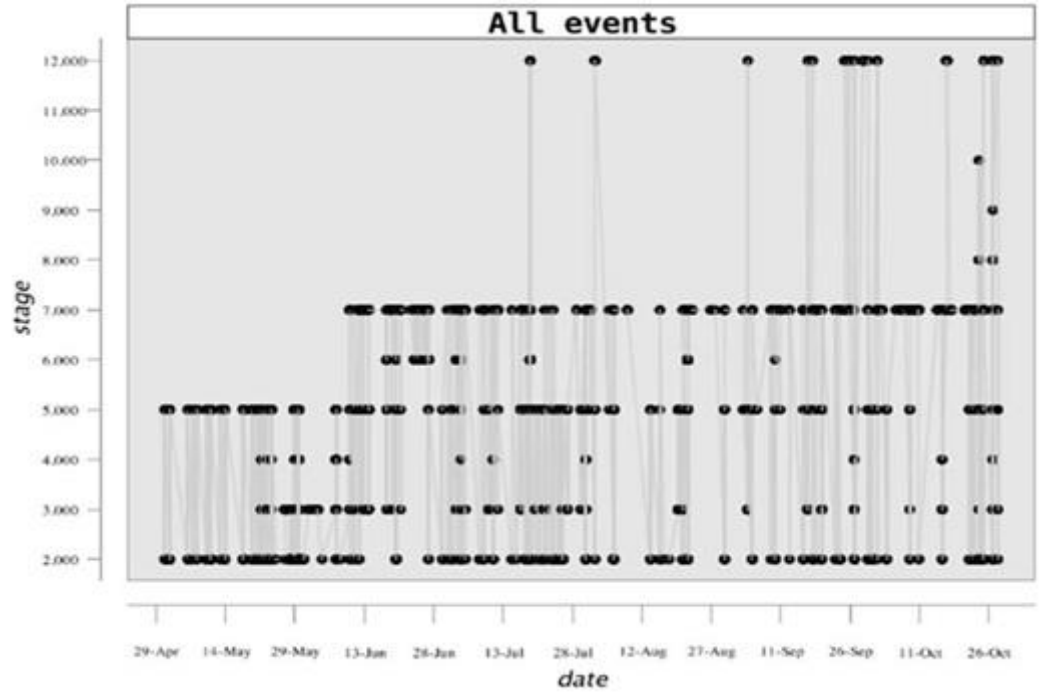
Тактика «Виконання» (Execution) – індикатори компрометації для технік

Техніка	TPN	Інші змінні	SEID / PE
T1191 CMSTP	cmstp. exe	CMD: OR Contains « /s», «.bat»	1, 11, 15
	cmstp. exe	-	1, 11, 15
	cmstp. exe	-	3
T1059 CommandLine Interface	cmd. exe	SPN: NOT Is «explorer. exe» FP: NOT Is NULL AND NOT Is ««c: / Ywindows // system32 // cmd. exe»», ««c: / Ywindows // syswow64 // cmd. exe»»	1
T1223 Compiled HTML File	hh. exe	CMD: OR Contains «hh. exe», «hh», «.bat»	1, 11, 15
	hh. exe	-	1, 11, 15
	hh. exe	-	3
T1173 Dynamic Data Exchange		TOP: Contains «AllowDDE» AND Contains «2» TOP: Contains «HKEY_CURRENT_USER / Software / Microsoft / Offic e/» AND Contains « /Word / Security»	12, 13
T1118 InstallUtil	installutil. exe	CMD: OR Contains «installutil. exe», «installutil», «.bat»	1, 11, 15
	-	SPN: installutil. exe	1, 11, 15
T1177 LSASS Driver		CMD: NOT IS «dword (0x00000001)» PPCMD: EndsWith «SYSTEM // CurrentControlSet // Control // Lsa // RunAs PPL» FP: EndsWith «lsass. exe»	12, 13
	-	FP: EndsWith «lsass. exe»	7
T1170 Mshta	mshta. exe	CMD: OR Contains «mshta. exe», «mshta», «.bat»	1, 11, 15
	mshta. exe	CMD: Contains «javascript:»	1, 11, 15
	-	SPN: mshta. exe	1, 11, 15
	mshta. exe	–	3
T1086 Powershell		CMD: OR Contains: «-noprofile», «-windowstyle hidden», «-executionpolicy bypass», «UTF8», «Base64», «-nop», «-w hidden», «-e», «- EncodedCommand», «Invoke-Expression»	PE
T1121 Regsvcs / Regasm	regsvcs. exe / regasm. exe	CMD: OR Contains: «regsvcs. exe», «regsvcs», «regasm. exe», «regasm», «.bat»	1, 11, 15
	regsvcs. exe / regasm. exe	CMD: false	7
T1117 Regsvr32	regsvr32. exe	CMD: OR Contains: «regsvr32. exe», «regsvr32», «.bat» RM: NOT Is «trusted»	1, 11, 15
	!=regsvr32. exe	SPN: regsvr32. exe	1, 11, 15
	regsvr32. exe	–	3
	regsvr32. exe	CMD: Contains «/i:»,	1, 11, 15, 3
	rundll32. exe	CMD: Contains «javascript:»	1, 11, 15

T1085	rundll32. exe	–	3
T1053 Scheduled Task	at. exe	CMD: Contains «/interactive»	1, 11, 15
	–	CMD: AND Contains: «SCHTASKS», «/interactive», «/Create», «/ST», «/TR»	1, 11, 15
T1064 Scripting	wmic. exe	CMD: Contains «.xsl»	1, 11, 15
	rundll32. exe	CMD: Contains «.sct»	1, 11, 15
	wscript. exe /cscript. exe	CMD: OR Contains: «.vbs», «wsc», «.wsf», «.wsh», «.vbe»	1, 11, 15
	–	CMD: OR Contains «.psdl», «.psml», «.psl»	PE
T1035 Service Execution	sc. exe	CMD: OR Contains «create», «delete», «config», «.bat»	1, 11, 15
T1216 Signed Script Proxy Execution	cscript. exe	–	1, 15
	cscript. exe	–	3
	cscript. exe	CMD: Contains «pubprn. vbs»	1, 15
T1127 Trusted Developer Utilities	msbuild. exe/ dnx. exe / rcsi. e	CMD: OR Contains «», «.bat»	1, 11, 15
	–	SPN: msbuild. exe, dnx. exe, rcsi. exe, windbg. exe, cdb. exe)	1, 15
T1047 Windows Management Instrumentation	-	SPN: wmic. exe	1, 15
	wmic. exe	CMD: OR Contains «useraccount», «.bat», «process», «qfe», «/node»	1, 11, 15
	wmic. exe	-	3
T1028 Windows Remote Management	-	CMD: Contains «Enable-PSRemoting»	PE
	powershell. ex e	CMD: AND Contains «createinstance», «MMC20. application», «gettypefromprogid»	PE
	wmic. exe	SPN: cmd. exe CMD: Contains «process call create»	1, 15
	-	CMD: Contains «gettypefromprogid»	PE
T1220 XSL Script Processing	msxsl. exe	CMD: OR Contains «msxsl. exe», «msxsl», «.bat»	1, 11, 15
	-	SPN: msxsl. exe	1, 15
	msxsl. exe	-	3
	wmic. exe	CMD: OR Contains «xsl», «/format:», «.bat»	1, 11, 15

Джерело: результати власних досліджень

Всього ця тактика містить 43 техніки. З цих методів 8 не охоплюються жодними тестами (3 з них залишають події лише для мережевих інструментів і пристроїв). Всього було охоплено випробуваннями, а потім правилами роботи за показаннями 33 методики.



Джерело: результати власних досліджень

Рис. 2.3. Графік послідовності застосування методу виявлення кібератак на основі індикаторів компрометації на початковому етапі (пошук максимальної кількості індикаторів компрометації за мінімальної кількості ТІ)

Якщо виділити ті технології, які раніше зустрічалися в інших тактиках, то Atomis Червона команда пропонує тести для 25 технологій. З них 1 техніка не залишила слідів у відповідних подіях, а 3 техніки доповнюються виявленими індикаторами атак. Також були запропоновані тести для 9 інших технологій. Про виявлені показники тактичних прийомів наполегливості ви можете дізнатися в таб. 2.5.

Таблиця 2.5

Тактика Постійність (Persistence) – індикатори компрометації для технік

Техніка	TPN	Інші змінні	SEID / PE
T1015 Accessibility Features	cmstp. exe	TOP: Contains «debugger» AND TOP: OR Contains «osk», «sethc», «utilman», «magnify», «narrator», «displayswitch», «atbroker» AND TOP: OR Contains «/software / microsoft / windows nt / currentversion / image file execution options/», «/software / wow6432node / microsoft / windows nt / currentversion / image file execution options/»	12, 13
T1098 Account Manipulation		CMD: OR Contains: (AND Contains «$member», «-like», «Rename- LocalUser -Name», «admin»), (AND Contains «Get-CimInstance -ClassName», «Filter», «Rename-LocalUser -Name»)	PE
T1182 AppCert DLLs		TOP: Contains «System / CurrentControlSet / Control / Session Manager / KnownDLLs»	12, 13
T1103 AppInit DLLs		TOP: Contains «appinit_dlls» TOP: OR Contains «software / microsoft / windows nt / currentversion / windows», «software / wow6432node / microsoft / windows nt / currentversion / windows»	12, 13
T1138 Application Shimming	sdbinst.	CMD: OR Contains «sdbinst. exe», «.bat», «sdbinst»	1, 11, 15
		TOP: Contains «appinit_dlls» TOP: OR Contains «hklm / software / microsoft / windows nt / currentversion / appcompatflags / installedsdb», «hklm / software / microsoft / windows nt / currentversion / appcompatflags / custom»	12, 13
T1131 Authentication Package	reg. exe	CMD: Contains «HKLM / SYSTEM / CurrentControlSet / Control / Lsa / A uthentication Packages»	12, 13
T1197 BITS Jobs	bitsadmin . exe	CMD: OR Contains «bitsadmin. exe», «.bat», «bitsadmin»	1, 11, 15
	-	CMD: Contains «Start-BitsTransfer»	PE
T1176 Browser Extensions		FP: «c: / program files (x86) /google / chrome / application / chrome. exe» TOP: Contains «AppData / Local / Google / Chrome / User Data / Default / Extensions»	1, 22, 3, 15
T1042 Change Default File Association	cmd. exe	CMD: Contains «assoc»	1, 15, 11

T1122 Component Object Model Hijacking		AND: TOP: Contains «/inprocserver32» TOP: OR Contains «hkcu / software / classes / dsid/», «hklm / software / dasses / clsid/», «hkcr / clsid/» (OR CMD: Contains «scrobj», (AND CMD: Contains «://», PM: NOT trusted, not available)))	13
T1136 Create Account	net. exe	CMD: AND Contains «user», «/ad»	1, 15, 11
	net1. exe	CMD: AND Contains «user», «/ad» SPN: NOT Is «net. exe»	1, 15, 11
	-	CMD: AND Contains «New-LocalUser», «-Name»	PE
T1038 DLL Search Order Hijacking		TOP: Contains «c: / temp»	7
T1158 Hidden Files and Directories	attrib. exe	CMD: OR Contains «+s», «.bat», «+h»	1, 15, 11
T1179 Hooking	mavinject . exe	CMD: Contains «/injectrunning»	1, 11, 15, 7, 3
T1062 Hypervisor		CMD: Contains «Hyper-V» CMD: OR Contains «Install-WindowsFeature», «Get-WindowsFeature»	PE
T1037 Logon Scripts	reg. exe	CMD: AND Contains «hkcu / environment», «userinitmprlogonscript»	1, 12, 13
T1031 Modify Existing Service	sc. exe	CMD: OR Contains «config», «binPath=»	1, 15, 11
T1128 Netsh Helper DLL	netsh. exe	CMD: AND Contains «add helper», «.dll»	1, 15, 11
	netsh. exe	TOP: Contains «/SOFTWARE / Microsoft / NetSh»	12, 13
T1050 New Service	sc. exe	SPN: cmd. exe CMD: OR Contains «create», «start», «stop», «delete»	1, 15, 11, 7
		CMD: OR Contains «New-Service», «Start-Service», «Stop-Service», («Get-WmiObject Win32 Service» AND «.DeleteQ»)	PE
T1137 Office Application Startup		SPN: OR Contains «winword. exe», «powerpnt. exe», «excel. exe» PPP: OR Contains «fastprox. dll», «wbemcomn. dll», «wbemdisp. dll», «wmiutils. dll»	7
	rundll32. exe	SPN: svchost. exe CMD: OR Contains «c08afd90-f2a1–11d1–8455–00a0c91f3880», «9BA05972-F6A8–11CF-A442–00A0C90A8F39»	1, 15, 11, 12, 13
T1060 Registry Run Keys / Startup Folder	reg. exe	CMD: OR Contains «SOFTWARE / Microsoft / Windows / CurrentVersion / Run», «SOFTWARE / Microsoft / Windows / CurrentVer sion / RunOnceEx»	1, 12, 13
T1180 Screensaver	reg. exe	CMD: Contains «/control panel / desktop» CMD: OR Contains «ScreenSaveActive», «ScreenSaverTimeout», «ScreenSaverlsSecure»	12, 13
	-	CMD: Contains «not-a-ssp»	1, 15

T1101 Security Support Provider	–	CMD: AND Contains «-ExpandProperty», «Security Packages»	1, 15
		CMD: AND Contains «Get-ItemProperty HKLM: / System / CurrentControlSet / Control / Lsa», «Security Packages»	1, 15
T1058 Service Registry Permissions Weakness		TOP: Contains «HKEY_LOCAL_MACHINE / SYSTEM / CurrentCon trolSet / services» TOP: OR Contains «FailureActions», «FailureCommand»	12, 13
T1084 WMI Event Subscription		CMD: OR Contains «New-CimInstance», «EventFilter», « FilterToConsumerBinding», «CommandLineEventConsumer», «Remove-WmiObject», (« InstanceModificationEvent» AND Contains «Query)	PE
T1004 Winlogon Helper DLL	powershell. exe / reg. exe	AND (CMD: Contains «Software / Microsoft / Windows NT / CurrentVersion / Winlogon / Notify» OR TOP: Contains «Software / Microsoft / Windows NT / CurrentVersion / Winlogon / Notify») TON: OR Contains «logon», «cmd. exe»	1, 12, 13
	powershell. exe / reg. exe	AND (CMD: Contains «software / microsoft / windows nt / currentversion / winlogon / shell» OR TOP: Contains «software / microsoft / windows nt / currentversion / winlogon / shell») TON: OR Contains «shell», «cmd. exe»	1, 12, 13
	powershell. exe / reg. exe	AND (CMD: Contains «software / microsoft / windows nt / currentversion / winlogon / shell» OR TOP: Contains «software / microsoft / windows nt / currentversion / winlogon / shell») TON: OR Contains «userinit», «cmd. exe»	1, 12, 13

Джерело: результати власних досліджень

Тактика «Підвищення привілеїв (Privilege Escalation)» налічує 21 техніку, із яких 5 не були покриті ніякими тестами. 16 технік мають покриття із тестів та правил на спрацювання. Atomic Red Team забезпечила 11 тестів для технік, 2 із них без отриманих подій, частина технік була доповнена тестами на основі відомих індикаторів атак, інші ж 5 тестів були повністю покриті власними тестами та опрацьовані для отримання індикаторів. Перелік індикаторів технік тактики Підвищення привілеїв описано у таб. 2.6.

