# НАУКОВА РОБОТА

ТЕМА**:** “Спосіб формування шаблону індикаторів компрометації для каналу дистанційного управління APT-атакою”

ШИФР “Кіберканал”

# ЗМІСТ

АНОТАЦІЯ……..……...3
ПЕРЕЛІК ВИКОРИСТАНИХ СКОРОЧЕНЬ ……..……....4
ВСТУП ……..……..…5
1. ВИЗНАЧЕННЯ ОСОБЛИВОСТЕЙ APT-АТАК ТА МЕТИ ДОСЛІДЖЕНЬ…6
2. ВИБІР МОДЕЛІ APT-АТАКИ ……...……..…….…...8
3. РОЗРОБКА МОДЕЛІ ПОВЕДІНКИ BD……..……...11
4. ВИЗНАЧЕННЯ ВІДПОВІДНОСТІ ПРОЦЕДУР УПРАВЛІННЯ В РАМКАХ BD ТА ЕЛЕМЕНТАРНИХ ПОДІЙ ITS ……..12
5. РОЗРОБКА СПОСОБУ ФОРМУВАННЯ ШАБЛОНУ ДЛЯ ВИЗНАЧЕННЯ BD APT-АТАКИ ……...14
ВИСНОВКИ ……..……..……..17
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ……...……..18

# АНОТАЦІЯ

наукової роботи “Спосіб формування шаблону індикаторів компрометації для визначення каналу дистанційного управління APT-атакою”

ШИФР “Кіберканал”

Широкомасштабне застосування проти національної критичної інфраструктури складних кібератак типу APT (Advanced Persistent Threat, вдосконала стійка загроза, або цільова атака) стало потужним стимулом для розвитку методів проактивного кіберзахисту. Характерним для APT-атак (далі, APTs) є:

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.

Основою багатьох APTs є використання зловмисником несанкціонованих каналів дистанційного управління через Інтернет (backdoor, BD), що дозволяють йому виконувати різні дій в кіберпросторі системі інформаційних технологій (Information Technology System, IT-system, далі – ITS, IT-система) жертви. Актуальним стає завдання своєчасного визначення BD ще на етапі підготовки цільової акції атаки. Такій підхід відповідає реалізації проактивної стратегії кіберзахисту.

За результатами досліджень інформаційних процесів формування та експлуатації BD в рамках атаки, організації процесів систем проактивного кіберзахисту розроблено спосіб формування шаблону індикаторів компрометації, що може бути використаний системою управління інформацією і подіями безпеки (SIEM) для визначення (детектування) несанкціонованих каналів дістанційного управління атакою.

Спосіб розроблено на основі використання кібернетичної моделі APT-атаки та застосування методів формалізованого аналізу інформаційних процесів сучасних систем оперативного кіберзахисту. На основі способу розроблено та реалізовано процедуру формування та використання багатоіндикаторного шаблону.

Теоретичні та практичні результати досліджень орієнтовано на застосування у складі центру операцій кібербезпеки (SOC) корпоративної IT-системи у рамках автоматизації процедур кіберзахисту.

Результати досліджень відображені у двох наукових публікаціях (тези доповідей на науково-технічних конференціях) та впроваджені в систему оперативного кіберзахисту корпоративної IT-системи (довідка про впровадження).

Відомості про наукові публікації авторів знаходяться в окремому конверті.

## ПЕРЕЛІК ВИКОРИСТАНИХ СКОРОЧЕНЬ

A - Actuator (актуатор, виконавчий пристрій)
APT - Advanced Persistent Threat
BD - backdoor (несанкціонований канал дистанційного управління)
FW - firewall (файервол, брандмауер, міжмережевий екран)
ITS - IT-system (система інформаційних технологій)
CD - Cyber Defense (кіберзахист)
CTI - Cyber Threat Intelligence (розвідка кіберзагроз)
IoC - Indicators of Compromise (індикатори компрометації)
IDS/IPS - Intrusion Detection System/ Intrusion Protection System (система виявлення вторгнень/система захисту від вторгнень)
SIEM - Security Information and Event Management (управління інформацією і подіями безпеки)
SOC - Security Operation Centre (центр операцій безпеки)
S - Sensor (сенсор, датчик)

# ВСТУП

Широкомасштабне застосування проти національної критичної інфраструктури складних кібератак типу APT (Advanced Persisten Threat, вдосконала стійка загроза, або цільова атака) стало потужним стимулом для розвитку методів проактивного кіберзахисту. Характерним для APT-атак (далі, APTs) є:

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.

Основою багатьох APTs є використання зловмисником несанкціонованих каналів дистанційного управління через Інтернет (backdoor, BD), що дозволяють йому виконувати різні дій в кіберпросторі системі інформаційних технологій (Information Technology System, IT-system, далі – ITS, IT-система) жертви. Актуальним стає завдання своєчасного визначення BD ще на етапі підготовки цільової акції. Такій підхід відповідає реалізації проактивної стратегії кіберзахисту.

**Об'єкт досліджень** – кіберзахист корпоративних IT-систем від APT-атак.

**Предмет дослідження** – детектування несанкціонованого каналу дистанційного управління через Інтернет в рамках APT-атаки. З метою встановлення оперативного контролю над цією атакою.

**Мета** – встановлення оперативного контролю над APT-атакою.

**Наукове завдання** – розробка на основі формалізованих моделей інформаційних процесів APT-атак і систем оперативного кіберзахисту способу формування шаблону індикаторів компрометації, що дозволяє в рамках SIEM визначати (детектувати) канали несанкціонованого дистанційного управління.

У рамках досліджень були виконані наступні часткові завдання:

1) формалізований аналіз інформаційних процесів формування та застосування несанкціонованих каналів дистанційного управління (backdoor, BD) в рамках APT-атаки;
2) вибір моделі APT-атаки;
3) розробка моделі поведінки BD;
4) визначення відповідності процедур управління в рамках BD та елементарних подій ITS;
5) розробка структури шаблону BD.

## 1. Визначення особливостей APT-атак та мети досліджень

Аналіз різних інформаційних джерел [1-7] 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) [5, 6, 9] 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

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. Такій підхід відповідає реалізації проактивної стратегії кіберзахисту, метою якої є переривання APT-атаки ще до початку етапу цільової акції [8, 11].

Аналіз різних доступних джерел [1-10] 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.

**2. Вибір моделі APT-атаки**

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 [1] - [4]. 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 [5] - [10] описує атаку за допомогою різних математичних конструкції (графи, логічні елементи, мурашиний алгоритм оптимізації, приховані Марківськи 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 [7].

За основу досліджень цей роботи була прийнята кібернетична модель APT-атаки [10, 8]. 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 представлена послідовністю циклів управління (рис.1):

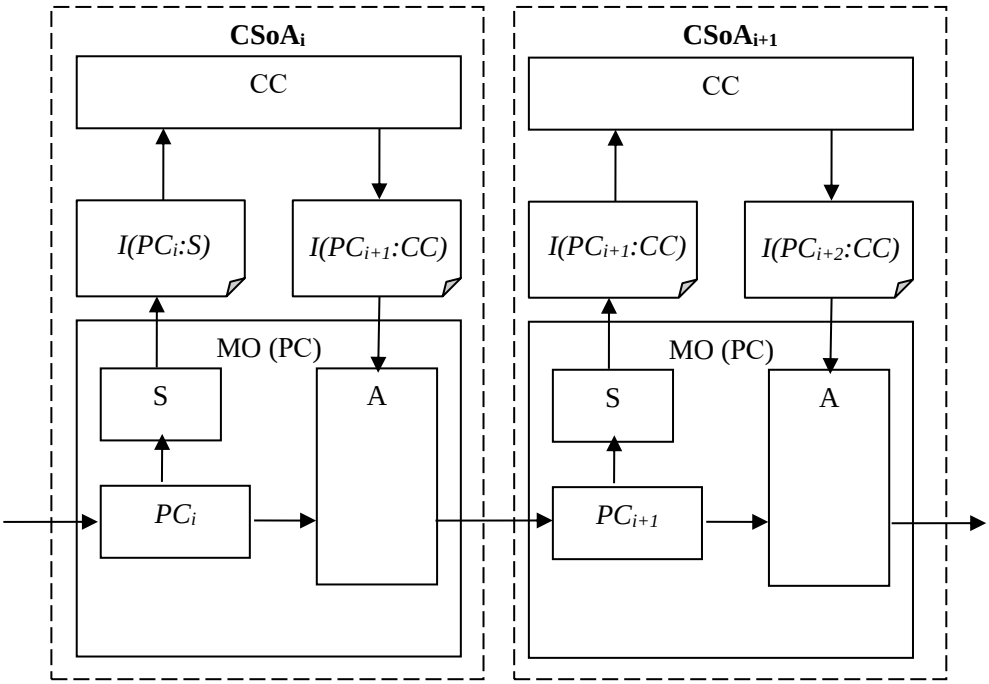


Рис. 1 – Графічна модель кібернетичної системи APT-атаки.