Таблиця 2.6

Тактика «Підвищення привілеїв (Privilege Escalation)» – індикатори компрометації

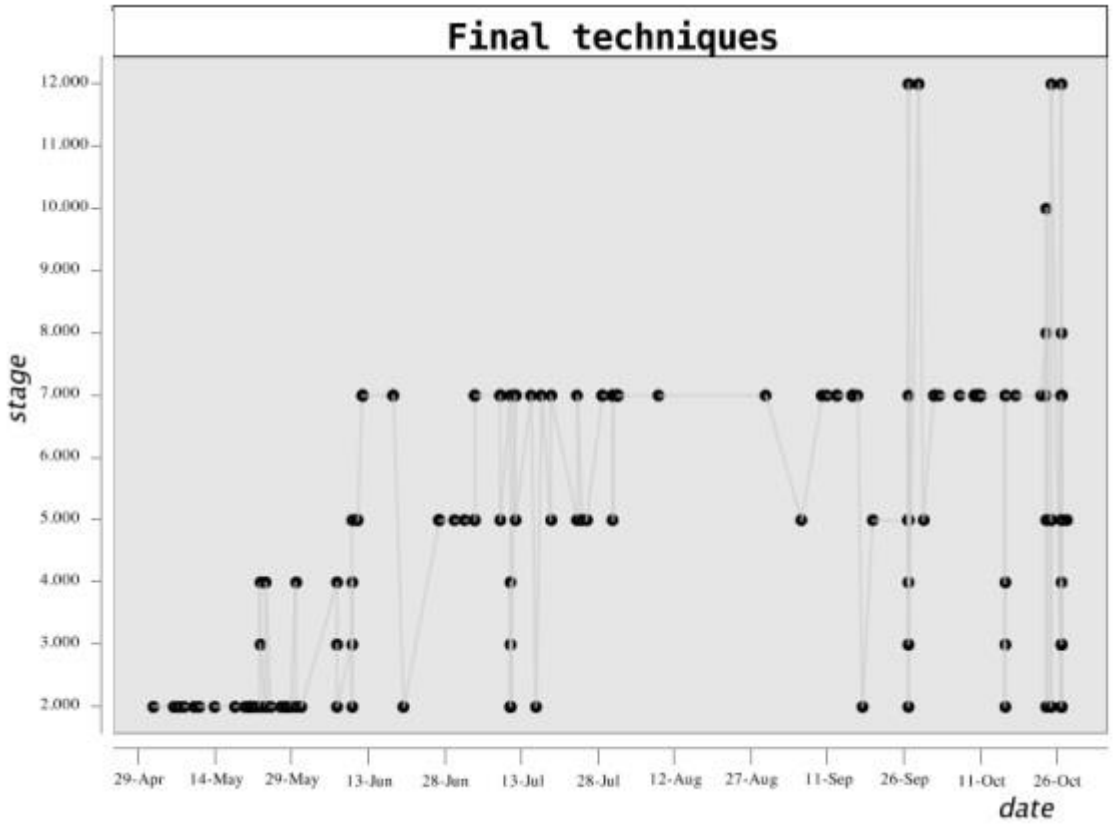
Техніка	TPN	Інші змінні	SEID / PE
T1088 Bypass User Account Control	powershell. exe / reg. exe	CMD: Contains «mscfile / shell / open / command» OR TOP: Contains «mscfile / shell / open / command»	1, 12, 13
	powershell. exe / reg. exe	(CMD: Contains «ms-settmgs / shell / open / command» OR TOP: Contains «ms- settings / shell / open / command») AND (CMD: Contains «m fodhelper. exe» OR TOP: Contains «fodhelper. exe»)	1, 12, 13
T1055 Process Injection	-	CMD: Contains «etc / ld. so. preload»	1, 15, 11
	–	CMD: OR Contains «-ProcessID», «Invoke-Dll», «Dll»	1, 15, 11
T1178 SID-History Injection		CMD: OR Contains «sIDHistory», «Get-ADUser»	PE

Джерело: результати власних досліджень

У тактиці «Обхід захисту (Defense Evasion)» описано методи які зловмисник може використати, щоб приховати зловмисну діяльність і запобігти виявленню засобами захисту. Варіанти прийомів інших тактик нападу, які допомагають подолати конкретні засоби захисту та запобіжні заходи, включені до методів обходу захисту. Навпаки, техніка обходу захисту використовується на всіх етапах атаки.

Всього ця тактика містить 57 прийомів, причому з деякими прийомами зустрічалися раніше, тому в таблиці 3.5 наведено ті прийоми, які зустрічаються вперше. 14 техніків залишилися без тестового покриття, 4 з них лише залишили сліди в мережевих подіях.

Команда Atomis Red Team надала 31 тест техніки, 2 з яких були без отриманих подій, частина методик була доповнена тестами на основі відомих індикаторів атак, а інші 12 тестів були повністю охоплені власними тестами та оброблені для отримання показників . 12 техніків з команди Atom Red також отримали нові індикатори, які не були виявлені під час їх тестування.



Джерело: результати власних досліджень

Рис. 2.4. Хронологія APT атаки з використанням методу виявлення кібератак на основі індикаторів компрометації

У таблиці 2.7 подані індикатори для виявлення застосування технік у розрізі даної тактики «Обхід захисту».

Під час тактики «Доступ до облікових даних (Credential Access)», отримавши облікові дані, зловмисник отримує доступ або навіть контроль над системою, доменом або службовими (технологічними) обліковими записами. Противник, ймовірно, буде намагатися дістати легітимні облікові дані користувача і адміністративних облікових записів, щоб ідентифікуватися в системі і отримати всі дозволи захопленого облікового запису, тим самим ускладнюючи процес виявлення його зловмисної активності. Противник також може створювати облікові записи з метою їх подальшого використання у цільовому середовищі.

Таблиця 2.7

Тактика Обхід захисту (Defense Evasion) – індикатори компрометації

Техніка	TPN	Інші змінні	SEID / PE
T1500 Compile After	csc. exe	CMD: OR Contains «.exe», «.dll» AND CMD Contains «.cs»	1, 15, 11
T1140 Deobfuscate /	-	CMD: OR Contains «copy», «certutil. exe»	1, 15, 11
	certutil. exe	CMD: OR Contains «-encode», «-decode»	1, 15, 11
T1089 Disabling Security Tools	appcmd. exe	CMD: OR Contains «set config»,	1, 15, 11
	fltmc. exe	CMD: OR Contains «unload», «sysmon»	1, 15, 11
	–	CMD: Contains «Set-MpPreference –	PE
	sc. exe	CMD: OR Contains «stop WinDefend»,	1, 15, 11
		Value: Contains «1» TOP: OR Contains «SOFTWARE / Policies /	12, 13
T1107 File Deletion	vssadmin. exe	CMD: Contains «delete»	1, 15, 11
	–	CMD: AND Contains «-path», «Remove-Item»	PE
T1222 File Permissions	takeown. exe/		1, 15, 11
	attrib. exe	CMD: Contains «-r»	1, 15, 11
T1484 Group Policy	–	CMD: Contains «New-GPOImmediateTask»	PE
	–	CMD: Contains «MACHINE / Microsoft /	1, 15, 11
T1070 Indicator	wevtutil. exe	CMD: Contains «delete» AND CMD: Contains	1, 15, 11
	fsutil. exe	CMD: AND Contains «delete», «usn»,	1, 15, 11
T1202 Indirect	forfiles. exe	-	1, 15, 11

Джерело: результати власних досліджень

Всього існує 16 технік, із яких 4 техніки без покриття тестами. Було використано 11 вже готових тестів для технік, розроблено для однієї техніки тести, а також допрацьовано існуючі техніки для покращення ефективності знаходження слідів потенційно зловмисної активності із обліковими записами. У

таблиці 2.8 подані індикатори для виявлення застосування технік у розрізі даної тактики.

Таблиця 2.8

Тактика «Доступ до облікових даних (Credential Access)» – індикатори компрометації для технік

Техніка	TPN	Інші змінні	SEID / PE
T1110 Brute	–	CMD: AND Contains «in», «net use», «for / f»,	1, 15, 11
T1003 Credential Dumping		CMD: OR Contains «gsecdump», «wce. exe», «procdump. exe», «ntdsutil», «vssadmin create	1, 15, 11, 3
	–	CMD: AND Contains «Invoke-Mimikatz», «-	PE
	-	CMD: OR Contains «reg save HKLM / sam»,	12, 13
T1081 Credentials in	–	CMD: Contains «Invoke-mimikittenz»	PE
	–	CMD: AND Contains «select-string», «-	PE
	–	CMD: AND Contains «findstr / si», «pass»	PE
T1214 Credentials in	reg. exe	CMD: AND Contains «password», «query», « /f»	1, 15, 11, 12, 13
T1056 Input	–	CMD: AND Contains «Get-Keystrokes», «-	PE
T1141 Input Prompt		CMD: AND Contains «GetNetworkCredential(). Password»,	PE
T1171 LLMNR /		TOP: AND Contains «HKLM / Software / Policies / Microsoft / Windows NT /	12, 13
T1040 Network	tshark. exe / du		1, 15, 11
T1174 Password		TOP: AND Contains «SYSTEM / CurrentControlSet / Control / Lsa/»,	12, 13
T1145 Private	–	CMD: OR Contains «cert. key», «.key»	1, 15, 11

Джерело: результати власних досліджень

Отримавши в результаті первинної компрометації доступ в систему, противник розгортає діяльність по вивченню цільової системи та відслідковує

можливості, які у нього з’явилися, і дізнається, чи достатньо поточних прав для досягнення тактичної або кінцевої мети. Цей етап атаки називається «Виявлення» (Discovery).

Операційні системи мають багато вбудованих інструментів, які дозволяють зловмиснику досліджувати внутрішній периметр цільової мережі після її зламу. У Windows для збору інформації можна використовувати засоби прямої взаємодії з функціями WMI, WMI та RoverShell. Зловмисник використовує методи виявлення під час вивчення навколишнього середовища, тому виявлення такої активності слід розглядати як частину атаки, яка супроводжуватиметься спробами просування супротивника через мережу [41]. Всього в цій тактиці є 22 прийоми, і всі ці прийоми були розглянуті в тестах. Серед них 18 технологій були розроблені командою Atomis Red і частково доповнені новими показниками, а інші чотири технології були розроблені самостійно. У таб. 2.9 подані індикатори для виявлення застосування технік у розрізі «Виявлення».

Тактика «Переміщення в мережі (Lateral Movement)» включає методи отримання противником доступу і контролю над віддаленими системами, підключеними до цільової мережі, а також для запуску шкідливих інструментів на віддалених системах. Переміщення в мережі дозволяє зловмисникові отримувати інформацію з віддалених систем без використання додаткових інструментів. Всього описано 17 можливих технік, із них 7 було не покрито тестами. Atomic Red Team створила тести для 6 технік, 1 техніка не залишила слідів у подіях, 4 із цих технік були доповнені новими індикаторами, також додатково 2 теста був розроблений самостійно. У таб. 2.10 подані індикатори для виявлення застосування технік у розрізі даної тактики.

Таблиця 2.9

Тактика «Виявлення (Discovery)» – індикатори компрометації

Техніка	TPN	Інші змінні	SEID / PE
T1087 Account Discovery	net1. exe /	CMD: OR Contains «user», «localgroup»	1, 15, 11
	-	CMD: Contains «query user»	PE
	-	CMD: Contains «cmdkey. exe»	PE
		(CMD: OR Contains «net», «get – «, «get») AND (CMD: OR Contains «user»,	PE
T1010 Application Windows	csc. exe / cvtres exe	CMD: Contains «-out:»	1, 15, 11
T1217 Browser Bookmark Discovery		CMD: OR Contains «AppData / Local / Packages / Microsoft. MicrosoftEdge _8wekyb3d8bbwe / AC / MicrosoftEdge / User / Default/ DataStore / Data ouser1 / 120712–0049 / F avorites»	1, 15, 11
T1482 Domain	nltest. exe	CMD: Contains «/domain trusts»	1, 15, 11
	dsquery. exe	CMD: Contains «/domain_trusts»	1, 15, 11
T1083 File and	–	CMD: Contains «-recurse» AND	PE
	tree. com	-	1, 15, 11
T1046 Network Service	telnet. exe / Co		1, 15, 11, 3
	-	CMD: Contains «Get-Service»	PE
T1135 Network	net. exe	CMD: Contains «view »	1, 15, 11, 3
T1201 Password Policy	net1. exe / net. e xe	CMD: Contains «accounts»	1, 15

Джерело: результати власних досліджень

Таблиця 2.10

Тактика «Переміщення в мережі (Lateral Movement)» – індикатори компрометації для технік

Техніка	TPN	Інші змінні	SEID / PE
T1037 Logon	reg. exe	CMD: AND Contains «hkcu / environment»,	1, 12, 13
T1076 Remote	–	CMD: AND Contains «tscon», «rdp-tcp#»	1, 15, 3
T1105 Remote	certutil.	CMD: Contains «-urlcache -split -f»	1,15, 11, 3
	-	CMD: AND Contains «certutil», «verifyctl -	PE
T1021 Remote	–	FP: OR Contains «putty», «vncviewer. exe»	1, 15, 3
T1077 Windows	-	CMD: AND Contains «admin», «net use»	1, 15
Admin Shares	–	CMD: AND Contains «New-PSDrive»,	PE

Джерело: результати власних досліджень

Тактика «Збір даних (Collection)» ті її методи збору даних у вразливому середовищі включають методи безпосередньої ідентифікації, визначення місцезнаходження та збору цільової інформації (наприклад, конфіденційних файлів), щоб підготувати її до подальшого проникнення.

Опис методів збору інформації також охоплює опис місць зберігання інформації в системах або мережах, де зловмисники можуть її шукати та збирати. Показаннями для впровадження більшості технологій збору даних, представлених в ATT&SK, є операції, які використовують ARI, WMI, PoVERShel, Cmd для захоплення цільової інформації з пристроїв введення-виведення або відкриття кількох файлів для читання з подальшим копіюванням отриманих даних у певне місце в файлова система або мережа. Інформація може бути зашифрована під час збору даних і об'єднана в архівні файли.

Всього 13 технологій, лише 6 з них пройшли випробування та правила експлуатаціїУ таблиці 2.11 подані індикатори для виявлення застосування технік у розрізі збору даних.

Тактика «Командування і управління (Command and Control)» включає техніки, за допомогою яких противник зв'язується із системами, підключеними до цільової мережі і які знаходяться під його керуванням. Залежно від конфігурації систем і топології цільової мережі відомо безліч способів організації прихованого каналу С2.

Таблиця 2.11

Тактика «Збір даних (Collection)» – індикатори компрометації для технік

Техніка	TPN	Інші змінні	SEID / PE
T1123 Audio Capture	explorer. exe	CMD: AND Contains «.wma», «shell:	1, 15, 11
	powershell.	CMD: Contains «-command	1, 15, 11
T1119 Automated Collection	-	CMD: AND Contains «for / R», «%f in», «do	1, 15, 11
	-	CMD: AND Contains « », «findstr / e», «dir c:	1, 15, 11
	-	CMD: AND Contains «Get-ChildItem -Recurse	PE
T1115	clip. exe	PPP: OR Contains «cmd. exe», «powershell.	1, 15, 11

Джерело: результати власних досліджень

Всього налічується 21 техніка, але покриття правилами було застосоване тільки до 4 із них, із решти не покритих тестами 8 технік містяться тільки у подіях мережевих засобів. 3 техніки із тестами були взяті у Atomic Red Team, 1 тест для техніки опрацьовано власноруч. У таблиці 2.12 подані індикатори для виявлення застосування технік у розрізі даної тактики.

Тактика «Просочення даних (Exfiltration)» або ж «Вилучення даних» описує техніки передачі даних, що застосовуються зловмисниками або шкідливим ПЗ для вилучення, крадіжки, витоку цільової інформації із скомпрометованої системи для досягнення поставленої цілі. Техніки, які застосовуються у цій тактиці, достатньо складні та не завжди підлягають універсалізації, тому для індикаторів було обрано ряд команд, які потенційно

можуть бути застосованими для різних ситуацій і є максимально універсальними.

Таблиця 2.12

Тактика «Командування і управління (Command and Control)» – індикатори компрометації для технік

Техніка	TPN	Інші змінні	SEID / PE
T1219 Remote Access Tools		FP: OR Contains «TeamViewer. exe», «Ammyy_Service. exe», «GoToAssist. exe»,	1, 15
T1071 Standard Application Layer Protocol	–	CMD: AND Contains «Get-Random -	PE
	–	CMD: AND Contains «-Domain», «-	PE
	–	CMD: AND Contains «-Domain», «-	PE
	–	CMD: AND Contains'Invoke-WebRequest»,	PE
T1065 Uncommonly		CMD: AND Contains «-ComputerName», «-port» AND CMD: NOT Contains 25, 80, 443,	PE

Джерело: результати власних досліджень

Усього було виявлено 9 технік, із яких 3 були покриті правилами на спрацювання у SIEM системі і протестовані у тестовому середовищі для збору подій та отримання індикаторів протестованих технік. У таб. 2.13 подані індикатори, за якими здійснювалося виявлення застосування технік у розрізі даної тактики. Із таблицею можна ознайомитися нижче.

Тактика «Вплив (Impact)» – остання стадія у розрізі життєвого циклу APT атаки – складається із технік, які супротивники використовують для порушення доступності або порушення цілісності системи, маніпулюючи бізнес- та операційними процесами. Методи, що застосовуються для впливу, можуть включати знищення чи підробку даних.

Усього існує 14 технік, із яких 4 техніки було опрацьовано та отримано для них події із індикаторами, що можуть говорити про потенційно зловмисну активність, решта 6 технік залишають сліди тільки у подіях мережевих засобів і не можуть бути викриті через sysmon і powershell події, тому дані техніки залишилися без покриття індикаторами та правилами на спрацювання у SIEM.

Таблиця 2.13

Тактика «Просочення даних (Exfiltration) «– індикатори компрометації

Техніка	TPN	Інші змінні	SEID / PE
T1002 Data Compressed	rar. exe	CMD: Contains «r »	1, 11, 15
	–	CMD: Contains «Compress-Archive –	PE
T1022 Data Encrypted	rar. exe	CMD: Contains «-hp»	1, 11, 15
	winzip64. exe	CMD: Contains «-s»	1, 11, 15
	7z. exe	CMD: Contains «-p»	1, 11, 15
T1048 Exfiltration Over	–	CMD: Contains «System. Net.	PE
		CMD: AND Contains «-Encoding Byte – ReadCount», «Get-Content -Path», «.Send»	PE

Джерело: результати власних досліджень

У таблиці 2.14 подані індикатори для виявлення застосування технік у розрізі даної тактики Вплив, із якими можна ознайомитися нижче. Індикатори було максимально універсалізовано.

Таблиця 2.14

Тактика «Вплив (Impact)» – індикатори компрометації

Техніка	TPN	Інші змінні	SEID /
T1485 Data	–	CMD: Contains «sdelete. exe»	1, 11, 15
T1490 Inhibit System		CMD: OR Contains «wmic. exe shadowcopy delete», «vssadmin. exe delete shadows / all / quiet», «rdp-	1, 11, 15
T1488 Disk Content Wipe_registry	reg. exe	TOP: OR Contains «System / CurrentControlSet / Control / SystemBootDevice», «System / CurrentControlSet / Control /	12, 13
T1489 Service Stop	sc. exe	CMD: Contains «stop»	1, 15
	net. exe	CMD: Contains «stop»	1, 15
	taskkill.	CMD: Contains «/f / im»	1, 15

Джерело: результати власних досліджень

2.3. Програмна реалізація етапів розробленого методу

Для реалізації таких етапів методу як: побудова зв’язків між процесами за допомогою алгоритму нечіткого пошуку, побудова послідовності застосування технологій MITRE та порівняння з життєвим циклом атаки APT, визначення хронології подій APT – розроблено спеціальний додаток на мові програмування Java з використанням бібліотек XChart A Grarhstream і Apache CSV для зчитування даних і подальшого їх графічного відображення. На виході робочого процесу програми формуються графіки з хронологією APT і списком пов’язаних подій [42].