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

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

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

де $PC_{i+1}$, $I(PC_i{:}S)$, $I(PC_{i+1}{:}CC)$, $PC_i$ - це кінцеві бітові множини;

$F_{cc}[.]$ - це оператор відображення, який на основі прийнятої інформації і по заданому правилу прийняття рішення формує команду про перехід в інший стан;

$F_A[.]$ - 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:

$$\boldsymbol{APT}=\{CSoA_i\},\ i=1,\ldots,I. \qquad (2)$$

де:

- ***APT*** - це кінцева множина, що складається з кінцевих підмножин $CSoA_i$ (відповідних циклів управління кібернетичної системи атаки);

- $CSoA_i = \{PC_i, I(PC_i{:}S), I(PC_{i+1}{:}CC)\}$ - підмножина, що складається з кінцевих бітових наборів (множин). Ці набори двох суміжних циклів *CSoA*, що пов'язані між собою системою рівнянь (1);

- $i = 1,\ldots,I$ - 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 2.

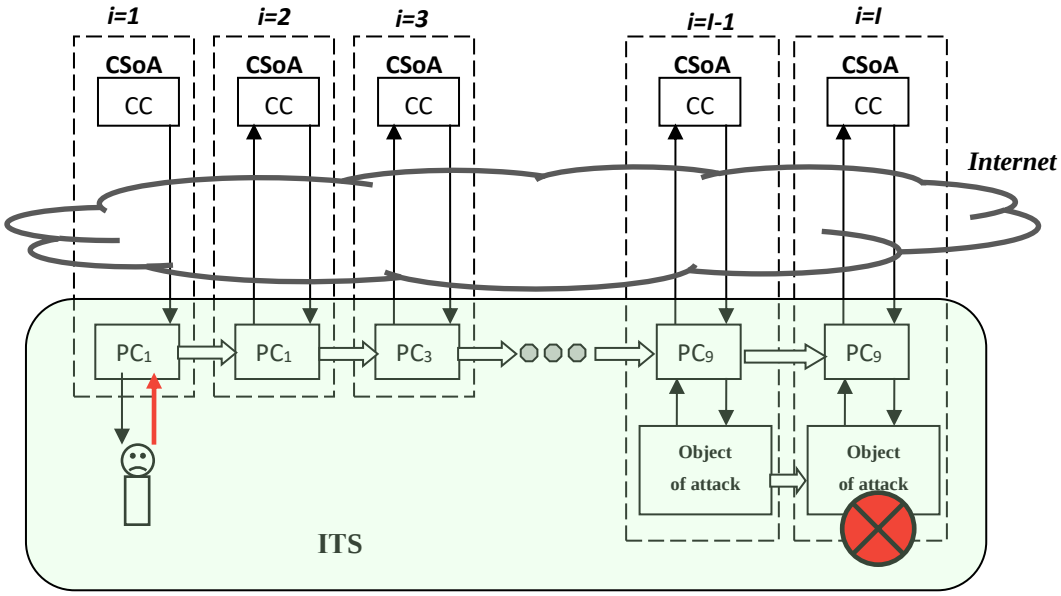


Рис. 2. Графічне представлення кібернетичної моделі APT атаки.Рис

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.

**3. Розробка моделі поведінки BD**

В загальному випадку BD складається із наступних частин, 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 (далі – Actuator BD, ABD).

За допомогою визначених складових можливо визначити структуру та модель поведінки BD (рис. 3).

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.