Всього були створені такі класи (див. додаток роботи): Chart. java, Eventjava, EventGraph. java, BuildAPTjava, IdTechniquesjava, Levensteinjava, ParserCsv. java, Tacticsjava, TechniqueChartjava, Techniquesjava. Головним класом є BuildAPTjava, у якому відбувається запуск функцій для реалізації усіх алгоритмів відбору даних. На рис. 2.5 представлена UML діаграма класів розробленого застосунку.

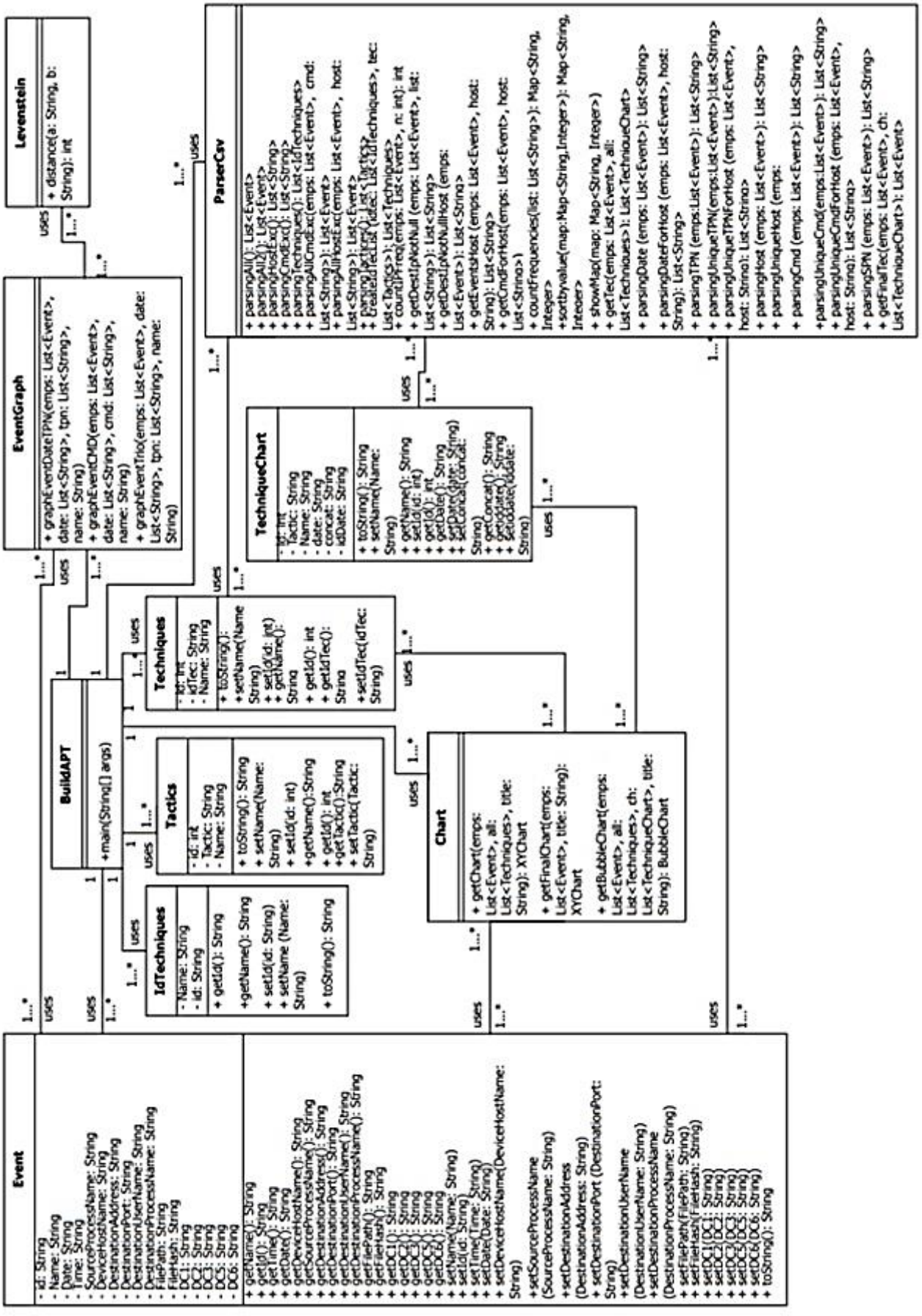

Event
- id: String
- Name: String
- Date: String
- Time: String
- SourceProcessName: String
- DeviceHostName: String
- DestinationAddress: String
- DestinationPort: String
- DestinationUserName: String
- DestinationProcessName: String
- FilePath: String
- FileHash: String
- DC1: String
- DC2: String
- DC3: String
- DC5: String
- DC6: String
+ getName(): String
+ getId(): String
+ getTime(): String
+ getDate(): String
+ getDeviceHostName(): String
+ getSourceProcessName(): String
+ getSourceProcessName(): String
+ getDestinationAddress(): String
+ getDestinationPort(): String
+ getDestinationUserName(): String
+ getDestinationProcessName(): String
+ getFilePath(): String
+ getFileHash(): String
+ getDC1(): String
+ getDC2(): String
+ getDC3(): String
+ getDC5(): String
+ getDC6(): String
+ setName(Name: String)
+ setId(id: String)
+ setTime(Time: String)
+ setDate(Date: String)
+ setDeviceHostName(DeviceHostName: String)
+setSourceProcessName (SourceProcessName: String)
+setDestinationAddress (DestinationAddress: String)
+ setDestinationPort (DestinationPort: String)
+setDestinationUserName (DestinationUserName: String)
+setDestinationProcessName (DestinationProcessName: String)
+ setFilePath(FilePath: String)
+ setFileHash(FileHash: String)
+ setDC1(DC1: String)
+ setDC2(DC2: String)
+ setDC3(DC3: String)
+ setDC5(DC5: String)
+ setDC6(DC6: String)
+ toString(): String
IdTechniques
- Name: String
- id: String
+ getId(): String
+getName(): String
+ setId(id: String)
+ setName (Name: String)
+ toString(): String
Tactics
- id: int
- Tactic: String
- Name: String
+ toString(): String
+ setName(Name: String)
+ setId(d: int)
+getName():String
+ getId(): int
+getTactic():String
+ setTactic(Tactic: String)
BuildAPT
+main(String[] args)
Techniques
- id: int
- idTec: String
- Name: String
+ toString(): +setName(Name String)
+ setId(id: int)
+ getName(): String
+ getId(): int
+ getIdTec(): String
+setIdTec(idTec: String)
Chart
+ getChart(emps: List<Event>, all: List<Techniques>, title: String): XYChart
+ getFinalChart(emps: List<Event>, title: String): XYChart
+ getBubbleChart(emps: List<Event>, all: List<Techniques>, ch: List<TechniqueChart>, title: String): BubbleChart
TechniqueChart
- id: int
- Tactic: String
- Name: String
- date: String
- concat: String
- idDate: String
+ toString(): String
+ setName(Name: String)
+ getName(): String
+ setId(id: int)
+ getId(): int
+ getDate(): String
+ getDate(date: String)
+ setConcat(concat: String)
+ getConcat(): String
+ getIdDate(): String
+ setIdDate(idDate: String)
EventGraph
+ graphEventDateTPN(emps: List<Event>, date: List<String>, tpn: List<String>, name: String)
+ graphEventCMD(emps: List<Event>, date: List<String>, cmd: List<String>, name: String)
+ graphEventTrio(emps: List<Event>, date: List<String>, tpn: List<String>, name: String)
ParserCsv
+ parsingAll(): List<Event>
+ parsingAll2(): List<Event>
+ parsingHostExc(): List<String>
+ parsingCmdExc(): List<String>
+ parsingTechniques(): List<IdTechniques>
+ parsingAllCmdExc(emps: List<Event>, cmd: List<String>): List<Event>
+ parsingAllHostExc(emps: List<Event>, host: List<String>): List<Event>
+ parsingTactics(): List<Tactics>
+ FreeMarkerList (date: List<IdTechniques>, tec: List<Tactics>): List<Techniques>
+ countFreq(emps: List<Event>, n: int): int
+ getDestIpNotNull (emps: List<Event>, list: List<String>): List<String>
+ getDestIpNotNullHost (emps: List<Event>): List<String>
+ getEventsHost (emps: List<Event>, host: String): List<String>
+ getCmdForHost(emps: List<Event>, host: List<String>)
+ countFrequencies(list: List<String>): Map<String, Integer>
+sortbyvalue(map:Map<String,Integer>): Map<String, Integer>
+ showMap(map: Map<String, Integer>)
+ getTec(emps: List<Event>, all: List<Techniques>): List<TechniqueChart>
+ parsingDate (emps: List<Event>): List<String>
+ parsingDateForHost (emps: List<Event>, host: String): List<String>
+ parsingTPN (emps:List<Event>): List<String>
+ parsingUniqueTPN(emps:List<Event>):List<String>
+ parsingUniqueTPNForHost (emps: List<Event>, host: String): List<String>
+ parsingHost (emps: List<Event>): List<String>
+ parsingUniqueHost (emps: List<Event>): List<String>
+ parsingCmd (emps: List<Event>): List<String>
+parsingUniqueCmd(emps:List<Event>): List<String>
+ parsingUniqueCmdForHost (emps: List<Event>, host: String): List<String>
+ parsingSPN (emps: List<Event>): List<String>
+ getFinalTec(emps: List<Event>, ch: List<TechniqueChart>): List<Event>
Levenstein
+ distance(a: String, b: String): int
uses
1...*
1

Рис. 2.5. Діаграма UML класів застосунку

Для коректного розбору даних за полями було реалізовані спеціальні типи даних. У класі Event. java описано тип даних для події, отриманої із файлу з кореляційними подіями від Sysmon та Powershell. Виділено основні характеристики події (типом даних для кожного із параметрів є String): унікальний ідентифікатор події (id), ім'я події (Name), дата (Date), час (Time), назва хосту (DeviceHostName), назва джерела процесу (SourceProcessName), адреса призначення (DestinationAddress), порт призначення (DestinationPort), ім'я цільового користувача (DestinationUserName), назва цільового процесу (DestinationProcessName), шлях до файлу (FilePath), хеш файлу (FileHash), командний рядок (DC1) або ж значення призначеного параметру у випадку події з реєстру, шлях до батьківського процесу (DC2) або ж повний шлях із назвою процесу чи сама назва, командний рядок батьківського процесу (DC3), тільки шлях до батьківського процесу (DC5), підпис бібліотеки (DC6). Крім того, для кожного з вибраних полів реалізовано по дві функції для налаштування та отримання параметра. Додатковою функцією цього класу є відображення основних параметрів події toString(). У класі IdTechniques.java реалізовано наступний тип даних, необхідний для аналізу файлу, що містить список усіх технологій та їхніх унікальних ідентифікаторів, основними полями цього типу є ідентифікатор (ID) і назва технології (Name), а також доступні функції для встановлення параметра та отримати це. Тип даних для полів — String.

Тип даних IdTechniques.java був створений для надання технік у термінах ідентифікатора техніки (idTes), її назви (Name) та порядкового номера стадії APT (id) - іншими словами, тактики в розділі MITRE. Тип даних параметрів - String. Функції налаштування та отримання того чи іншого основного параметра реалізовані за замовчуванням. Tactics.Java зроблена для збереження даних після аналізу даних про тактику MITRE.

Основними параметрами є назва тактики (String Tactic), її порядковий номер (int id), а також назва техніки (String Name), яка використовується в

контексті цієї тактики. Також були створені функції для встановлення описаних вище параметрів і повернення їх значення [54].

TechniqueChart.Java — це спеціальний клас для опису типу даних, який призначений для малювання графіків у класі Chart.java. Основні параметри цього класу: порядковий номер етапу APT (id), дата (date), ідентифікатор техніки MITRE (name), параметр, що поєднує дату та ідентифікатор технології (concat), параметр, що поєднує змінні, такі як ідентифікатор технології, серійний номер етапу APT і дата (iddate). Також реалізовано ряд функцій для визначення та повернення значень параметрів класу, функція для повернення ключових значень (ID, ПІБ, дата).

У класі ParserCsvjava є 30 функцій, які призначені для парсингу подій та виділення певних параметрів з списків. Дані функції та опис їх призначення подано у таб. 2.15.

Таблиця 2.15

Функції класу ParserCsv

Функція та параметри на	Призначення функції
List<Event> parsingAll ()	Парсинг подій із файлу формату. csv, в якому зберігаються усі події за техніками MITRE, за
List<Event> parsingAll2 ()	Парсинг подій із файлу формату. csv, в якому зберігаються кінцеві події за техніками MITRE,
List<Event> parsingAllCmdExc	Функція видалення подій із типовими для організації командних рядків із початкового
List<Event> parsingAllHostExc	Функція видалення подій із хостами, на яких не було виявлено підозрілої діяльності, із
List<String> parsingHostExc ()	Парсинг списку із переліком хостів,, на яких не було виявлено підозрілої діяльності
List<String> parsingCmdExc	Парсинг списку із переліком командних рядків,
List<IdT echniques>	Парсинг списку із переліком усіх технік MITRE

List<Tactics> parsingTactices ()	Парсинг списку, що описує матрицю MITRE, де вказано порядковий номер тактики у розрізі
List<Techniques> createIdTecList (List<IdTechniques> idtec	Функція для створення об'єднаного списку із порядкового номеру тактики, ідентифікатору та
int countIPFreq (List<Event> emps, int n)	Функція обрахунку кількості не порожніх адрес призначення у списку подій
List<String> getDestIpNotNull	Пошук та збереження не порожніх адрес призначення у список формату String.
List<String> getDestIpNotNullHost	Пошук та збереження у списку хостів, із яких спостерігалися підключення до зовнішніх адрес.
List<Event> getEventsHost (List<Event> emps, String	Пошук усіх хостів зі списку подій.
void getCmdF orHost (List<Event>	Виведення поєднання хост та командний рядок із події.
Map<String, Integer> countFrequencies	Підрахунок кількості будь-якого параметру зі String списку.
Map<String, Integer> sortbyvalue (Map<String,	Сортування частоти виникнення певного параметру за спаданням.
void showMap (Map<String, Integer> map)	Виведення поєднання ключ та значення.
List<String> parsingDate (List<Event> emps)	Пошук та збереження унікальних дат у списку подій
List<String> parsingDateForHost	Пошук та збереження унікальних дат у списку подій для певного хосту
List<String> parsingTPN (List<Event> emps)	Пошук та збереження усіх цільових процесів зі списку подій
List<String> parsingUniqueTPN	Пошук та збереження унікальних цільових процесів зі списку подій
List<String> parsingUniqueTPNF orHost	Пошук та збереження унікальних цільових процесів зі списку подій для певного хосту.
List<String> parsingHost (List<Event> emps)	Пошук та збереження усіх хостів зі списку подій
List<String>	Пошук та збереження унікальних хостів зі
List<String> parsingCmd (List<Event> emps)	Пошук та збереження усіх командних рядків зі списку подій

List<String> parsingUniqueCmd	Пошук та збереження унікальних командних рядків зі списку подій
List<String> parsingUniqueCmdForHost	Пошук та збереження унікальних командних рядків зі списку подій для певного хосту.
List<String> parsingSPN (List<Event> emps)	Пошук та збереження усіх процесів із джерела зі списку подій

Джерело: результати власних досліджень

У цій категорії реалізовані функції, відповідальні за проведення підготовчих дій для отримання необхідних даних, які пізніше будуть використані в інших функціях.

Для відображення взаємозв’язків подій між процесами, датами, командними рядками тощо використовувалися дві бібліотеки – Graphstream для побудови графів та XChart для створення графіків різних типів. Для аналізу подій із форматованих файлів. csv, використовувалася бібліотека Csv від Apashe. Необхідність графічного відображення подій і зв'язків між ними пов'язана з тим, що при текстовому відображенні всіх подій аналітику дуже важко встановити зв'язки між подіями або визначити правомірність операцій або команд. параметри лінії. Але коли події групуються за певними доменами та переглядаються протягом певного періоду часу, це полегшує задачу розрізняти звичайну діяльність і зловмисну діяльність, а також ідентифікувати потенційно шкідливі вторгнення [44].

Клас Chart відповідає за такі етапи розробленого методу аналізу APT атак: побудова послідовності застосування технік MITRE та співставлення із життєвим циклом APT атаки, визначення хронології подій APT атаки.

Chart. java містить основні функції для створення відображення хронології подій із технік на основі різних масивів даних. Функція XYChart getChart (List<Event> emps, List<Techniques> all, String title) створює регулярний графік на основі списку подій, з якого ви вибираєте техніку, що використовується щодня, і порівнюєте її з фазою APT. На вхід функції надсилається список подій, список технологій з їх ідентифікаторами та назвою майбутньої таблиці.

Функція XYChart getFinalChart (List<Event> emps, String title) по структурі наслідує попередню функцію та призначена для відображення кінцевої хронології потенційної APT атаки. Також існує ще одна функція BubbleChart getBubbleChart (List<Event> emps, List<Techniques> all, List<TechniqueChart> ch, String title) для створення особливого типу графіку. Залежно від типів вхідних даних ця функція схожа на дві попередні, але тип діаграми BubbleChart визначає, що на діаграмі точка з використаною технікою на перетині історії та фази ART описуватиметься не однією точкою діаметром, але діаметром, який відповідає кількості разів використання цієї техніки на день (Це не залежить від хоста, лише загалом). Кожна з цих функцій повертає графік і створює його графічне представлення.

Ще один клас для графічного відображення зв’язків між подіями з певними ідентичними параметрами по днях і робочих станціях — EventGraph. java. Цей клас реалізує фазу методу аналізу атаки APT – побудова зв’язків між процесами за допомогою алгоритму нечіткого пошуку. При сукупному розгляді подій виявлено, що найважливішими параметрами для кореляції подій є цільові процеси та значення командного рядка, оскільки ці поля є найбільш інформативними та можуть детально описувати потенційно зловмисні дії. Інші поля змінної типу Event є допоміжними або допоміжними полями для вказаних параметрів.

Перша функція void graphEventDateTPN (List<Event> emps, List<String> date, List<String> tpn, String name***)*** приймає як вхідні дані список подій, список цільових дат і операцій, який розраховується на основі списку подій разом із назвою для графіка. Типами вершин для графа є цільові дати та операції. Ребра графа будуються на основі обчислення відстані Левенштейна.Якщо в певну дату є подія використання технології з певним цільовим процесом, це ребро з'єднує відповідні вершини з датою і з цільовим процесом. При виклику функція створює відповідний графік і відображає його в паралельному потоці.

Функція void graphEventCMD (List<Event> emps, List<String> date, List<String> cmd, String name) Отримує як вхідні дані список подій, списки дат і командні рядки, що відповідають подіям, а також назву графіка. Цей граф містить вершини з датою та вершини з командними рядками, а зв'язки між вершинами будуються на основі дати та того, який командний рядок був присутній у події протягом певного дня. Розрахунок відстані Левенштейна використовується для зв'язування командних рядків із датами полів події та записами зі списків дат і командних рядків. Після виведення генерується графік із відображеними датами та значеннями командного рядка, які використовуються для кожної дати.

Найбільш комплексною функцією з точки зору побудови графу є void graphEventTrio (List<Event> emps, List<String> date, List<String> tpn, String name). Ця функція має три типи вершин: дата, цільовий процес і командний рядок. Щоб зіставити ключові поля з подій і переданих елементів списку з датами, операціями та командними рядками, також використовується функція Левенштейна, яка обмежена певним значенням (у більшості випадків це 0), яке визначає рівень подібності. Ребра графіка будуються в такій послідовності: спочатку визначаються зв'язки між датою та цільовими процесами, які використовувалися у відповідний день, потім шукаються ті події, де дата та цільовий процес мають певний рівень подібність до існуючих вершин і ребер, і генерується ребро процесу До існуючого командного рядка за вказану дату. Результат повертає графік, що відображає пов'язані зв'язки.

BuildAPT. java – це основний клас програми, де створюються об'єкти та викликаються функції для аналізу даних і створення хронології подій APT. Основний алгоритм дій у головному класі:

Створення об'єкту класу ParserCsv.

Проаналізувати події з вибраного файлу за допомогою функції parsingAllQ і зберігти дані у списку типів Event.

Розібрати ключові поля в окремі списки типу String: дати, цільові процеси, робочі станції, командний рядок і вихідні процеси, а також аналізує унікальні значення вищезазначених полів в інші окремі списки.

Парсинг файлів з файлів, використовуючи техніку, тактику, та їхні ідентифікатори, щоб створити один загальний список типу Techniques.

Створення діаграм і графіків на основі початкового списку Event. Діаграми та діаграми аналізує аналітик, виводячи список звичайних командних рядків, які відповідають типовій діяльності організації.

Проаналізуйте файл із винятками командного рядка, знайдіть ці командні рядки у вихідному файлі для аналізу, витягніть відповідні події та збережіть результати в новому списку типу "Event". Повторіть кроки 3–6 на основі нового списку.

Після аналізу графічних відображень виводиться список робочих станцій (за наявності), для яких не відображається небезпечна або потенційно небезпечна діяльність.

Проаналізуйте файл із винятками командного рядка та файл із винятками робочої станції, знайдіть ці командні рядки та робочі станції в попередньому файлі подій, щоб проаналізувати та вилучити пов’язані події та збережіть результати в новому списку типів подій.

Повторюйте кроки 3-6 і 9-10 на основі нового списку, доки не залишиться подій, які можна було б назвати нормальними, і ця діяльність не буде підтверджена організацією як нормальна.

Викличте функцію getTes на основі останнього проаналізованого файлу типу Event, щоб отримати список типу TechniqueChart з даними, необхідними для створення остаточних діаграм і графіків.

Висновки по розділу №2

Детально розглянуто такі комерційні платформи для комерційної кіберрозвідки, як Anomali ThreatStream, Anomali Enterprise, ThreatConnect, TC

Identify, TC Manage, TC Analyze, ThreatConnect CAL, TC Complete, ThreatQ та дано їх переваги перед конкурентами.

Проаналізовано підходи до класифікації типів кіберрозвідки та коротко проаналізовано основні. Зроблено аналіз моделей та методів захисту кіберпростору (стандарти аналізу ризиків, NIST, методологія Azure та ISO 2700x) та зроблено порівняння методів оцінки ризиків.

Окремо дана характеристика методу пошуку максимальної кількості індикаторів компрометації (IoC) та їх розповсюдження. Індикатори компрометації – це життєво необхідна складова для багатьох рівнів захисту інфраструктури. Їх можна використовувати як на рівні мережі, так і на рівні хосту. Кожен день з’являються нові атаки, які занадто складно відстежувати спеціалісту з кібербезпеки, або навіть команді спеціалістів. Саме тому існують такі проекти для розповсюдження індикаторів компрометації, як MISP, що дають можливість компаніям ділитись між собою атаками, які вони вже змогли виявити. Прикладами IoC є адреси командних серверів ботнетів, електронні адреси розсильників фішингових листів і спаму, сигнатури вірусів, хеш-суми шкідливих файлів.

В другій частині дослідження зроблено опис розробленого методу аналізу APT. Представлено виявлені індикатори технік MITRE, які призначені для першого етапу методу – фільтрації подій та зменшення їх кількості шляхом пошуку застосування технік у подіях. Описано програмну реалізацію, яка покриває інші етапи методу аналізу, зокрема підходи до побудови послідовності подій та хронології виявленої APT атаки шляхом виявлення кібератак на основі індикаторів компрометації.

Розділ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДУ ТА ОЦІНКА ЕФЕКТИВНОСТІ

3.1. Визначення особливостей APT-атак та мети досліджень

Аналіз різних інформаційних джерел [38, 39] дозволяє визначити наступні характерні особливості APTs:

- атака представляє складний набір взаємозв'язаних за часом і простором дій зловмисника. Окремо ці дії можуть не викликати підозр;
- цільова акція атаки в кіберсегменті об'єкта готується тривалий час (від декількох місяців до року і більше);
- сукупність дій зловмисника – це ланцюжок тактик, виконання яких дозволяє досягти мети атаки (цільової акції). Незважаючи на різноманітність засобів, що використовуються в APTs, набір більшості тактик і їх сутність залишаються постійними.

Подальший аналіз цих характерних тактик (етапів) [1, 5] дозволяє уточнити суть дій зловмисника в рамках APT атаки. Після визначення корпоративної ITS і її ресурсу, який критичний для зловмисника (наприклад: база даних, диспетчерський комп'ютер SCADA, веб-сайт або інше. Далі – об'єкт атаки), він діє таким чином.

Етап 1. Зовнішня розвідка. Здійснюється збір інформації про характеристики IT-систему з різноманітних джерел поза нею.

Етап 2. Проникнення в IT-систему. На основі інформації зовнішньої розвідки приймається рішення про засоби і способи запуску несанкціонованих процесів в одному із хостів системи. За допомогою комп'ютера зловмисника здійснюється реалізація рішення шляхом направлення через Інтернет необхідних даних. На основі прийнятих повідомлень запускаються процеси, які встановлюють прихований канал віддаленого (дистанційного) управління хостом (backdoor, BD).

Етап 3. Доставка засобів впливу. Отримана зловмисником інформація про встановлений прихований канал управління запускає процес доставки набору несанкціонованих програмних засобів, що дозволяють здійснити внутрішню розвідку в межах корпоративної комп'ютерної мережі.

Етап 4. Внутрішня розвідка. Шляхом запуску несанкціонованих і штатних процесів здійснюється збір даних про компоненти мережі. Зібрана інформація надсилається по прихованому каналу зловмисникові. Після її оцінки приймається і реалізується рішення про просування від одного вузла мережі до іншого до моменту виявлення критичного ресурсу.

Етап 5. Цільовий вплив (цільова акція атаки). На основі отриманих даних про знаходження критичного ресурсу зловмисником приймається рішення про засоби і способи реалізації цільового впливу. За допомогою BD до 7 критичного хоста доставляються необхідні програмні засоби. Запускаються несанкціоновані процеси, які реалізують компрометацію цільового ресурсу (отримання доступу до критичної інформації і передача зловмисникові, отримання доступу до управління технологічним процесом і переведення його в потрібний стан, порушення процесів обробки інформації).

Етап 6. Приховування слідів атаки. За допомогою несанкціонованих процесів на всіх хостах стираються дані, які були пов'язані з атакою. Проведений аналіз дозволяє стверджувати, що формування BD та його застосування є основними процесами, які дозволяють зловмиснику в рамках APT-атаки отримувати інформацію про стан IT-системи, визначати, доставляти та застосовувати необхідні програмні засоби для проведення несанкціонованих дій.

Таким чином, актуальною стає завдання своєчасного визначення (детектування) BD ще на етапі підготовки цільової акції. Встановлення оперативного контролю над BD дозволяє приймати своєчасні рішення про припинення атаки, або про проведення додаткових заходів зниження збитків від цієї атаки у випадку неможливості її припинення. Такий підхід відповідає

реалізації проактивної стратегії кіберзахисту, метою якої є переривання APT-атаки ще до початку етапу цільової акції.

Аналіз різних доступних джерел [3, 7] про механізми проведення APT-атак та відповідні заходи захисту дозволяє стверджувати, що:

1) BD дозволяє зловмиснику реалізовувати план проведення атаки шляхом впровадження програм-агентів та вдавленого управління ними;

2) BD є базовим засобом реалізації APT-атаки;

3) переривання BD засобами захисту IT-системи може спровокувати запуск механізмів знищення інформаційних ресурсів, що пов’язано зі значним збитками;

4) детектування BD на протязі часу перед цільовою акцією атаки та встановлення оперативного контролю за командами зловмисника дозволяє значно знизити відповідні ризики безпеки;

5) основою сучасних підходів проактивного захисту від APT-атак є системи управління інформацією та подіями безпеки (Security of Information and Event Management, SIEM), які визначають несанкціоновані дії шляхом збору інформації з журналів події різних сенсорів безпеки IT-системи та порівнюють цю інформацію із шаблонами APT-атак;

6) шаблон APT-атаки – це набір індикаторів (сигнатур) подій в системі, що визначені на основі закономірностей, які притаманні атаці. Закономірності визначаються на основі моделей APT;

7) більшість APT-атак – це атаки 0-day: постійно змінюються засоби та тактики атаки. Постійною складовою більшості APT-атак є її BD. Шаблон для BD може дозволити детектувати різні APT-атаки.

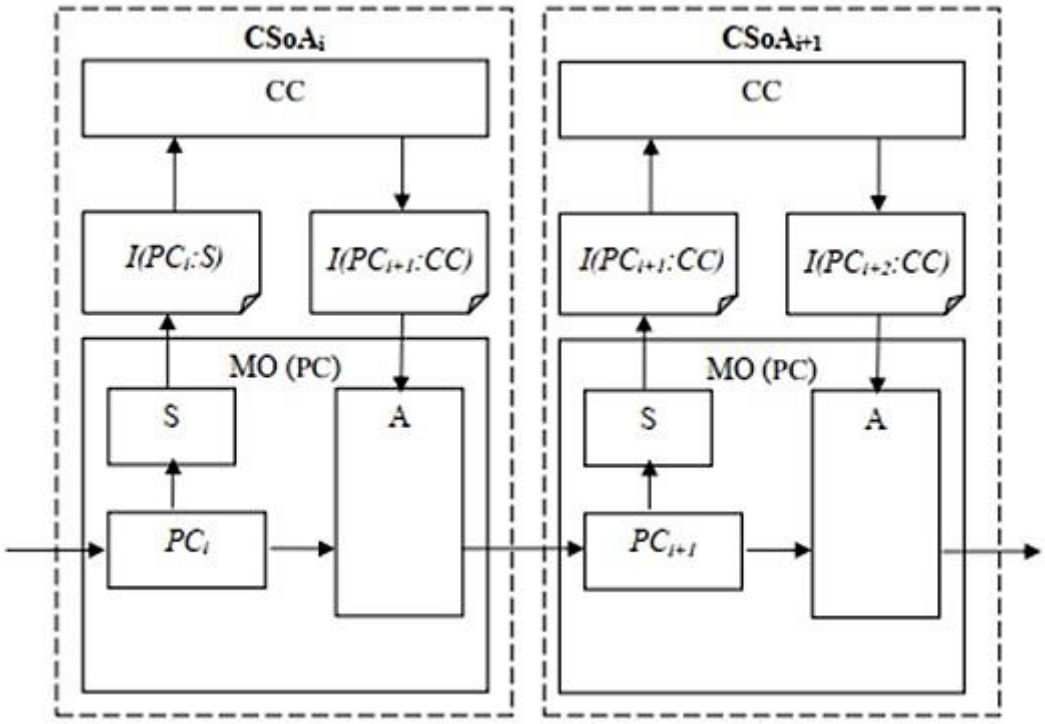
3.2. Вибір моделі APT-атаки та розробка моделі поведінки BD

Проведений аналіз різних моделей APT-атак на предмет їх використання для формування BD-шаблону показує, що їх більшість представлені у вигляді

вербального опису цілій етапів атаки та загального сенсу механізмів їх досягнення. Переваги таких моделей – вони виділяють загальні закономірності для різних атак. Загальний недолік – неможливість прямого застосування в SIEM через відсутність логічного зв'язку між описом подій в рамках етапів та відповідних індикаторами компрометації, які необхідно представляти у бітовому форматі.

Інша група моделей описує атаку за допомогою різних математичних конструкції (графи, логічні елементи, алгоритм оптимізації, приховані марківські процеси, піраміда атаки та інші). Переваги таких моделей – дозволяють уявити масштабні дії зловмисника у вигляді одного складного процесу. Загальний недолік – складно зв'язуються з технологічними процесами в корпоративному кіберсегменті.

За основу досліджень цей роботи була прийнята кібернетична модель APT-атаки. В основі моделі є представлення дій зловмисника у вигляді кібернетичної системи (CyberSystem of APT, CSoA), об'єктом управління котрої є хост (хост – комп'ютер IP-мережі) зі складу ITS жертви, а суб'єктом управління – віддалений хост зловмисника. Поведінка CSoA може бути представлено рисунком 3.1.



Джерело: результати власних досліджень

Рис. 3.1. Графічна модель кібернетичної системи APT-атаки

Персональний комп'ютер (PC), що входить до складу корпоративної мережі, виступає в ролі об'єкта управління (МО). Зловмисник і його комп'ютер представлені як центр управління (СС). *I (PCi: Б)* – це інформація про стан *PCI* персонального комп'ютера в рамках актуальної (поточної) фази *CSOAI.* Дана інформація сформована і направлена до СС сенсором S. На основі прийнятої інформації центр управління СС приймає рішення про переведення об'єкта управління МО в наступний стан PC_{I+I} і оформлює це рішення в вигляді інформації *I (PCI+1: CC).* Далі ця інформація пересилається до МО, де прийняте рішення реалізується за допомогою актуатора А: об'єкт управління переходить в наступний стан PC_i+_1. Кожний і-й цикл управління $C8OЛ_i+_1$ закінчується переходом в цикл $C8OЛ_i+_1$ на основі виконання актуатором А команди *I (PCI+1: CC).*

Процес управління в рамках CSoA і поведінку самої CSoA (перехід з одного циклу в інший) може бути описаний наступною системою рівнянь:

$$\begin{cases} I(PC_{i+1}:CC) = F_{cc}[I(PC_i:S)]; \\ PC_{i+1} = F_A[PC_i, I(PC_{i+1}:CC)]. \end{cases}$$

де *PCi + 1, I (PCi: S), I (PCi+1: CC), PCi* – це кінцеві бітові множини;

PCC [.] – це оператор відображення, який на основі прийнятої інформації і по заданому правилу прийняття рішення формує команду про перехід в інший стан;

FA [.] – це оператор відображення, який на підставі прийнятої команди переводить об'єкт управління з одного стану в інший.