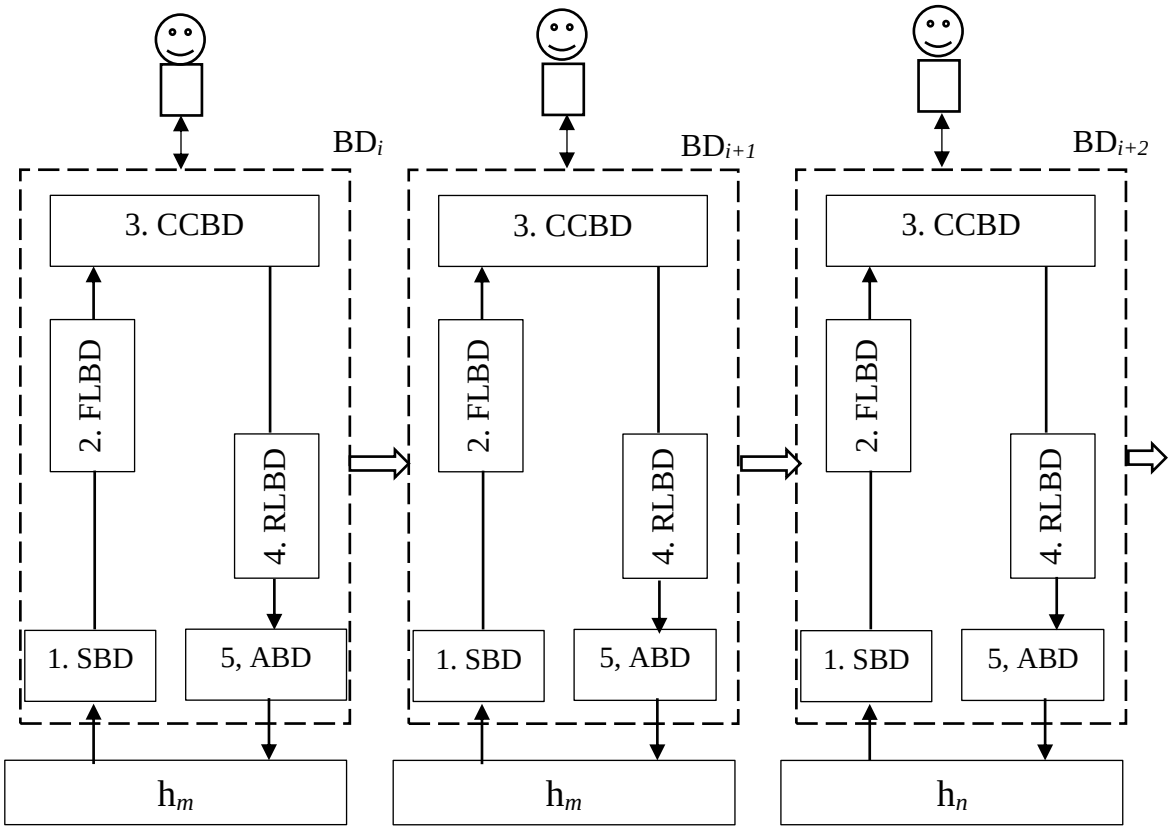


Рис. 3. Структура та модель поведінки BD в рамках APT-атаки.

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

Процедури (*procedure, Pr*) (1)-(5) 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 (далі – сигнатура, *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 (далі – процес, *process, Prs*);

2) послідовність даних, якими обмінюються обчислювальні процеси різних хостів за допомогою мережі (далі – трафік, *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, MAC-адреса, *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 (мал. 4) дозволяє кожної процедурі (1) -(5) поставити у відповідність наступні елементарні події (таблиця 1), що можуть бути детектуванні сенсорами безпеки ITS:

Таблиця 1.

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

| Компонента моделі BD | Процедура циклу, *Pr* | Елементарна подія ITS | Назва індикатору компрометації, IoC | Перемінне значення IoC |
|---|---|---|---|---|
| SBD | *Pr1* | 1) вихідний трафік хоста, $Trc_1$<br>2) процес хоста, $Prs_1$ | $Sign(Trc_1)$<br>$Sign(Prs_1)$ | $x_{1-1}$<br>$x_{1-2}$ |
| FLBD | *Pr2* | вихідний трафік ITS, $Trc_2$ | $Sign(Trc_2)$ | $x_2$ |
| CCBD | *Pr3* | вихідний трафік хоста зловмисника, $Trc_3$ | $Sign(Trc_3)$ | $x_3$ |

| | | | | |
|---|---|---|---|---|
| RLBD | *Pr4* | вхідний трафік ITS, $Trc_4$ | $Sign(Trc_4)$ | $x_4$ |
| ABD | *Pr5* | 1) вхідний трафік хоста, $Trc_5$<br>2) процес хоста, $Prs_5$ | $Sign(Trc_5)$<br>$Sign(Prs_5)$ | $x_5$ |
| h | *Pr6* | процес хоста, що активований BD, $Prs_6$ | $Sign(Prs_6)$ | $x_6$ |
| … | | … | … | … |

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 $Prs_6$. Ця процедура не є циклічною (в табл.1 - *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: $Sign(Prs_6)$; $Sign(Trc_5)$.