Вся APT-атака за допомогою CSoA може бути представлена у вигляді наступної множини:

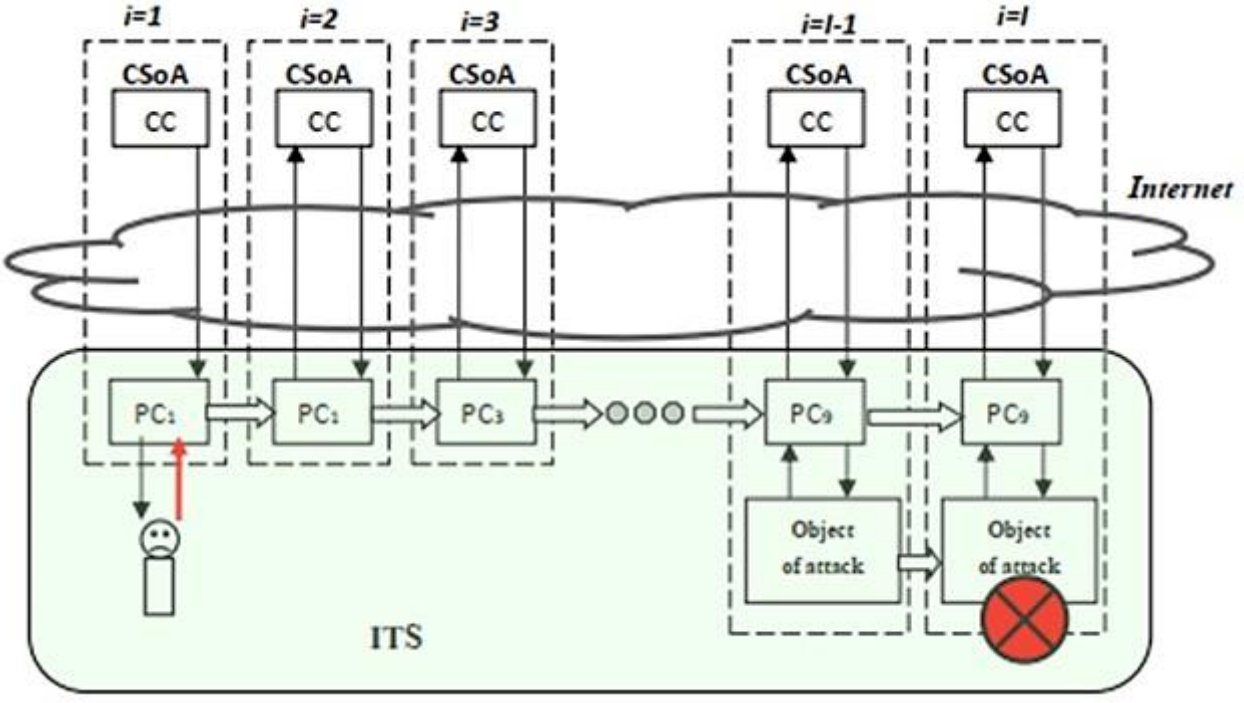
APT*={CSoAi}, i= 1,..., I.*

де: ***APT –*** це кінцева множина, що складається з кінцевих підмножин *CSoAi* (відповідних циклів управління кібернетичної системи атаки);

CSoAi = {PCi, I (PCi: S), I (PCi+1: CC)} – підмножина, що складається з кінцевих бітових наборів (множин). Ці набори двох суміжних циклів *CSoA*, що пов'язані між собою системою рівнянь;

i = 1,..., I – номер поточного циклу *CSA*; *I* – кількість циклів APT атаки.

За допомогою такої формалізації вдалося представити APT атаку у вигляді послідовності фаз кібернетичної системи атаки. Кожна фаза – це послідовність регулярно повторюваних дій, які можна назвати процедурами атаки. Часові межі кожної фази визначаються моментами встановлення нового стану об'єкта управління. Під новим станом слід розуміти або зміни в керованому комп'ютері, або перехід до іншого комп'ютера в мережі. Візуальним поясненням запропонованої моделі може бути структура на рисунку 3.2.



Джерело: результати власних досліджень

Рис. 3.2. Графічне представлення кібернетичної моделі APT атаки

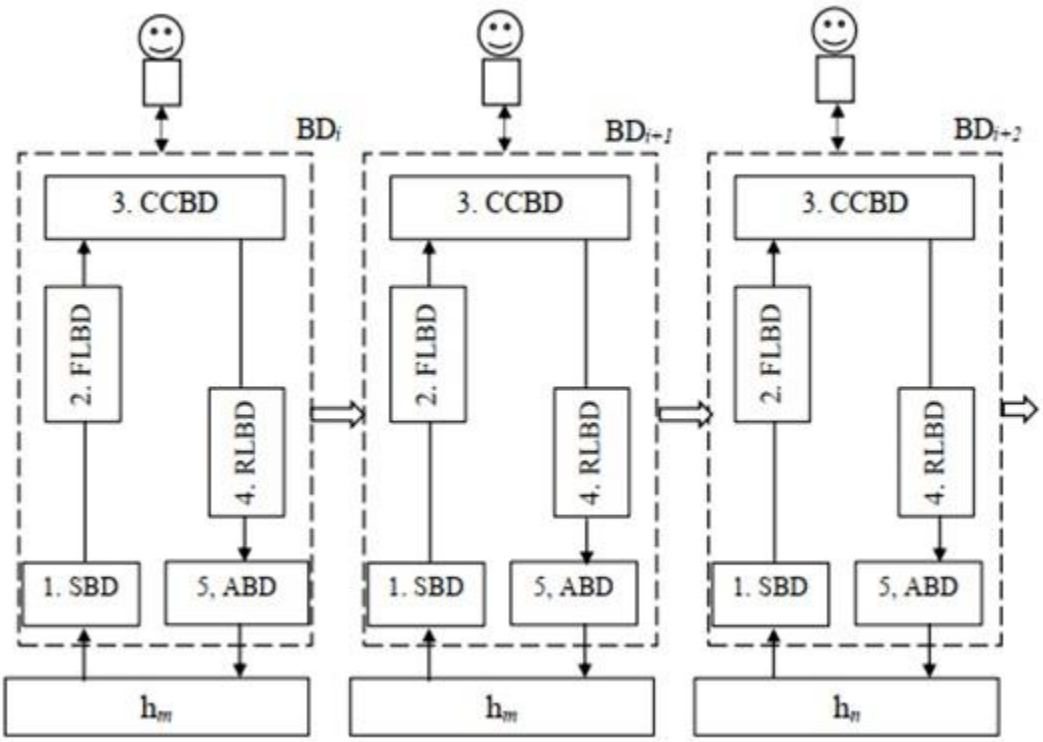
Кібернетична модель APT-атаки дозволяє:

– кожний етап вербальної моделі атаки представити у вигляді одного або декількох циклів кібернетичної системи;
– кожний цикл представити у вигляді конкретних інформаційних процесів (процедур атаки);
– кожної процедурі атаки поставити бінарні набори, які відображають елементарні події в комп'ютерному середовищі. Ці події можуть бути зафіксовані комп'ютерними пристроями корпоративної ІТС та представлені на обробку в;
– із елементарними подіями або набором елементарних подій в ІТС.

Розробка моделі поведінки BD включає такі частини, що відповідають розглянутим процедурам CSoA:

1. програма-агент, що збирає та передає дані про стан хоста-жертви (далі – Sensor BD, SBD);
2. прямий канал BD (Forward Link BD, FLBD), за допомогою якого повідомлення про стан хоста-жертви доставляється до хоста-зловмисника;
3. програма хоста-зловмисника, що приймає та представляє зловмиснику інформацію про стан хоста-жертви (Control Center BD, CCBD);
4. зворотній канал BD (Return Link BD, RLBD), за допомогою якого команди та повідомлення від зловмисника доставляються до хоста-жертви;
5. програма-агент, що приймає та виконує команди від хоста-зловмисника (Actuator BD, ABD).

За допомогою визначених складових можливо визначити структуру та модель поведінки BD (рис. 3.3).



Джерело: результати власних досліджень

Рис. 3.3. Структура та модель поведінки BD в рамках APT-атаки

В рамках розробленої моделі поведінка BD в рамках корпоративному кіберсегменті реалізується у вигляді послідовності циклів з наступних процедур:

- формування сенсором SBD повідомлення зловмиснику про стан хоста (1);
- передача повідомлення через прямий канал FLBD (2);
- прийняття повідомлення CCBD, його аналіз зловмисником та прийняття рішення подальші дії, формування CCBD команди для актуатора ABD (3);
- передача команди через зворотній канал RLBD (4);
- прийом команди актуатором ABD та їх реалізація**.**

Альтернативним методом оцінки індикаторів компрометації можна запропонувати рішення, продемонстроване у розрахунковій формулі. З його допомогою з’явилася можливість бути незалежним від джерела даних, де базове значення вираховується як комбінація QoD (Quality of Detection), FPR (False Positive Rate), а також додається значення швидкості спадання з логістичною функцією.

$$score = 100 \cdot \frac{(1 + QoD - FPR)}{2} \cdot \frac{1}{1 + e^{(x-24)}}$$

False Positive Rate – це коефіцієнт помилково визначених даних відносно загальної кількості у відсотковому співвідношенні [5], використовується значення в проміжку від 0 до 1. Для визначення швидкості спадання, з якою загальний бал з часом зменшується, ми використовуємо логістичну функцію. Якщо вважати що індикатори компрометації ввести у використання займає небагато часу, в середньому спеціаліст з кібербезпеки зможе почати їх використовувати упродовж свого робочого дня. Проте, враховуючи перепади у часових поясах, можна припустити що більшість великих компаній почнуть його використовувати протягом 24 години після оприлюднення. Отже, після перших 24 годин оцінка індикатора спаде у два рази, та буде активно рухатись у напрямку спадання. Quality of Detection – значення в проміжку від 0% до 100%, що описує надійність виконаного виявлення вразливості або продукту. Для формули ми переводимо значення у проміжок від 0 до 1. OpenVAS категоризували QoD як показано у таб. 3.1.

Таблиця 3.1

Категоризація QoD від Open VAS

QoD	Тип QoD	Опис
100%	exploit	Виявлення відбулося за допомогою експлойту, а отже повністю підтверджено.
99%	remote_ vu1	Віддалені активні перевірки (віддалене виконання коду, атака обходу каталогу, sql-ін’єкції, тощо), де відповідь чітко вказує на наявність вразливості.
98%	remote_app	Віддалені активні перевірки (віддалене виконання коду, атака обходу каталогу, sql-ін’єкції, тощо), де відповідь чітко вказус на наявність вразливого додатка.

97%	package	Автентифіковані перевірки на основі пакетів для систем Linux.
97%	registry	Автентифіковані перевірки на основі реєстру для систем Windows.
95%	remote_active	Віддалені активні перевірки (віддалене виконання коду, атака обходу каталогу, sql-ін'єкції, тощо), коли відповідь показує ймовірну присутність вразливої програми або вразливості. «Ймовірну» означає, що можливі лише рідкісні обставини, коли виявлення буде неправильним.
80%	remote_banner	Віддалена перевірка програм, які пропонують виправлення у нових версіях.
80%	executable_version	Автентифікована виконувана версія для систем Ілпих або / Vindows, де програми пропонують виправлення у новій версії.
70%	remote_analysis	Віддалені перевірки, які проводять певний аналіз, але не завжди надійні.
50%	remote_probe	Віддалені перевірки, де проміжні системи, такі як брандмауери, можуть передбачити правильне виявлення, так що насправді незрозуміло, де відповіла сама програма. Це може статися, наприклад, для з'єднань без підключено TLS.
30%	remote_banner_unreliable	Віддалена перевірка банерів програм, які не пропонують рівень виправлення в ідентифікації версії. Наприклад, це часто трапляється у багатьох продуктах з відкритим кодом.
30%	executeable_version_unreliable	Перевірена автентифікація виконуваної версії для систем Linux, де програма не пропонує виправлення в новій версії.

Для прикладу можна навести скомпрометовану IP адресу. Quality of Detection для IP-адреси у нашому випадку буде 100%, тобто 1, взявши це з таблиці 3.1. Припустимо, що для пошуку IP-адрес використовуються сервіси як feodotracker, рівень False Positive Rate не повинен бути високий [46], будемо вважати, що він рівний 0.2. Отже, отримуємо формулу та графік на рисунку 3.4, з якого бачимо, що за деякий час актуальність даних падає.

$$score = 100 \cdot \frac{(1 + 1 - 0.2)}{2} \cdot \frac{1}{1 + e^{-(x-24)}}$$

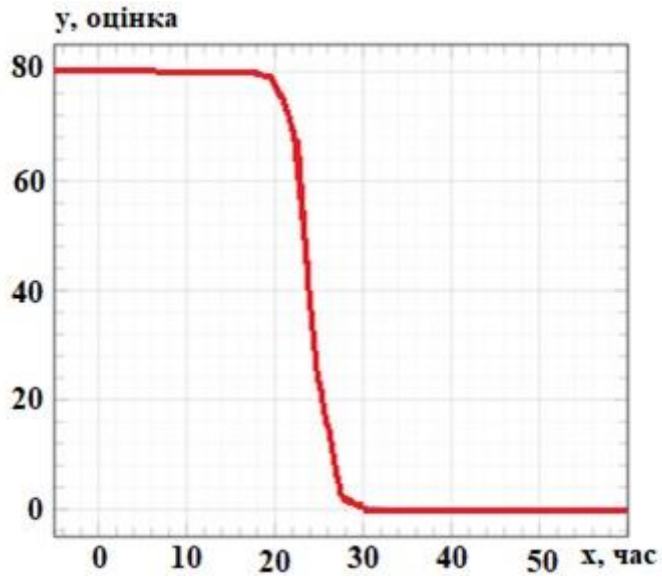


Рис. 3.4 Графік актуальності індикатора для скомпрометованої IP-адреси

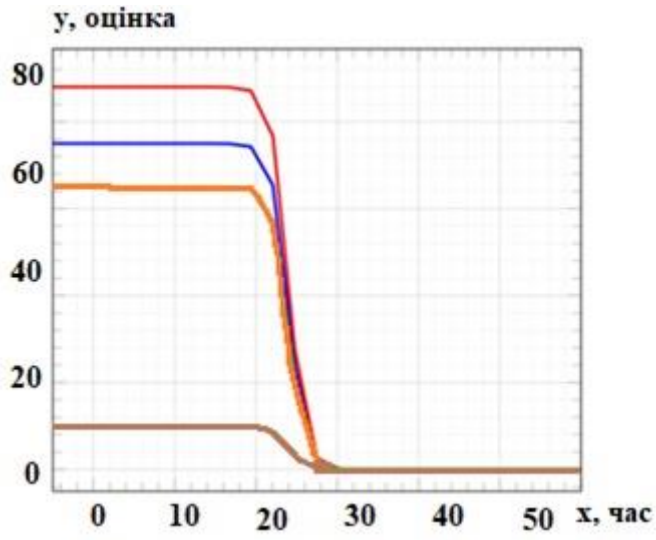
На рис. 3.5 зображено чотири графіки для функцій наведених в формулі.

$score_a = 100 \cdot \frac{(1 + 1 - 0.5)}{2} \cdot \frac{1}{1 + e^{-(x-24)}}$ - **синій колір графіка**

$score_b = 100 \cdot \frac{(1 + 1 - 0.24)}{2} \cdot \frac{1}{1 + e^{-(x-24)}}$ - **червоний колір графіка**

$score_c = 100 \cdot \frac{(1 + 0.5 - 0.2)}{2} \cdot \frac{1}{1 + e^{-(x-24)}}$ - **помаранчевий колір графіка**

$score_d = 100 \cdot \frac{(1 + 0.1 - 0.9)}{2} \cdot \frac{1}{1 + e^{-(x-24)}}$ - **коричневий колір графіка**



Джерело: результати власних досліджень

Рис. 3.5 Приклад варіантів оцінок індикаторів компрометації

В якості прикладу приведемо порядок використання альтернативної скорингової системи на статистичних даних шкідливого програмного забезпечення Regin Regin – комп'ютерний черв'як, що вражає комп'ютери під управлінням операційної системи Microsoft Windows, виявлений Kaspersky Lab і Symantec в листопаді 2014 року.

За оцінкою представників «Лабораторії Касперського», перші повідомлення про цей вірус з'явилися навесні 2012 року, а найбільш ранні виявлення екземпляри датуються 2003 роком. Regin – це шкідливе забезпечення, яке використовує модульний підхід, що дозволяє йому завантажити функції, необхідні для обліку індивідуальних особливостей зараженого комп'ютера або мережі. Структура вірусу розрахована на постійне, довготривале цільове спостереження за численними об'єктами. Regin не зберігає дані в файловій системі зараженого комп'ютера, замість цього він має свою власну зашифровану віртуальну файлову систему (EVFS), яка виглядає як єдиний файл.

В якості методу шифрування EVFS використовує варіант блочного шифру RC5. Regin здійснює комунікації через Інтернет з використанням ICMP / Ping, команд, вбудованих в HTTP cookie і протоколів TCP і UDP, перетворюючи заражену мережу в ботнет. Переглянувши доповідь Kaspersky Lab розслідування

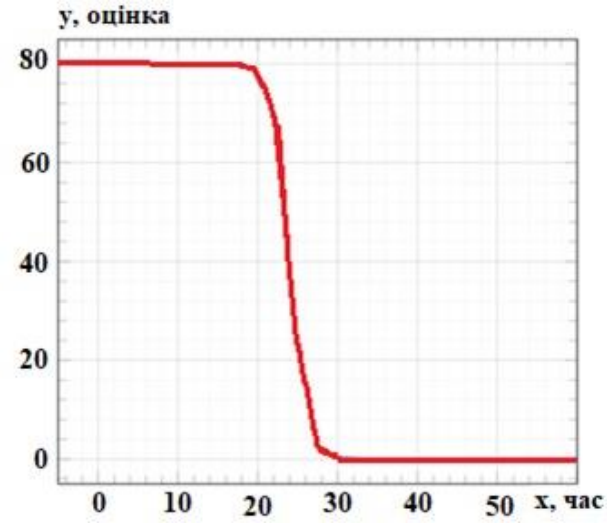
цього шкідливого програмного забезпечення, а також переглянувши дані з Loki – утиліта що використовуються для скану індикаторів, ми можемо виявити 33 хеші, і також 17 false positive хешів, деякі з яких можна побачити у таблиці

Таблиця 3.2

Приклали false positive хешів шкідливого програмного забезпечення Regin

6e5ebbc8b70c 1 d593634dafl) c 190deadfda 18c3 cbc8ß52a76fl 56ß869efl) 5b	Microsoft USB Scanner драйвер
a26db2eb9ße2509b4eba949db97595cc32332 d9321 df68283bfc 102e66d766f	Windows Serial драйвер
0099940a366b401 f30faaf820f4815083778383 a2b 1 e9fab58e 16d 10b8965e3 f	USB Scanner драйвер
5d7509ee8bfl c3c 14c 10b9c2be3d58d56acedfb 08444t9c774e5d8caa8659043	Client. exe
b04a85et2edbc5ac7b312e9d57b533d9d355d0 c7cbbd24a8085c6873baf941 lf	SCSI драйвер Windows
519a0d7ebc75dcf65c80d61 f952768e49c33c5c 7c320a4cc4b4a 12a0e9ß337d	SPI. CAB MSDN Disc 3498

$$score = 100 \cdot \frac{(1 + 1 - 0.24)}{2} \cdot \frac{1}{1 + e^{(x-24)}}$$



Джерело: результати власних досліджень

Рис. 3.6. Оцінка індикатора компрометації базована на хешах шкідливого програмного забезпечення Regin

Отже, з отриманих даних отримуємо, що значення False Positive Rate рівне 0.24, а з таблиці 3.2 обираємо значення Quality of Detection. Нехай у вказаному випадку воно буде дорівнювати 1. Таким чином за допомогою функції для оцінки індикатора отримуємо графік, що характеризує оцінку, що була побудована на хешах Regin.

3.3. Визначення відповідності процедур управління в рамках BD та елементарних подій ITS

Процедури (*procedure, Pr*) виконуються циклічно в рамках визначеної послідовності, але з різною протяжністю відповідного часового періоду (далі – періоду циклу, T***i***). Закінчення періоду циклу визначається моментом часу, що відповідає закінченню виконання останньої команди від зловмисника. Кожний цикл BD***i*** пов'язаний із конкретним хостом (*host, h***)** корпоративної ITS. Зловмисник може виконувати один або декілька циклів на одному хості, а потім продовжувати використовувати BD відносно іншого хосту.

Якщо кожну процедура циклу *Pr* пов'язати з якоїсь бітовою послідовність (*signature, Sign*), то з'являється можливість відслідковувати за допомогою

засобів SIEM за часом та кіберпростором ITS. Можливо розглядати наступні види елементарних подій (об'єктів) в корпоративному кіберсегменті:

1) обчислювальні процеси на хостах (*process*, *Prs*);

2) послідовність даних, якими обмінюються обчислювальні процеси різних хостів за допомогою мережі (*traffic*);

3) файли даних, які формуються процесами, та зберігаються на носіях. З одного боку кожна елементарна подія пов'язана із набором індивідуальних характеристик конкретного хоста комп'ютерної мережі. Наприклад: кожний трафік пов'язаний із просторовими характеристиками мережи: IP-адреса, MACадреса, *domen name* та інші. Також трафік пов'язаний із видом транспортного протоколу (TCP або UDP) і із конкретним обчислювальним процесом (через номер IP-порта).

Кожний обчислювальний процес також пов'язаний із рядом характеристик: образ виконуваного машинного коду; пам'ять (зазвичай деяка область віртуальної пам'яті) і її стан; стан стеку викликів; дескриптори ресурсів операційної системи; файлові дескриптори; набір повноважень процесу (допустимі операції); стан процесору (контекст процесору) та інші характеристики. Операційна система зберігає більшу частину інформації про процеси в таблиці процесів. Структура та модель поведінки BD (рис. 3.6) дозволяє кожної процедурі (1) – (5) поставити у відповідність наступні елементарні події (таб. 3.3), що можуть бути детектуванні сенсорами безпеки ITS:

Таблиця 3.3

Відповідність процедур циклу BD, елементарних подій ITS та індикаторів компрометації BD

Компонента моделі BD	Процедура циклу, Pr	Елементарна подія ITS	Назва індикатору компрометац	Перемінне значення IoC

SBD	*PR1*	вихідний трафік хоста, *TRC1* процес хоста, *PRS1*	*SIGN (TRC1)* *SIGN (PRS1)*	*x1–1* *x1–2*
FLBD	*PR2*	вихідний трафік ITS, *TRC2*	*SIGN (TRC2)*	*x2*
CCBD	*PR3*	вихідний трафік хоста зловмисника, *TRC3*	*SIGN (TRC3)*	*x3*
RLBD	*PR4*	вхідний трафік ITS, TRC4	*SIGN (TRC4)*	*x4*
ABD	*PR5*	вхідний трафік хоста, TRC5 процес хоста, PRS5	*SIGN (TRC5)* *SIGN (PRS5)*	*X5*
h	*PR6*	процес хоста, що	*SIGN (PRS6)*	*X6*

Джерело: результати власних досліджень

Таблиця 1 може бути розширена за допомогою додаткових знань про політику застосування BD. Наприклад, за допомогою BD зловмисник доставляє шкідливу програми, а потім на її основі активує шкідливий процес *Prs6*. Ця процедура не є циклічною (в табл. 3.3 – *Pr6*). Якщо за допомогою SIEM в рамках циклу BD***i*** буде визначено зв'язок міх цими подіями, то для наступного циклу BD_{i+1} можливо сформувати додаткові IoC: *Sign (Prs6)*; *Sign (Trc5).*

Запропоновані модель BD та підхід до відповідності процедур циклу BD елементарним подіям в ITS (табл. 3.3) дозволяють розробити наступну структуру шаблону для детектування BD (таб. 3.4). Структура розроблялася для ITS, що має локальну корпоративну мережу з підключенням до ресурсів Інтернет через роутер периметру *R* та файєрвол нового покоління ***NGFW***.

Таблиця 3.4

Структура шаблону для детектування BD

	BDi=i		BDi=2			BDi=i	
	IoCi=i	Мітка про детектуван	IoCi=2	МД		IoCi=i	МД
NGFW	Sign (Trc3, inp) Sign (Trc3	+	Sign (Trc3, inp) Sign (Trc3	+ +		Sign (Trc3, inp) Sign (Trc3	+ +
	Sign (Trci)	+	Sign (Trci)			Sign (Trci)	

hm=1	Sign (Prsi)	+	Sign (Prsi)			Sign (Prsi)	
	Sign (Trc5)	+	Sign (Trc5)			Sign (Trc5)	
	Sign (PrS5)	+	Sign (PrS5)			Sign (PrS5)	
			Sign (Prs6)			Sign (Prs6)	
	hm=2		Sign (Trci)	+		Sign (Trci)	
	Sign (Prsi)		Sign (Prsi)	+		Sign (Prsi)	
	Sign (Trc5)		Sign (Trc5)	+		Sign (Trc5)	
	Sign (PrS5)		Sign (PrS5)	+		Sign (PrS5)	
			Sign (Prse)			Sign (Prse)	
	hm=M		Sign (Trci)			Sign (Trci)	+
	Sign (Prsi)		Sign (Prsi)			Sign (Prsi)	+
	Sign (Trc5)		Sign (Trc5)			Sign (Trc5)	+
	Sign (PrS5)		Sign (PrS5)			Sign (PrS5)	+
						Sign (PrS5)	

Джерело: результати власних досліджень

Ця структура шаблону (далі – СШ) об'єднує індикатори компрометації таким чином, що дозволяє відслідковувати поведінку BD за часом (номер циклу процедур управління *i=1,..., I*) та простором ITS (файєрвол *NGFW* та хости *hm*, *m= 1,..., M*). СШ дозволяє використовувати різни політики детектування BD. Розглянемо одну з цих ПБ (далі – ПБ–1):

NGFW фіксує вхідний трафік *Trc3, inp* та вихідний трафік *Trc3, out*;

формується припущення, що це перший цикл управління BD***i=1***;

формуються наступні значення IoC:

Sign (Trc3, inp)= (IP-адреса, IP-порт)

на *hm*, що визначений за *IP-адресою Sign (Trc3, inp)*, визначається новий *Prs1*, що пов'язаний з обміном даних через *IP-порт Sign (Trc3, inp)*;

сформовані *Sign (Trc3, inp)*; *Sign (Trc3, out); Sign (Prs1)* використовуються для визначення наступних циклах управління (на цьому, або іншому хосту);

за мітками детектування відслідковується траєкторія поведінки BD.

Для ситуації коли СШ пов'язується з декількома траєкторіями BD (одна – істинна, а інші – помилкові), то рішення приймається на основі порівняння ваг цих траєкторій.

Працездатність запропонованого способу було перевірено за допомогою обладнання ситуаційного центру кібербезпеки. До складу макету корпоративної ITS було включено; фізичний роутер периметру, фізичний NGFW FortiGate 6300F / 6500F, чотири віртуальні хости. З хоста зловмисника (віртуальний хост) засобами ОС Kali Linux шляхом впровадження Reverse Shell через порт 80 було встановлено канал дистанційного управління хостом ITS. В якості сенсорів безпеки використовувались FortiGate 6300F / 6500F та розроблено програмне забезпечення, що дозволяє визначати обчислювальний процес на хості. Для обробки даних від сенсорів безпеки застосовувались штатні засоби FortiGate 6300F / 6500F (журнали подій). Аналіз подій проводився відповідно розробленому шаблону BD.

Висновки по розділу №3

Досліджено етап фільтрації подій та особливості опису індикаторів технік для фільтрації подій шляхом застосування технік MITRE та співставлення із життєвим циклом APT атаки. Наведено програмну реалізацію розробленого методу. Для коректного розбору даних за полями було реалізовані спеціальні типи даних. У класі Event. java описано тип даних для події, отриманої із файлу з кореляційними подіями від Sysmon та Powershell. Побудова ребер графу відбувається у наступній послідовності: спочатку визначаються взаємозв’язки між датою та цільовими процесами, що були використані у відповідний день, далі відбувається пошук тих подій, де дата та цільовий процес має заданий рівень схожості із наявними вершинами та ребрами, та будує ребро від процесу до знайденого командного рядка у розрізі певної дати.

В практичній частині дослідження зроблено визначення особливостей APT-атак та мети досліджень. Описано вибір моделі APT-атаки та розробку моделі поведінки BD. В якості альтернативного методу оцінки індикаторів компрометації запропоновано рішення, де базове значення вираховується як комбінація QoD (Quality of Detection), FPR (False Positive Rate), а також додається

значення швидкості спадання з логістичною функцією. Для запропонованого методу проведено практичну реалізацію та результат представлено у графічному вигляді. Використано скорингову систему до даних, зібраних про шкідливе програмне забезпечення Regin, для якого було виявлено 33 хеші та 17 false positive хешів. Побудовано візуалізацію оцінки індикатора компрометації.

Розділ 4(5).
Охорона навколишнього середовища

Техносфера - це сфера життєдіяльності людини, яка включає в себе всі штучно створені об'єкти і системи, а також їх вплив на навколишнє середовище. Вона постійно розвивається і розширюється, що призводить до зростання антропогенного навантаження на біосферу.

Екологічні чинники техносфери - це фактори, які впливають на стан навколишнього середовища в результаті діяльності людини. Вони можуть бути прямими і непрямими, короткочасними і тривалими, локальними і глобальними.

До прямих екологічних чинників техносфери відносяться ті, які безпосередньо впливають на навколишнє середовище. До них належать:

• Забруднення атмосфери - це надходження в атмосферу шкідливих речовин, які можуть негативно впливати на здоров'я людини, рослин і тварин. Забруднюючі речовини можуть надходити в атмосферу в результаті спалювання палива, промислового виробництва, автотранспорту, сільськогосподарської діяльності тощо.

• Забруднення води - це надходження в воду шкідливих речовин, які можуть погіршувати її якість і робити її непридатною для використання. Забруднюючі речовини можуть надходити в воду в результаті промислового виробництва, сільського господарства, побутових стоків тощо.

• Забруднення ґрунту - це надходження в ґрунт шкідливих речовин, які можуть пошкоджувати рослини, тварин і навіть людей. Забруднюючі речовини можуть надходити в ґрунт в результаті промислового виробництва, сільського господарства, діяльності транспорту тощо.

• Шум - це фізичний фактор, який може негативно впливати на здоров'я людини. Шум може виникати в результаті роботи промислового обладнання, автотранспорту, авіації тощо.

• Іонізуюче випромінювання - це фізичний фактор, який може викликати рак і інші захворювання. Іонізуюче випромінювання може надходити в навколишнє середовище в результаті роботи атомних електростанцій, промислових підприємств, медичних закладів тощо.

• Радіоактивні відходи - це небезпечні відходи, які містять радіоактивні речовини. Радіоактивні відходи можуть утворюватися в результаті роботи атомних електростанцій, промислових підприємств, військових об'єктів тощо.

До непрямих екологічних чинників техносфери відносяться ті, які впливають на навколишнє середовище опосередковано. До них належать:

• Зміна клімату - це зміна середньої температури повітря і інших кліматичних параметрів. Зміна клімату може бути викликана багатьма факторами, в тому числі і антропогенним впливом.

• Знищення лісів - це зменшення площі лісів. Ліси відіграють важливу роль в регулюванні клімату, збереженні біорізноманіття та очищенні води.

• Знищення озонового шару - це зменшення концентрації озонового шару в атмосфері. Озоновий шар захищає Землю від шкідливого впливу ультрафіолетового випромінювання.

• Закислення ґрунтів - це підвищення кислотності ґрунтів. Закислення ґрунтів може бути викликано викидами в атмосферу сірководню, азоту та інших кислотних сполук.

• Надмірне використання природних ресурсів - це використання природних ресурсів у більших обсягах, ніж вони можуть відновлюватися. Надмірне використання природних ресурсів може призвести до їх виснаження і деградації екосистем.

Короткочасні екологічні чинники техносфери - це ті, які впливають на навколишнє середовище протягом короткого періоду часу. До них належать, наприклад, викиди шкідливих речовин в атмосферу в результаті аварії на промисловому підприємстві.

Тривалі екологічні чинники техносфери - це ті, які впливають на навколишнє середовище протягом тривалого періоду часу. До них належать, наприклад, зміна клімату в результаті викидів парникових газів.

Локальні екологічні чинники техносфери - це ті, які впливають на навколишнє середовище в обмеженому просторі. До них належать, наприклад, забруднення повітря в результаті роботи промислового підприємства, забруднення води в результаті аварії на очисних спорудах тощо.

Глобальні екологічні чинники техносфери - це ті, які впливають на навколишнє середовище в масштабах всієї планети. До них належать, наприклад, зміна клімату, знищення озонового шару, надмірне використання природних ресурсів тощо.

Екологічні чинники техносфери мають значний вплив на навколишнє середовище. Вони можуть призводити до забруднення повітря, води і ґрунту, знищення лісів, зміни клімату, виснаження природних ресурсів тощо.

Забруднення навколишнього середовища може негативно впливати на здоров'я людини, рослин і тварин. Воно може викликати такі захворювання, як рак, астма, серцево-судинні захворювання тощо.

Знищення лісів може призвести до таких проблем, як зміна клімату, деградація ґрунтів, ерозія земель тощо.

Зміна клімату може призвести до таких проблем, як підвищення рівня моря, зміни в розподілі опадів, зростання частоти і інтенсивності стихійних лих тощо.

Виснаження природних ресурсів може призвести до таких проблем, як дефіцит енергії, продовольства, води тощо.

Заходи щодо зменшення впливу екологічних чинників техносфери на навколишнє середовище.

Для зменшення впливу екологічних чинників техносфери на навколишнє середовище необхідно вжити таких заходів:

• Впровадження екологічно чистих технологій. Використання екологічно чистих технологій дозволяє зменшити викиди шкідливих речовин в навколишнє середовище.

• Впровадження систем екологічного контролю. Системи екологічного контролю дозволяють відстежувати стан навколишнього середовища і вчасно виявляти і усувати джерела забруднення.

• Охорона природи. Охорона природи дозволяє зберігати природні екосистеми і запобігати їх деградації.

Впровадження цих заходів дозволить зменшити антропогенний вплив на навколишнє середовище і забезпечити його стійкий розвиток.

ВИСНОВКИ

1. На початку дослідження наголошено на значному розвитку кіберрозвідки в інформаційному просторі. Сказано, що крім комерційної кіберрозвідки існують також і проникнення, за які передбачається кримінальна відповідальність (парсинг на іноземні держави в військових департамента). Тому для захисту від різних атак та спроб вторгнення порушників з метою попередження можливих загроз необхідний аналіз та реєстрування ризиків кібербезпеки, а також впровадження комплексу дій, що охоплюють науково-дослідні роботи в області захисту інформації в кіберпросторі.

2. Описано основні підходи сучасних науковців та законодавчих органів до тлумачення поняття «кіберрозвідка». Для найбільш вдалого тлумачення дано розширений коментар. Описано головні етапи проведення кіберрозвідки та вказано умови автоматизації процесу.