## 5. Розроблення способу формування шаблону для визначення BD APT-атаки

Запропоновані модель BD та підхід до відповідності процедур циклу BD елементарним подіям в ITS (табл.1) дозволяють розробити наступну структуру шаблону для детектування BD (табл. 2). Структура розроблялася для ITS, що має локальну корпоративну мережу з підключенням до ресурсів Інтернет через роутер периметру *R* та файєрвол нового покоління *NGFW*.

Таблиця 2

Структура шаблону для детектування BD

| | $BD_{i=1}$ | | $BD_{i=2}$ | | … | $BD_{i=I}$ | |
|---|---|---|---|---|---|---|---|
| | $IoC_{i=1}$ | Мітка про детектування (МД) | $IoC_{i=2}$ | МД | | $IoC_{i=I}$ | МД |
| *NGFW* | $Sign(Trc_{3,inp})$<br>$Sign(Trc_{3,out})$ | + | $Sign(Trc_{3,inp})$<br>$Sign(Trc_{3,out})$ | +<br>+ | | $Sign(Trc_{3,inp})$<br>$Sign(Trc_{3,out})$ | +<br>+ |
| $h_{m=1}$ | $Sign(Trc_1)$ | + | $Sign(Trc_1)$ | | … | $Sign(Trc_1)$ | |
| | $Sign(Prs_1)$ | + | $Sign(Prs_1)$ | | | $Sign(Prs_1)$ | |
| | $Sign(Trc_5)$ | + | $Sign(Trc_5)$ | | | $Sign(Trc_5)$ | |
| | $Sign(Prs_5)$ | + | $Sign(Prs_5)$ | | | $Sign(Prs_5)$ | |
| | | | $Sign(Prs_6)$ | | | $Sign(Prs_6)$ | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | … | | | | | | |
| $h_{m=2}$ | $Sign(Trc_1)$ | | $Sign(Trc_1)$ | + | | $Sign(Trc_1)$ | |
| | $Sign(Prs_1)$ | | $Sign(Prs_1)$ | + | | $Sign(Prs_1)$ | |
| | $Sign(Trc_5)$ | | $Sign(Trc_5)$ | + | | $Sign(Trc_5)$ | |
| | $Sign(Prs_5)$ | | $Sign(Prs_5)$ | + | | $Sign(Prs_5)$ | |
| | | | $Sign(Prs_6)$ | | | $Sign(Prs_6)$ | |
| | … | | | | | | |
| … | | | | | … | | |
| $h_{m=M}$ | $Sign(Trc_1)$ | | $Sign(Trc_1)$ | | | $Sign(Trc_1)$ | + |
| | $Sign(Prs_1)$ | | $Sign(Prs_1)$ | | | $Sign(Prs_1)$ | + |
| | $Sign(Trc_5)$ | | $Sign(Trc_5)$ | | | $Sign(Trc_5)$ | + |
| | $Sign(Prs_5)$ | | $Sign(Prs_5)$ | | | $Sign(Prs_5)$ | + |
| | | | | | | $Sign(Prs_5)$ | |
| | … | | | | | | |

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

1) *NGFW* фіксує вхідний трафік $Trc_{3,\ inp}$ та вихідний трафік $Trc_{3,\ out}$;
2) формується припущення, що це перший цикл управління $BD_{i=1}$;
3) формуються наступні значення IoC:

   $Sign(Trc_{3,\ inp})$= *(IP-адреса, IP-порт)*
4) на $h_m$ , що визначений за *IP-адресою* $Sign(Trc_{3,\ inp})$, визначається новий $Prs_1$, що пов'язаний з обміном даних через *IP-порт* $Sign(Trc_{3,\ inp})$;
5) сформовані $Sign(Trc_{3,\ inp})$; $Sign(Trc_{3,\ out})$; $Sign(Prs_1)$ використовуються для визначення наступних циклах управління (на цьому, або іншому хосту);
6) 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

Основою багатьох APTs є використання зловмисником несанкціонованих каналів дистанційного управління через Інтернет (backdoor, BD), що дозволяють йому виконувати різні дій в кіберпросторі системі інформаційних технологій жертви. Актуальним стає завдання своєчасного визначення BD ще на етапі підготовки цільової акції. Такій підхід відповідає реалізації проактивної стратегії кіберзахисту.