3. Детально розглянуто такі комерційні платформи для комерційної кіберрозвідки, як Anomali ThreatStream, Anomali Enterprise, ThreatConnect, TC Identify, TC Manage, TC Analyze, ThreatConnect CAL, TC Complete, ThreatQ та дано їх переваги перед конкурентами.

4. Проаналізовано підходи до класифікації типів кіберрозвідки та коротко проаналізовано основні. Зроблено аналіз моделей та методів захисту кіберпростору (стандарти аналізу ризиків, NIST, методологія Azure та ISO 2700x) та зроблено порівняння методів оцінки ризиків.

5. Окремо дана характеристика методу пошуку максимальної кількості індикаторів компрометації (IoC) та їх розповсюдження. Індикатори компрометації – це життєво необхідна складова для багатьох рівнів захисту інфраструктури. Їх можна використовувати як на рівні мережі, так і на рівні хосту. Кожен день з’являються нові атаки, які занадто складно відстежувати

спеціалісту з кібербезпеки, або навіть команді спеціалістів. Саме тому існують такі проекти для розповсюдження індикаторів компрометації, як MISP, що дають можливість компаніям ділитись між собою атаками, які вони вже змогли виявити. Прикладами IoC є адреси командних серверів ботнетів, електронні адреси розсильників фішингових листів і спаму, сигнатури вірусів, хеш-суми шкідливих файлів.

6. В другій частині дослідження зроблено опис розробленого методу аналізу APT. Представлено виявлені індикатори технік MITRE, які призначені для першого етапу методу – фільтрації подій та зменшення їх кількості шляхом пошуку застосування технік у подіях. Описано програмну реалізацію, яка покриває інші етапи методу аналізу, зокрема підходи до побудови послідовності подій та хронології виявленої APT атаки шляхом виявлення кібератак на основі індикаторів компрометації.

7. Досліджено етап фільтрації подій та особливості опису індикаторів технік для фільтрації подій шляхом застосування технік MITRE та співставлення із життєвим циклом APT атаки. Наведено програмну реалізацію розробленого методу. Для коректного розбору даних за полями було реалізовані спеціальні типи даних. У класі Event. java описано тип даних для події, отриманої із файлу з кореляційними подіями від Sysmon та Powershell. Побудова ребер графу відбувається у наступній послідовності: спочатку визначаються взаємозв’язки між датою та цільовими процесами, що були використані у відповідний день, далі відбувається пошук тих подій, де дата та цільовий процес має заданий рівень схожості із наявними вершинами та ребрами, та будує ребро від процесу до знайденого командного рядка у розрізі певної дати.

8. В практичній частині дослідження зроблено визначення особливостей APT-атак та мети досліджень. Описано вибір моделі APT-атаки та розробку моделі поведінки BD. В якості альтернативного методу оцінки індикаторів компрометації запропоновано рішення, де базове значення вираховується як комбінація QoD (Quality of Detection), FPR (False Positive Rate), а також додається

значення швидкості спадання з логістичною функцією. Для запропонованого методу проведено практичну реалізацію та результат представлено у графічному вигляді. Використано скорингову систему до даних, зібраних про шкідливе програмне забезпечення Regin, для якого було виявлено 33 хеші та 17 false positive хешів. Побудовано візуалізацію оцінки індикатора компрометації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.
2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 р. № 96 / 2016. Офіційний вісник України. 2016. № 23. Ст. 899.
3. Архипов О. Є. Адаптивний підхід до обробки даних експертного оцінювання при вирішенні завдань у сфері захисту інформації. *Захист інформації*. 2019. Т. 21, № 3. С. 158–167.
4. Бурячок В. Л. Соціальна інженерія як метод розвідки інформаційнотелекомунікаційних систем. *Захист інформації.* 2012. № 4 (57). С. 5–12.
5. Бучик С. С. Методика оцінювання інформаційних ризиків в автоматизованій системі. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*. Житомир: ЖВІ ДУТ, 2015. Вип. 11. С. 33.
6. Веселова Л. Ю. Кібернетичні загрози у контексті сучасного сприйняття їх в Україні. *Вісник Харківського національного університету імені В. Н. Каразіна.* Серія «Право». 2020. Вип. 29. С. 169–175.
7. Гайдур Г. І. Механізм функціонування цілісної інформаційної системи в умовах кібернетичного впливу. *Сучасний захист інформації.* 2019. № 4 (40). С. 22–26.
8. Галахов С. М. Розвиток моделей кібератак у площині інформаційної безпеки підприємства. *Телекомунікаційні та інформаційні технології.* 2019. № 4 (65). С. 12–24.
9. Гільгурт С. Методи побудови оптимальних схем розпізнавання для реконфігуровних засобів інформаційної безпеки. *Безпека інформації.* 2019. Т. 25, № 2. С. 74–81.

10. Джулій В. М. Метод виявлення та протидії розподіленим атакам, спрямованим на відмову в обслуговуванні. *Вісник Хмельницького національного університету. Серія: Технічні науки*. 2019. № 2. С. 122–127.
11. Довбешко С. В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. *Сучасний захист інформації*. 2019. № 1 (37). С. 6–15.
12. Журиленко Б. Є. Метод проектування та оцінка працюючого одиночного технічного захисту інформації за обраним напрямом злому. *Захист інформації.* 2019. Т. 21, № 3. С. 143–149.
13. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах. *Системи обробки інформації. Л.: Академія сухопутних військ імені гетьмана Петра Сагайдачного*, 2015. Вип. 3 (128). С. 75–79.
14. Кирилов В. А. Система збору та кореляції подій (SIEM) як ядро системи інформаційної безпеки. *Вісник технологічного університету*. 2016. №13. С. 135.
15. Ковальов І. Оцінка ризиків інформаційної безпеки з використанням алгоритму нечіткої кластеризації k-середніх. Дніпро, 2018. 78 с.
16. Козак Н., Цимбал П., Варшавець Я. Деякі аспекти виявлення і попередження інцидентів кібербезпеки. URL: http: // ir. nusta. edu. ua / jspui / bitstream / 123456789 / 2339 / 1 / 2219_IR. pdf (дата звернення: 1.11.2023).
17. Корченко О. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія. Київ, 2017. 435 с.
18. Корченко О. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія. К., 2017. 435 с.
19. Куцаєв В. В., Радченко М. М., Терещенко Т. П. Модель оцінки готовності інформаційно-телекомунікаційного вузла зв’язку в умовах кібернетичних атак. *Захист інформації.* 2015. № 3. С. 43–50.

20. Леонов Б. Д. Удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності. *Інформація і право*. 2019. № 4 (31). С. 98–106.
21. Макеев А. С. Менеджмент рисков информационной безопасности как непрерывный процесс. *Молодий учений.* 2016. №10. С. 62–66.
22. Мельник М. О. Аналіз побудови моделі політики інформаційної безпеки підприємства. *Системи обробки інформації.* 2017. Вип. 2. С. 126–128.
23. Микитенко Т. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України ім. І. Черняховського*. 2016. № 2. С. 24–31.
24. Моделювання кібератак засобами теорії графів. *Сучасний захист інформації.* 2019. № 4 (40). С. 6–11.
25. Мохор В. В. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури. *Ядерна та радіаційна безпека*. 2019. № 2 (82). С. 57–61.
26. Платоненко А. В. Сучасні загрози інформаційної безпеки для державних та приватних установ України. *Сучасний захист інформації*. 2015. №4. С. 86–90.
27. Пузиренко О. Г. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційнотелекомунікаційних систем. *Системи обробки інформації.* Л.: Академія сухопутних військ імені гетьмана Петра Сагайдачно го, 2014. Вип. 8 (124). С. 128–134.
28. Рудий Т. Засади захисту інформації в інформаційних системах підприємств. *Актуальні проблеми економіки.* № 2 (152). 2014. С. 551–557.
29. Савельєва Т., Панаско О., Пригодюк О. Аналіз методів і засобів для реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2018. Т. 1, № 4. С. 81–89.

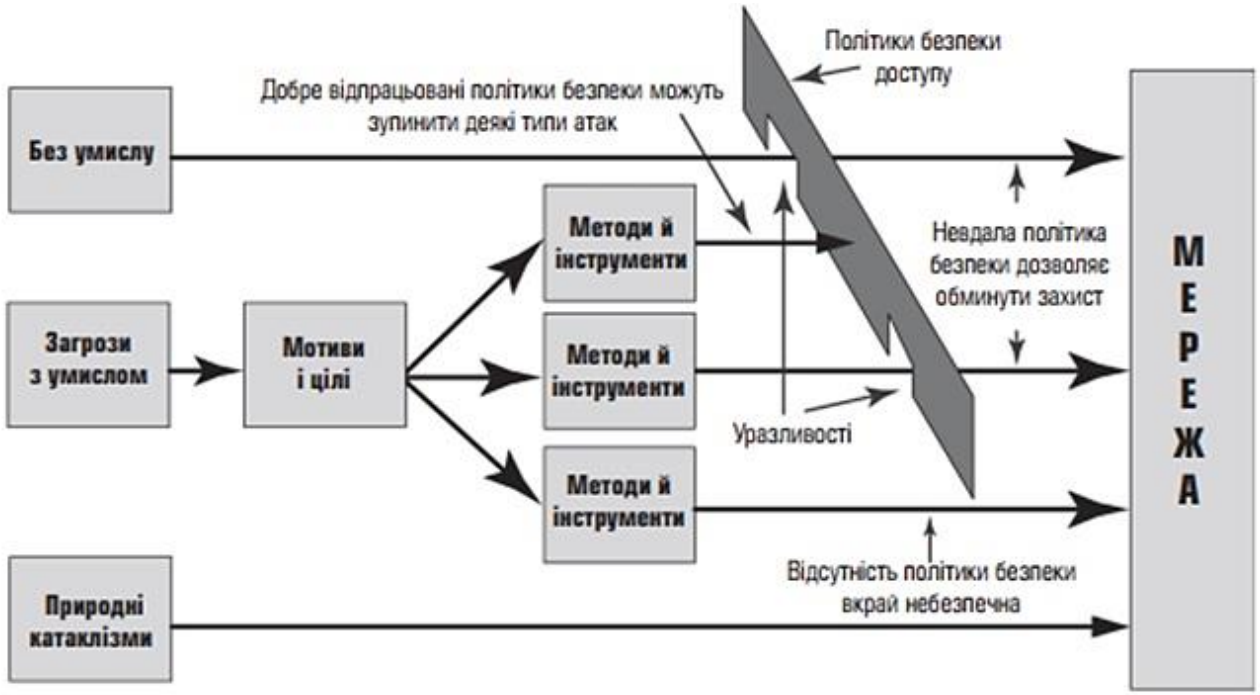
30. Савченко В. А. Управління ризиками кібербезпеки на основі теоретико-ігрового підходу. *Сучасний захист інформації.* 2019. № 2 (38). С. 6–16.
31. Северина С. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету.* 2016. № 1. С. 155–161.
32. Сорокін Д. В. Інфраструктура промислових мереж IoT та кіберзагрози в доступі при використанні IoT рішень. *Телекомунікаційні та інформаційні технології.* 2019. № 4 (65). С. 120–127.
33. Ступень П. В. Моделювання характеристик обладнання комп'ютерних мереж у ракурсі інформаційної безпеки. *Вісник Черкаського державного технологічного університету. Серія: Технічні науки*. 2019. № 4. С. 42–48.
34. Твердохліб І. Управління інцидентами кібербезпеки на малих комерційних підприємствах. Дніпро, 2018. 132 с.
35. Ткаченко В. Кібератаки в автоматичному режимі. Мережі і бізнесю. 2019. № 6 (109). С. 52.
36. Ткаченко І. В. Спосіб організації оцінки стану кіберзахисту критичної інформаційної інфраструктури в режимі реального часу з урахуванням індикаторів кіберзагроз. *Сучасний захист інформації.* 2019. № 4 (40). С. 88–93.
37. Толюпа С. Вплив кібернетичних атак на інформаційну систему. *Педагогічні інновації: ідеї, реалії, перспективи*. 2017. Вип. 2. С. 83–87.
38. Федорченко А. В. Кореляція інформації в системах на основі графа зв'язків типів подій. Санкт-Петербург: Університет ІТМО, 2018. 67 с.
39. Хоменко В. М., Савченко В. О. Косиченко О. О. Проблеми латентності кіберзлочинності. *Використання сучасних інформаційних технологій в діяльності національної поліції України*. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. С. 136–141.
40. Чередниченко О. Ю., Процюк Ю. О., Шемендюк О. В., Мальцева І. Р. Способи вдосконалення схем захисту від кібернетичних атак в інформаційно-телекомунікаційних системах. *Захист інформації.* 2015. № 5. С. 103–109.

41. Чеховська М. М. Кібершпигунство як загроза національній безпеці. *Актуальні проблеми управління інформаційною безпекою держави.* Київ: Наук-вид. відділ НА СБ України, 2012. С. 232–234.
42. Шевченко А. Аналіз застосування методів машинного навчання на основі штучних нейронних мереж для виявлення кіберзагроз. *Information Technology and Security*. January-June 2019. Vol. 7, Iss. 1 (12). P. 79–90.
43. Шлапаченко В. М. Шпигунство як діяльність зі здобування інформації / В. М. Шлапаченко // Інформаційна безпека людини, суспільства, держави. К., 2015 р. 1 (17). С. 99–109.
44. Шудрова К. Соціальна інженерія в інформаційній безпеці. *Директор з безпеки.* 2012. № 10. С. 13–17.
45. Carson Zimmerman. Ten Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation, 2014. [Online]. URL: https: // www. mitre. org / sites / default / files / publications / pr – 13–1028-mitre – 10-strategiescyber-ops-center. pdf (дата звернення: 1.11.2023).
46. Charies K. OpenVAS Terms to Know. Keller Charies. 2018. Режим доступу: https: // securityorb. com / general-security / openvas-term-to-know (дата звернення: 1.11.2023).
47. Chen P. A study on Advanced Persistent Threats. *iMinds-DistriNet, KU Leuven* – 2014. URL: http: // zempirians. com / ebooks / 2014-apt-study. pdf (дата звернення: 1.11.2023).
48. Gylling A., Eliasson P. Mapping cyber threat intelligence to probabilistic attack graphs. *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience*, CSR 2021, Virtual, Rhodes. 2021. P. 304–311.
49. Derek Young, Juan Lopez Jr., Mason Rice, Benjamin Ramsey. A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*. Vol. 14. 2016. P. 43–57.

50. Indicators of Compromise (IoCs) and Their Role in Attack Defence. UK National Cyber Security Centre. 2021. URL: https: // datatracker. ietf. org / doc / html / draft-paine-smart-indicators-of-compromis e – 02 (дата звернення: 1.11.2023).
51. Jain P., Pasman H. J., Waldram S. Process Resilience Analysis Framework. *Journal of Loss Prevention in the Process Industries*. 2018. Vol. 53. P. 61–73.
52. Jinsoo Shin, Hanseong Son, Gyunyoung Heo. Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET. *Nuclear Engineering and Technology*. Vol. 49. Issue 3. 2017. P. 517–524.
53. Malhotra A., Rawat L., Kumar L. Mini security operations center using elk. International Research Journal of Modernization in Engineering Technology and Science. 2020. № 02 (11). P. 461–466.
54. MITRE. URL: https: // attack. mitre. org (дата звернення: 1.11.2023).
55. NIST. Managing Information Security Risk: Organization, Mission, and Information System View Approach URL: https: // tsapps. nist. gov / publication / get_pdf. cfm? pub_id=908030 (дата звернення: 1.11.2023).
56. Panwar A. iGen: Toward Automatic Generation and Analysis of Indicators of Compromise (IOCs) using Convolutional Neural Network. A. Panwar. 2016. URL: https: // repository. asu. edu / items / 44216 (дата звернення: 1.11.2023).
57. Petar Radanlieva. Future developments in cyber risk assessment for the internet of things. *Computers in Industry*. Vol. 102. 2018. P. 14–22.
58. Time-Dependent Analysis of Attacks / F. Arnold, H. Hermanns. *Principles of Security and Trust*. 2014. URL: https: // link. springer. com / chapter / 10.1007%2F978–3–642–54792–8_164. (дата звернення: 1.11.2023).
59. Vulfin A. M. Cyber Threat Intelligence Data Management System. *Modeling, Optimization and Information Technology*. 2021;9 (1). URL: https: // moitvivte. com / ru / journal / pdf? id=925 (дата звернення: 1.11.2023).
60. Anti-Malware/ URL: https: // www. anti-malware. com / practice / methods / threat-intelligence-platform/ (дата звернення: 1.11.2023).

ДОДАТКИ

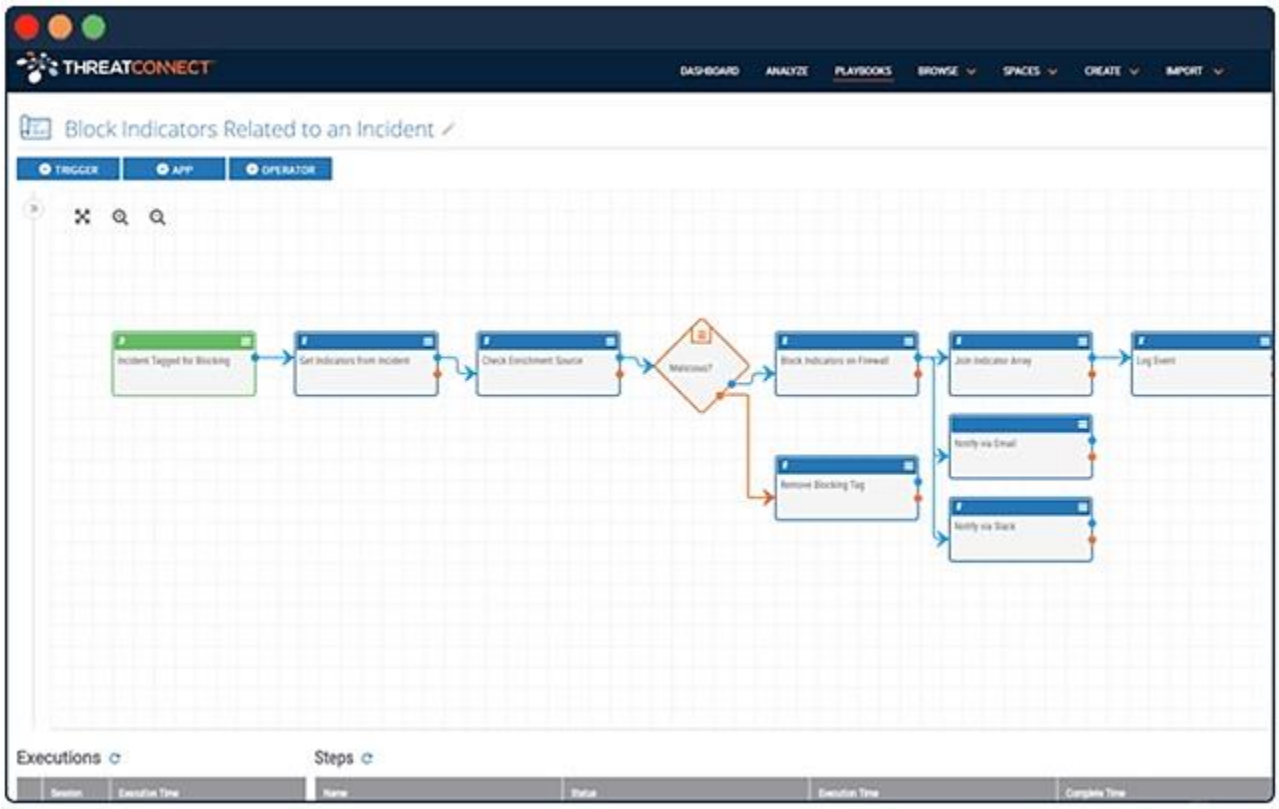
Додаток А. Алгоритм реалізації кібератаки



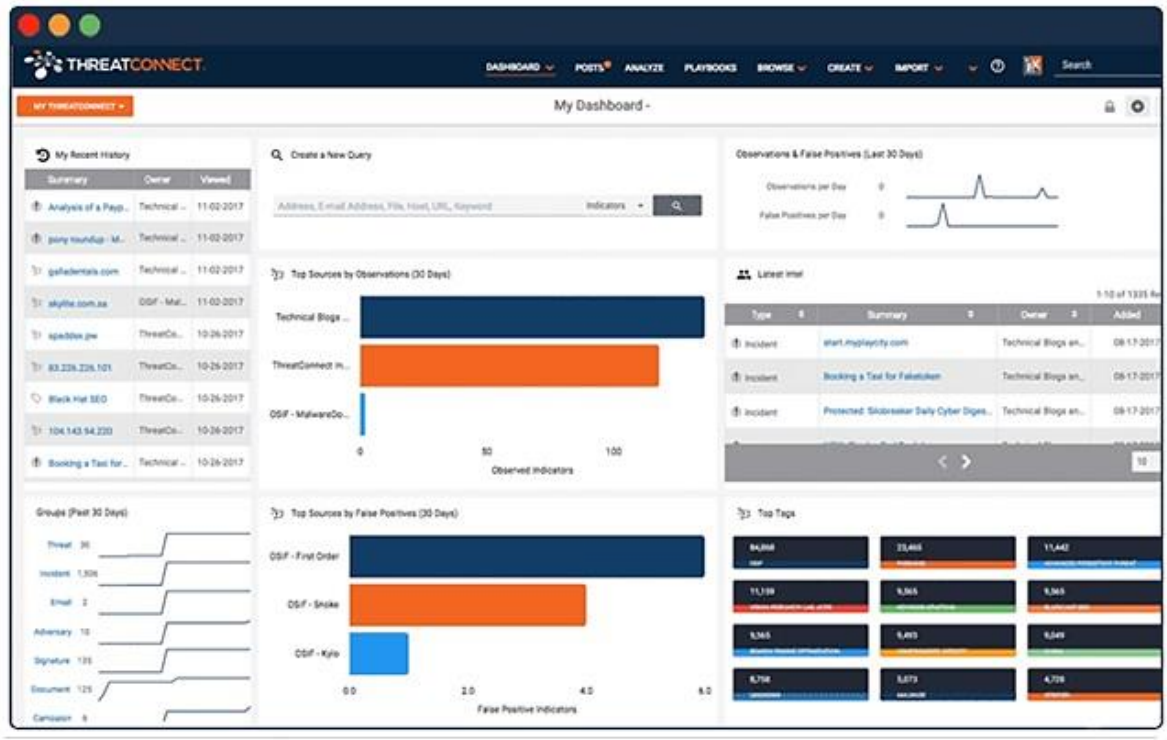
Додаток Б. Головні підходи до здійснення кіберрозвідки

Додаток В. Основні загрози інформаційної безпеки

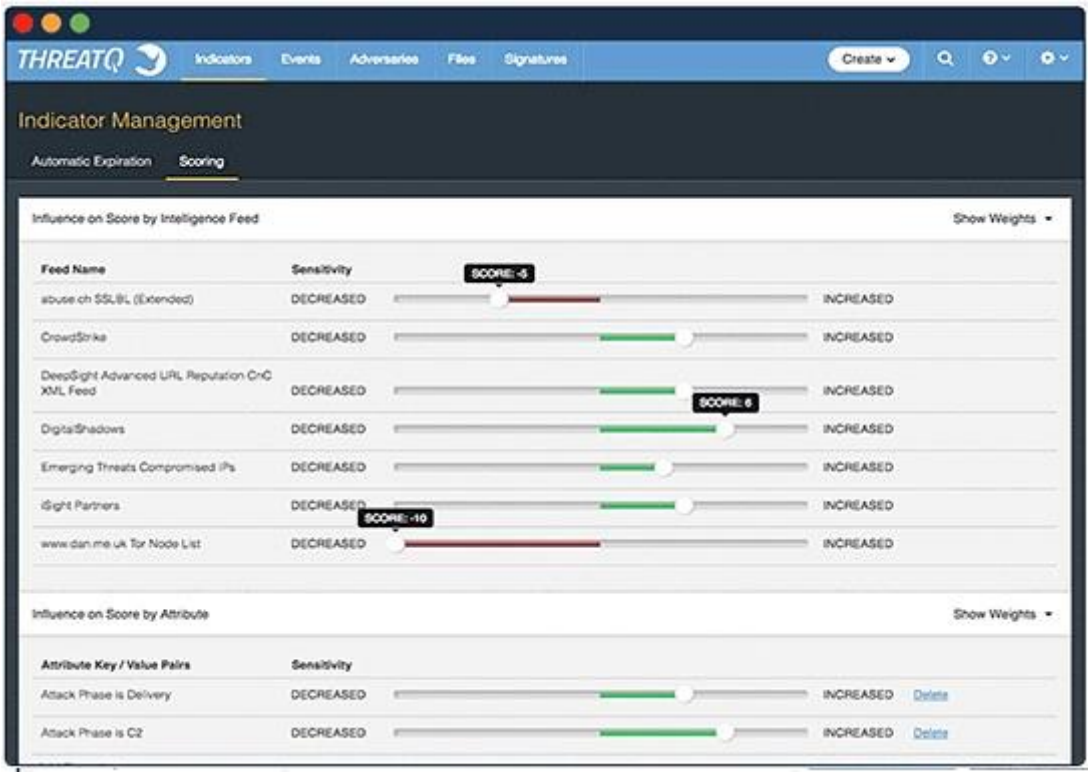
Додаток Г Робоче вікно ThreatConnect: Playbook



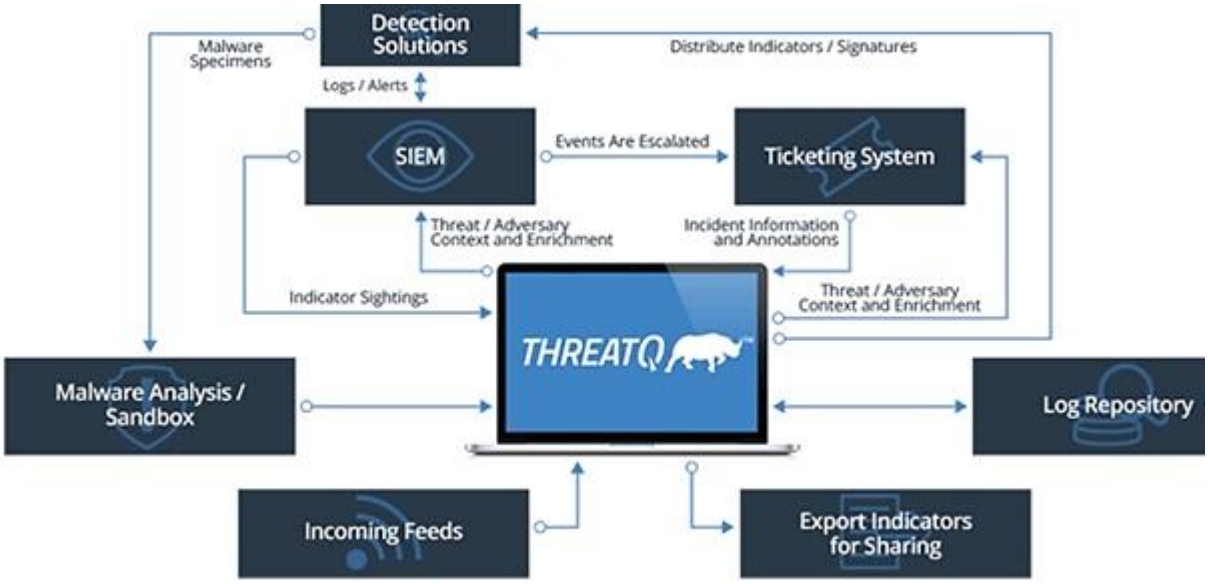
Додаток Д. Робоче вікно ThreatConnect: Dashboard



Додаток Е. Робоче вікно ThreatQ Self-Tuning: налаштування



Додаток Ж. Робоче вікно ThreatQ: архітектурне рішення



Додаток З. Етапи створення комплексної системи захисту інформації

Додаток И. Фрагмент програмного коду реалізованого методу

Techniques. java

```
package fuzzystringsearch;

/**
 *
 * @author ira
 */
public class Techniques {
        private int id;
        private String idTec;
    private String Name;

    public int getId() {
        return id;
    }
        public void setId(int id) {
        this.id = id;
    }
        public String getIdTec() {
        return idTec;
    }
        public void setIdTec(String idTec) {
        this.idTec = idTec;
    }
    public String getName() {
        return Name;
    }
        public void setName(String Name) {
        this.Name = Name;
    }

    @Override
    public String toString(){
        return "ID of tactic="+id+",ID of technique="+idTec+",Name="+Name+"\n";
    }
}
```

Tactics. java

```
package fuzzystringsearch;

/**
 *
 * @author ira
 */
public class Tactics {
        private int id;
    private String Tactic;
        private String Name;

    public int getId() {
        return id;
    }
        public void setId(int id) {
        this.id = id;
    }

    public String getName() {
        return Name;
    }
        public void setName(String Name) {
        this.Name = Name;
    }

    public String getTactic() {
        return Tactic;
    }
        public void setTactic(String Tactic) {
        this.Tactic = Tactic;
    }

        @Override
    public String toString(){
        return "ID="+id+",Name="+Name+",Tactic="+Tactic+"\n";
    }

}
```

ParserCsv. java

```
import static fuzzystringsearch.Levenstein.distance;
import java.io.FileReader;
import java.io.IOException;
import java.util.ArrayList;
import java.util.List;
import org.apache.commons.csv.CSVFormat;
import org.apache.commons.csv.CSVParser;
import org.apache.commons.csv.CSVRecord;
import java.util.HashMap;
import java.util.LinkedHashMap;
import java.util.Map;
import java.util.stream.Collectors;

public class ParserCsv  {

        public List<Event> parsingAll () throws IOException {
            List<Event> emps = new ArrayList();
            CSVFormat format = CSVFormat.EXCEL.withHeader().withDelimiter(';');
            CSVParser parser = new CSVParser(new FileReader("/Users/ira/Downloads/th_events_all_rows.csv"), format);
            for(CSVRecord record : parser){
            Event event = new Event();
            event.setId(record.get("ID"));
            event.setName(record.get("Name"));
                        event.setDate(record.get("Date"));
            event.setTime(record.get("Time"));
                        event.setDeviceHostName(record.get("Event-Device Host Name"));
            event.setSourceProcessName(record.get("Event-Source Process Name"));
            event.setDestinationAddress(record.get("Event-Destination Address"));
            event.setDestinationPort(record.get("Event-Destination Port"));
                        event.setDestinationUserName(record.get("Event-Destination User Name"));
            event.setDestinationProcessName(record.get("Event-Destination Process Name"));
            event.setFilePath(record.get("Event-File Path"));
            event.setFileHash(record.get("Event-File Hash"));
                        event.setDC1(record.get("Event-Device Custom String1"));
            event.setDC2(record.get("Event-Device Custom String2"));
            event.setDC3(record.get("Event-Device Custom String3"));
                        event.setDC5(record.get("Event-Device Custom String5"));
            event.setDC6(record.get("Event-Device Custom String6"));
            emps.add(event);
        }
        parser.close();
                return emps;
        }

 public List<Event> parsingAll2 () throws IOException {
     List<Event> emps = new ArrayList();
     CSVFormat format = CSVFormat.EXCEL.withHeader().withDelimiter(';');
     CSVParser parser = new CSVParser(new FileReader("/Users/ira/Downloads/new_all_rows.csv"), format);
     for(CSVRecord record : parser){
     Event event = new Event();
     event.setId(record.get("ID"));
     event.setName(record.get("Name"));
                 event.setDate(record.get("Date"));
     event.setTime(record.get("Time"));
                 event.setDeviceHostName(record.get("Event-Device Host Name"));
     event.setSourceProcessName(record.get("Event-Source Process Name"));
     event.setDestinationAddress(record.get("Event-Destination Address"));
     event.setDestinationPort(record.get("Event-Destination Port"));
                 event.setDestinationUserName(record.get("Event-Destination User Name"));
     event.setDestinationProcessName(record.get("Event-Destination Process Name"));
     event.setFilePath(record.get("Event-File Path"));
     event.setFileHash(record.get("Event-File Hash"));
                 event.setDC1(record.get("Event-Device Custom String1"));
     event.setDC2(record.get("Event-Device Custom String2"));
     event.setDC3(record.get("Event-Device Custom String3"));
                 event.setDC5(record.get("Event-Device Custom String5"));
     event.setDC6(record.get("Event-Device Custom String6"));
     emps.add(event);
 }
     parser.close();
     return emps;
 }
```

```
public List<Event> parsingAllCmdExc (List<Event> emps,  List<String> cmd) throws IOException {
        List<Event> emps1=emps;
        List<Event> list=new ArrayList();
        for(Event record : emps1){
            for(String val : cmd){
            if(record.getDC1().equals(val) ){
                list.add(record);
            }
        }
    }
    emps1.removeAll(list);
    return emps1;
}

public List<Event> parsingAllHostExc (List<Event> emps,  List<String> host) throws IOException {
    List<Event> res=emps;
    List<Event> list=new ArrayList();
    for(Event record : res){
        for(String val : host){
        if(record.getDeviceHostName().contains(val) ){
                list.add(record);
        }
    }
    }
    res.removeAll(list);
    return res;
}


public List<String> parsingHostExc () throws IOException {
    List<String> host = new ArrayList();
    CSVFormat format = CSVFormat.EXCEL.withHeader().withDelimiter(';');
    CSVParser parser = new CSVParser(new FileReader("/Users/ira/Downloads/hosts_exc.csv"), format);
    for(CSVRecord record : parser){
                String k = record.get(0);
    host.add(k);
}
parser.close();
        return host;
}

public List<String> parsingCmdExc () throws IOException {
    List<String>  cmd= new ArrayList();
    CSVFormat format = CSVFormat.EXCEL.withHeader().withDelimiter(';');
    CSVParser parser = new CSVParser(new FileReader("/Users/ira/Downloads/cmd_exc.csv"), format);
    for(CSVRecord record : parser){
                String k = record.get(0);
    cmd.add(k);
}
parser.close();
        return cmd;
}

public List<IdTechniques> parsingTechniques () throws IOException {
    List<IdTechniques> idtec = new ArrayList();
    CSVFormat format = CSVFormat.EXCEL.withHeader().withDelimiter(';');
    CSVParser parser = new CSVParser(new FileReader("/Users/ira/Downloads/all_techniques.csv"), format);
    for(CSVRecord record : parser){
    IdTechniques event = new IdTechniques();
    event.setId(record.get("ID"));
    event.setName(record.get("Name"));
    idtec.add(event);
}
parser.close();
        return idtec;
}
```