В рамках проведених досліджень:

1) на основі кібернетичнох моделі APT-атаки розроблено модель BD та його поведінки. Модель дозволяє зв'язати етапи APT-атаки та цикли управління BD з елементарними подіями в кіберсегменті корпоративної інформаційної системи (файли, трафіки, обчислювальні процеси);
2) на основі моделі BD розроблено багатоіндикаторну структуру шаблону для SIEM. Це дозволяє на основі моніторингу елементарних подій на пристроях інформаційної системи детектувати BD та відслідковувати траєкторію його поведінки за часом та обладнанням інформаційної системи;
3) структура шаблону дозволяє використовувати різни сценарії детектування BD. В роботі запропоновано один із сценаріїв, проведена відповідна перевірка працездатності на обладнані ситуаційного центру кібербезпеки;
4) розроблені модель BD та структури шаблону детектування дозволяють розширити можливості SIEM в напрямку удосконалення проактивного захисту від APT-атак.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Chen P. A study on Advanced Persistent Threats [Електронний ресурс] / P. Chen, L. Desmet, C. Huygens // iMinds-DistriNet, KU Leuven – 2014. – Режим доступу до ресурсу: http://zempirians.com/ebooks/2014-apt-study.pdf.
[2] Bejtlich R. What Is APT and What Does It Want? [Електронний ресурс] / Richard Bejtlich. – 2010. – Режим доступу до ресурсу: http://taosecurity.blogspot.be/2010/01/what-is-apt-and-what-does-it-want.html, 2010.
[3] The Advanced Persistent Threat. [Електронний ресурс] // Mandiant. – 2010. – Режим доступу до ресурсу: https://wikileaks.org/hbgary-emails//fileid/27714/8307.
[4] Advanced Persistent Threats: A Symantec Perspective [Електронний ресурс] // WHITE PAPER. – 2011. – Режим доступу до ресурсу: https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf.
[5] Time-Dependent Analysis of Attacks [Електронний ресурс] / F.Arnold, H. Hermanns, R. Pulungan, M. Stoelinga // Principles of Security and Trust. – 2014. – Режим доступу до ресурсу: https://link.springer.com/chapter/10.1007%2F978-3-642-54792-8_164.
[6] Camtepe, S., Yener, B.: Modeling and detection of complex attacks. In: SecureComm Third International Conference on Security and Privacy in Communications Networks and the Workshops, 2007. pp. 234–243 (Sept 2007)
[7] Flåten, O., Lund, M.S.: How good are attack trees for modelling advanced cyber threats? Norwegian Information Security Conference (NISK) 7(1), 2014.
[8] Ihor Yakoviv. “Cybernetic model of the Advanced Persistent Threat”, *Information technology and security*, vol. 6, iss.1(10), pp.46-58, 2018. Kyiv, Ukraine: Institute of special communications and information security NTUU “Igor Sikorsky KPI”. [Online]. Available: http:/ http://its.iszzi.kpi.ua/article/view/153140/152522/.
[9] David E. Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies”. *Schweitzer Engineering Laboratories, Inc,* 70th Annual Conference for Protective Relay Engineers. 2017. [Online]. Available: https://doi.org/10.1109/CPRE.2017.8090056.
[10] Ihor Yakoviv. “The base model of informational processes of management and safety criteria for cybernetic systems”, *Information technology and security*, vol. 3, iss.1(4), pp. 68-73, 2015. Kyiv, Ukraine: Institute of special communications and information security NTUU “Igor Sikorsky KPI”. [Online]. Available: http://its.iszzi.kpi.ua/article/view/57735/53977.
[11] Ihor Yakoviv. “Basic model of information processes and behavior of a cyber defense system”, *Information technology and security*, vol. 7, iss. 2 (12), pp. 183-196,

2019. Kyiv, Ukraine: Institute of special communications and information security NTUU “Igor Sikorsky KPI”. [Online]. Available: http://its.iszzi.kpi.ua/article/view/190568.
[12] Carson Zimmerman. Ten Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation, 2014. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf