MATHEMATICAL AND COMPUTER MODELING

DOI 10.20535/2411-1031.2019.7.2.190568
УДК 004.056.53:621.391

ІГОР ЯКОВІВ

БАЗОВА МОДЕЛЬ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ ТА ПОВЕДІНКИ СИСТЕМИ КІБЕРЗАХИСТУ

Зростання складності та інтенсивності кібератак призводить до актуальності завдання реалізації проактивної стратегії захисту систем інформаційних технологій. Впровадження проактивної стратегії захисту пов'язане з жорсткими часовими обмеженнями на прийняття рішення про оцінювання текучої ситуації та прийняття відповідних рішень ще до переривання кібератаки. Ці обмеження значно звужують сферу використання методів експертного оцінювання. Зростає необхідність широкого застосування засобів автоматизації, які дозволять значно знизити час визначення подій безпеки, формування та реалізації відповіді на вторгнення у кіберпростір ІТ-системи. Особливість таких засобів – значний рівень інтелектуалізації, що адекватний рівню компетентності операторів кібербезпеки. Базовою компонентою процедури розробки засобів автоматизації є формування процесної моделі об'єкту досліджень, на основі якої за допомогою відомих технологічних платформ формується код відповідного програмного забезпечення. Відомі засоби формалізованого опису бізнес-процесів дозволяють формувати моделі інформаційних процесів. При цьому широко застосовується термін "інформація", але не розкривається його сутність. Це, в свою чергу, приводить до ряду невизначеностей відносно властивостей цих процесів (будови, структури, функцій, організації). Відсутність конструктивного визначення терміну "інформація" значно ускладнюэ аналіз процесів кіберзахисту. У кіберпросторі події безпеки та інформація безпеки – це процедури оброблення, зберігання і передавання даних. У цих умовах складно однозначено відобразити існуючими засобами моделювання семантичний звязок між небезпечною подією в системах інформаційних технологій, інформаційними обєктами, що відображають цю подію і процесами кіберзахисту. Проблема "інформаційних невизначеностей" при моделюванні системи кіберзахисту значно звужує коло процесів, які можна алгоритмізувати з метою створення засобів їх автоматизування. Вирішення цієї проблеми є актуальним для сфери автоматизації процесів системи проактивного кіберзахисту. З метою збільшення результативності процесу розробки засобів автоматизації для сучасних систем кіберзахисту на основі атрибутивно-трансфертного підходу до сутності інформації та базової моделі інформаційних процесів управління кіберсистемою розроблено нову модель такої системи. В рамках цієї моделі ІТ-система є об'єктом управління, безпекою якого керує сукупність узгоджених інформаційних процесів кіберзахисту. Ця сукупність процесів пов'язана циклом управління. Послідовність циклів є траєкторію поведінки системи кіберзахисту. Розроблені засоби графічної та математичної формалізації можливо застосовувати в рамках ієрархічної декомпозиції інформаційних процесів, яка дозволяє з загальних позицій описувати їх з необхідною ступеню деталізації у вигляді двійкових наборів (файлів, трафіків, обчислювальних процесів). За допомогою моделей проведено декомпозицію одного із процесів розвідки кіберзагроз та розроблено відповідний засіб автоматизації.

Ключові слова: проактивний кіберзахист, проблеми автоматизації, сутність інформації, інформаційні процеси управління, цикли та поведінка системи кіберзахисту.

Постановка проблеми. Збільшення складності та інтенсивності кібератак робить актуальним завдання реалізації проактивної стреатегіі захисту систем інформаційних технологій (Information Technology System, IT-system, далі – ITS).

Така стратегія пов'язана з жорсткими часовими обмеженнями на прийняття рішення про оцінювання текучої ситуації та прийняття відповідних рішень ще до переривання кібератаки. Ці обмеження значно звужують сферу використання методів експертного оцінювання. Зростає необхідність широкого застосування засобів автоматизації, які дозволять значно знизити час визначення подій безпеки, формування та реалізації відповіді на вторгнення у кіберпростір ITS. Особливість таких засобів – значний рівень інтелектуалізації, що адекватний рівню компетентності операторів кібербезпеки.

Базовою компонентою процедури розробки засобів автоматизації є формування процесної моделі об'єкту досліджень, на основі якої за допомогою відомих технологічних платформ формується код відповідного програмного забезпечення. Відомі засоби формалізованого опису бізнес-процесів дозволяють формувати моделі інформаційних процесів. При цьому широко застосовується термін "інформація", але не розкривається його сутність. Це, в свою чергу, приводить до ряду невизначеностей відносно властивостей цих процесів (складу, структури, функціям, організації тощо).

Відсутність конструктивного визначення терміну "інформація" значно ускладнює аналіз процесів кіберзахисту. У кіберпросторі події безпеки та інформація безпеки – це процедури обробки, зберігання та передавання даних (бітових наборів). В цих умовах складно однозначно виразити існуючими засобами моделювання семантичний зв'язок між небезпечною подією в ITS, інформаційними об'єктами, що відображають цю подію, та процесами кіберзахисту. Проблема "інформаційних невизначеностей" при моделюванні системи кіберзахисту значно звужує коло процесів, які можливо алгоритмізувати з метою створення засобів їх автоматизації.

Вирішення цієї проблеми є **актуальним** для сфери автоматизації процесів системи проактивного кіберзахисту.

Аналіз останніх досліджень і публікацій. Актуальні публікації із різною ступеню формалізації описують проблеми функціонування систем проактивного кіберзахисту (далі – системи захисту). Для забезпечення ефективного захисту від складних кібератак, що динамічно змінюють методи та засоби несанкціонованого втручання, необхідно обробляти зетабайтові обсяги актуальних даних на протязі короткого інтервалу часу [1]. В цих умовах людський фактор стає найслабшою ланкою кіберзахисту. Подолання проблеми пропонується вирішити завдяки використанню засобів автоматизації, що розроблено на основі методів штучного інтелекту (розпізнавання образів, когнітивний інтелект, нейронні мережі, інтелектуальні агенти, штучна імунна система, машинне навчання, обмін даними, нечітка логіка, евристика тощо). В першу чергу, ці засоби автоматизації пропонується застосовувати в процесах раннього попередження, виявлення вторгнень та запобігання атакам. В той же час не розглядаються методи формалізації самих цих процесів, що дозволяють конкретизувати їх сутність для подальшої алгоритмізації.

В ряді публікаціях [2] - [4], [6], [7] конкретизується перелік процесів кіберзахисту та компонентів системи захисту, що їх реалізують. Так [2], [3] виділяють процес розвідки кіберзагроз (далі – загроз), який є першочерговим відносно наступних процесів захисту:

– моніторинг стану ITS (збір інформації про стан безпеки ITS, реалізується системою детектування вторгнень, Intrusion Detection System, IDS);

– збір, зберігання та аналіз інформації про текучі загрози (реалізується офіцерами безпеки та системою управління подіями і інформацією безпеки, Security Information and Event Management, SIEM);

– підготовка відповіді на інцидент кібербезпеки та її реалізація (впроваджується офіцерами безпеки за допомогою системи запобігання вторгненням, Intrusion Prevention System, IPS).

Сам процес розвідки загроз реалізується наступними процесами [2]:

– збір інформації із різних зовнішніх джерел про відомі актуальні загрози;

– збір інформації про вразливості ITS організації;

– аналіз зібраної інформації та її застосування в процесах виявлення кібератак.

В свою чергу, [6] виділяє таку обов'язкову компоненту сучасної системи ефективного захисту як центр операцій кіберзахисту (cybersecurity operations center, CSOC, або – просто SOC). За визначенням автора публікації "SOC – команда, що в основному складена із аналітиків з питань безпеки, яка організовується для виявлення інцидентів кібербезпеки, їх аналізу, підготовки звітів та відповідей щодо подальшого запобігання".

В публікаціях [2], [4], [5] крім вербального опису процесів кіберзахисту надаються графічні моделі, які конкретизують їх сутність. Моделі різних варіантів організації процесу розвідки загроз [2] пояснюють взаємозв'язок різних процесів в системі захисту двома видами потоків: потік розвідки (Intel flow) і потік сигналізації (Alarm flow). Графічна модель "The Defense Chain" (Оборонний ланцюг) [4] візуалізує роботу системи кіберзахисту лінійною послідовністю етапів: планування захисту; реалізація захисту; моніторинг захисту; виявлення атак; формування звіту; відповідь; удосконалення захисту. Графічна модель "The Pyramid of Pain" [5] у вигляді ієрархічних рівнів піраміди представляє сукупності ознак (індикаторів, показників) кібератаки, які може застосовувати захист для виявлення втручань. Складність ознак збільшується від ніжних рівнів (хеш образи, IP-адреси, доменні імена) до ознак тактик, методів та процедур (Tactics, Techniques, Procedures, TTPs), які використовує зловмисник.

Для організації ефективної протидії вдосконалим атакам запропонована концепція адаптивної системи захисту [7]. В основі архітектури цієї системи є цикл із наступних етапів:

"запобігання" – об'єднує процеси: збору та аналізу інформації із різних джерел про можливі загрози; визначення політик та засобів протидії цим загрозам; конфігурування системи захисту;

"виявлення" – визначення та протидія тим атакам, ознаки яких не було враховано при конфігуруванні процесів захисту на попередньому етапі;

"ретроспективне дослідження" – збір та аналіз інформації про інциденти безпеки, визначення та реалізація дій, що запобігають повторним подіям;

"прогнозування" – порівняльний аналіз (свого досвіду, досвіду інших організацій, інформації про можливі нові вразливості) з метою вдосконалення системи захисту.

Безперервна послідовна реалізація циклів, які складаються з зазначених етапів, дозволяє адаптувати систему захисту під постійне вдосконалення можливостей атакуючої сторони.

Розглянути в рамках досліджень моделі (вербальні та графічні) з різною ступеню деталізації формалізують архітектуру системи захисту та окремих її процесів. Це дозволяє підвищувати компетенції фахівців у сфері кіберзахисту та сприяє удосконаленню протидії атакам. Але, загальним недоліком цих моделей є те, що вони не орієнтовані на машинну реалізацію. Відсутність інформації (інформаційних об'єктів) у представленні процесів супроводжується рядом невизначеностей щодо:

– структури інформаційного процесу;
– сутності інформації (інформаційних об'єктів) у складі інформаційного процесу;
– властивостей цих об'єктів (просторових, часових, структурних та інших);
– взаємозв'язку між властивостями інформаційного об'єкту і об'єкту-прообразу;
– характеру взаємозв'язку інформацій між собою (порядку перетворення однієї інформації в іншу).

В умовах тенденції зниження впливу людського фактору **актуальним** стає завдання розробки таких моделей, що орієнтовані на впровадження в систему кіберзахисту інтелектуальних засобів автоматизації.

Метою роботи є розробка моделей системи кіберзахисту та її інформаційних процесів, що орієнтовані на розробку засобів автоматизації для цієї системи.

Основний матеріал досліджень. Основою автоматизації систем захисту є розробка алгоритмів, що однозначно описують сутність їх складових інформаційних процесів. Значно

спроститити цю розробку можливо шляхом зниження рівня багатьох невизначеностей за допомогою формалізації проблемної ситуації (вербальної, графічної та математичної), що дозволяє конкретизувати та деталізувати:

- перелік процесів та його повноту;
- сутність процесів (склад, структуру, функціонал, організацию тошо);
- взаємозвязок процесів.

1. Стратегії захисту, процеси захисту, компоненти системи захисту. Проведений аналіз сучасних практик захисту корпоративних ITS, що використовують ресурси Інтернет, дозволяє виділити дві стратегії протидії зовнішнім кібератакам: реактивний захист і проактивний (превентивний) захист. Для реактивної стратегії прийняття рішення про виявлення атаки завершується після її закінчення. Заходи протидії можуть запобігти тільки такий же наступній атаці. В рамках проактивного (превентивного) захисту виявлення атаки має відбутися ще до її завершення. В цьому випадку залишається час на визначення та реалізацію заходів переривання зовнішнього втручання. Загальною основою для цих стратегій має бути реалізація циклу протидії атаці, що складається із послідовності наступних інформаційних процесів [2], [3], [6]:

1) спостереження у реальному часі за допомогою сенсорів безпеки за подіями в корпоративному сегменті кіберпростору ;

2) формування за допомогою сенсорів безпеки інформації про події безпеки, її збір і нормування в єдиному центрі оперативної обробки;

3) аналіз подій і прийняття рішення про наявність кібератаки (інциденту кібербезпеки);

4) визначення вразливостей, що сприяли атаці, прийняття рішення про протидію та реалізація цього рішення за допомогою актуаторів безпеки (виконавчих пристроїв системи захисту, засобів захисту).

Ключовою частиною сучасних систем кіберзахисту корпоративних ITS є центри операцій кібербезпеки (SOC) [6]. Такі центри за допомогою операторів (офіцерів) безпеки та/або засобів управління інформацією і подіями безпеки (SIEM) з різним ступенем автоматизації реалізують перераховані вище процеси 1-4.

Формування інформації про текучі події безпеки в ITS здійснюється за допомогою використання індикаторів компрометації (indicators of compromise, IOCs). Це цифрові (бітові) послідовності (сигнатури), що є ознаками небезпечного трафіку або обчислювального процесу. Повідомлення про інциденти (події) безпеки формуються сенсорами безпеки (security sensors, SS або засоби IDS) на основі IOCs.

Формування актуальних IOCs [2] - [5] здійснюється в рамках розвідки кіберзагроз (Cyber Threat Intelligence, CTI), що реалізується циклом розвідки загроз через послідовність наступних процесів [2], [6]:

1) визначення індивідуальних характеристик ITS (мережева технологія, топологія мережі, тип операційних систем, перелік програмних застосувань, перелік апаратного забезпечення та інше);

2) визначення переліку можливих актуальних загроз (лист загроз) на основі збору інформації від зовнішніх відкритих або комерційних джерел (баз даних про вразливості та загрози);

3) визначення актуальних вразливостей ITS (лист вразливостей ITS) за результатами тестування на проникнення (peneration test, PT);

4) формування на основі листа вразливостей ITS набору актуальних для ITS індикаторів компрометації (IOCs).

Таким чином, інформаційні процеси сучасних системи захисту можливо поділити на дві групи: 1) процеси розвідки кіберзагроз; 2) процеси протидії атакам. В рамках кожної групи процеси послідовно взаємопов’язані в рамках відповідних циклів. Обов’язковою умовою ефективної роботи системи захисту є наявність актуального набору індикаторів

компрометації. Цей набір визначає траєкторію (вектор) поведінки системи в умовах комплексу можливих втручань. За підтримку актуального стану набору індикаторів компрометації відповідає черговий цикл розвідки загроз. Основою для запуску нового циклу можуть бути люби зовнішні або внутрішні події, що потребують зміни набору індикаторів компрометації (інформація про нові загрози із різних зовнішніх джерел, зміні в архітектурі корпоративної ITS, результати планового або позапланового тестування на проникнення, зміна політики безпеки, заміна комп'ютерного обладнання тощо).

Подальша графічна та математична формалізація, що дозволяє знизити рівень невизначеностей при описі системи захисту, була проведена за допомогою:

– атрибутивно-трансфертного підходу до сутності інформації [8], що дозволяє представити процеси захисту у вигляди інформаційних процесів (далі – інформаційний підхід);

– кібернетичного підходу, що дозволяє представити систему захисту у вигляді кібернетичної (керованої) системи [9].

2. Інформаційній підхід, інформація та інформаційний процес. В основі цього підходу є наступний набір тверджень:

– принципово важливо відрізняти реальні об'єкти з їх властивостями (склад, структура, колір, вага, можливі стани, розташування в навколишньому середовищі, їх поведінку і багато інших) від інформації про ці об'єкти та їх властивості;

– властивості об'єктів визначаються характером упорядкованості їх складових частин і проявляються через взаємодію з іншими об'єктами;

– інформація – це особливий результат фізичної взаємодії реальних об'єктів;

– інформація завжди пов'язана з матеріальним об'єктом, що є її носієм, і розташована в конкретній точці простору-часу.

Така система поглядів дозволяє дати наступні визначення, що пояснюють сутність інформації:

"інформація" – це властивості (атрибути), що перенесені (трансферт) з одного об'єкту на інший;

"носій інформації" – об'єкт, в якому відображені властивості іншого об'єкту.

В рамках математичної інтерпретації можливо більш конкретизувати визначення терміну "інформація":

"інформація" про об'єкт A в об'єкті B (далі – інформація $I(A:B)$) – це впорядкований набір (множина) елементів $P^{(B)}$ об'єкту B, що сформований в результаті взаємодії f_{map} з об'єктом A та є образом впорядкованого набору $P^{(A)}$ цього об'єкту, тобто:

$$I(A:B) = P^{(B)} \mid f_{map} : P^{(A)} I \rightarrow P^{(B)},$$

де $P^{(A)}$ – множина елементів об'єкту A , що описує його властивість;

f_{map} – оператор відображення (індекс $_{map}$ – від англійського слова *mapping*, відображення) описує характер фізичної взаємодії об'єктів;

$P^{(B)}$ – множина елементів об'єкту B, що описує сформовану в результаті взаємодії його нову властивість. Від характеру механізму інформаційної взаємодії залежить вид відношень між властивостями $P^{(A)}$ та $P^{(B)}$:

відношення подібності – впорядкованість елементів $P^{(A)}$ зберігається в $P^{(B)}$, але в інших пропорціях (приклад – людина та її світлина);

відношення тотожності – впорядкованість елементів $P^{(A)}$ замінюється в $P^{(B)}$ на іншу (приклад з молекулярної біології – впорядкований набір нуклеотидів ДНК визначає впорядкований набір амінокислот в синтезованому білку (процедури транскрипції та трансляції).

В рамках комп'ютерного середовища (кіберпростору) носіями інформації є різні електронні сигнали, пристрої запам'ятовування та обробки інформації. Сама інформація представляє собою впорядковані набори у форматі бітових (двійкових) даних. Такий підхід дозволяє представити інформаційній процес комп'ютерних систем у вигляді сукупності:

– початкового набору даних (початкова інформація або вхідна інформація процесу, $I_{вх}$);

– набору дій (функції) з цією інформацією (ця сукупність – технологія обробки інформації (TOI), або - інформаційна технологія, information technology ();

– кінцевий набір даних (інформаційний продукт або вихідна інформація процесу, $I_{вих}$), що формується за результатами виконання сукупності дій над $I_{вх}$.

Інформаційний процес (*information process, IPr*) можливо представити трійкою множин:

$$IPr = (I_{вх}; IT; I_{вих}),$$

де $I_{вх}, I_{вих}$ – бітові множини, що пов'язані між собою інформаційною технологією:

$$I_{вих} = IT(I_{вих});$$

$IT:= (I; F)$ – орієнтований граф, для якого $I=\{i_1, i_2, \dots i_n\}$ – набір з n інформацій, що формуються в рамках процесу; $F=\{f_1, f_2, \dots f_m\}$ – набір з m функцій, що визначають сутність технології обробки інформації. Кожна функція в рамках інформаційного процесу у випадку можливості її алгоритмізації також може бути представлена у вигляді бітового набору.

Розроблений спосіб формалізації дозволяє:

– визначати межи інформаційних процесів ($I_{вх}, I_{вих}$);

– деталізувати до потрібного рівня кожний процес через набір інформацій $I=\{i_1, i_2, \dots i_n\}$ та набір дій з цією інформацією $F=\{f_1, f_2, \dots f_m\}$;

– взаємопов'язувати інформаційні процеси між собою (вихідна інформація одного процесу є вхідною інформацією для іншого).

3. Кібернетичний підхід і моделі системи захисту. В рамках цього підходу приставка "кібер-" застосовується не в контексті цифрових процесів в рамках середовищ комп'ютерних систем (кіберпростір, кіберподія, кіберзахист, кібератака та інше), а для опису особливостей процесів кібернетичних (управляємих, керованих) систем.

В проведеної декомпозиції процесів системи захисту в рамках підсистеми протидії атака можливо виділити послідовність дій, яка регулярно повторюється появою кожної атаки:

– отримання SOC за допомогою сенсорів безпеки інформації про події в ITS;

– аналіз подій в SOC і прийняття рішення про наявність кібератаки;

– прийняття рішення про протидію атаці і реалізація цього рішення за допомогою актуаторів безпеки.

Такий регулярний порядок дій дозволяє відповідно до базової моделі інформаційних процесів управління кібернетичної системи [9] представити процеси протидії атака у вигляді траєкторії поведінки керованої (кібернетичної) системи. У такій системі, назвемо її кібернетичної системою оперативного захисту (Cybernetic Operational Protection System, COPS), можна виділити наступні компоненти:

– об'єкт управління (Management Object, MO) – це ITS, яку необхідно захистити;

– підсистема управління захистом (Protection SubSystem, PSS), яка складається з: центру операцій безпеки (SOC); сенсорів безпеки (security sensor, SS) і актуаторів безпеки (security actuator, SA) – це процеси комп'ютерів, які відповідають за формування інформації про події безпеки і реалізацію інформації про керуючий вплив на ITS;

– каналів прямого зв'язку від SS до SOC (Forward Link, FL) і зворотного зв'язку від SOC до актуаторів SA (Return Link, RL) – це комп'ютерна мережа, що забезпечує обмін інформацією між центром управління SOC і об'єктом управління ITS.

При розробці моделі COPS використовується ряд тверджень, які дозволяють спростити графічний та математичний опис ситуації:

– будь-які характеристики та стан системи інформаційних технологій (комп'ютерних пристроїв) можна представити у вигляді кінцевої множини двійкових одиниць (бітів);

– інформація про будь-який стан будь-якого комп'ютерного пристрою, яка передається через мережу ITS, може бути представлена також множиною бітів, як і сам стан;

– роль сенсорів безпеки в ITS виконують обчислювальні процеси, які передають інформацію про стан комп'ютерів ITS через мережу за вказаною адресою;

– роль актуатора безпеки в ITS виконують обчислювальні процеси, який на основі прийнятих команд від SOC запускають нові процеси, що виконують необхідні дії захисту.

Дані твердження дозволяють спростити початкову модель [5] і представити графічно дві суміжні фази COPS у вигляді наступної структури (див. рис. 2).

У рамках цієї моделі корпоративна ITS виступає в ролі об'єкта управління (*MO*). Центр операцій кіберзахисту (SOC) – в ролі центру управління (Control Center, CC) кібернетичної системи. $I(ITS_i:S)$ – це інформація на сенсорах безпеки про текучий стан ITS_i в рамках актуальної (поточної) фази $COPS_i$. Дана інформація сформована і направлена до SOC сенсорами SS. На основі прийнятої інформації SOC приймає рішення про переведення системи інформаційних технологій в наступний стан ITS_{i+1} і оформлює це рішення в вигляді команди $I(ITS_{i+1}:SOC)$. Далі ця інформація надсилається до ITS, де прийняте рішення реалізується за допомогою актуаторів безпеки SA: об'єкт управління переходить в наступний стан протидії атаці ITS_{i+1}.

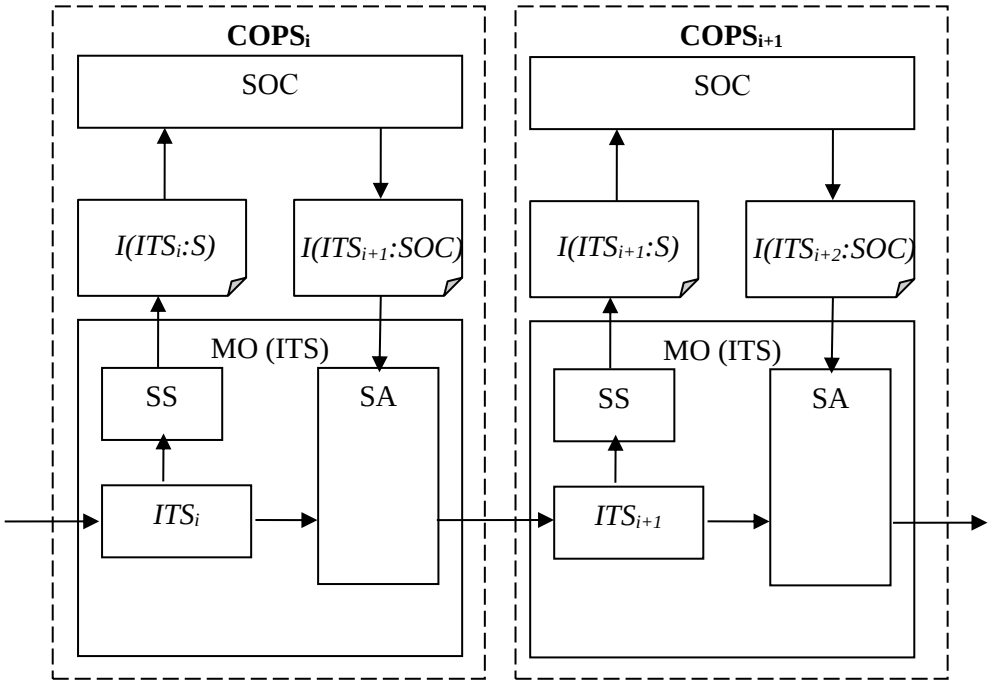


Рисунок1 – Модель поведінки кібернетичної системи захисту ITS в режимі протидії атаці

Процес управління в рамках COPS і поведінку самої COPS (перехід з однієї фази в іншу) може бути описаний наступною системою рівнянь:

$$\begin{cases} I(ITS_{i+1}:SOC) = F_{SOC}[I(ITS_i:SS)]; \\ ITS_{i+1} = F_A[ITS_i,\ I(ITS_{i+1}:SOC)], \end{cases} \quad (1)$$

де $I(ITS_{i+1}:SOC) = F_{SOC}[I(ITS_i:SS)]$ – це взаємозв'язок між командою на протидію з інформацією від сенсору безпеки (всі інформаційні об'єкти - кінцеві бітові множини);

$F_{SOC}[\cdot]$ – 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.

Отримані результати графічної і математичної формалізації дозволяють математично представити процес протидії кібератакам (Protection Process, траєкторія поведінки COPS) у вигляді множини:

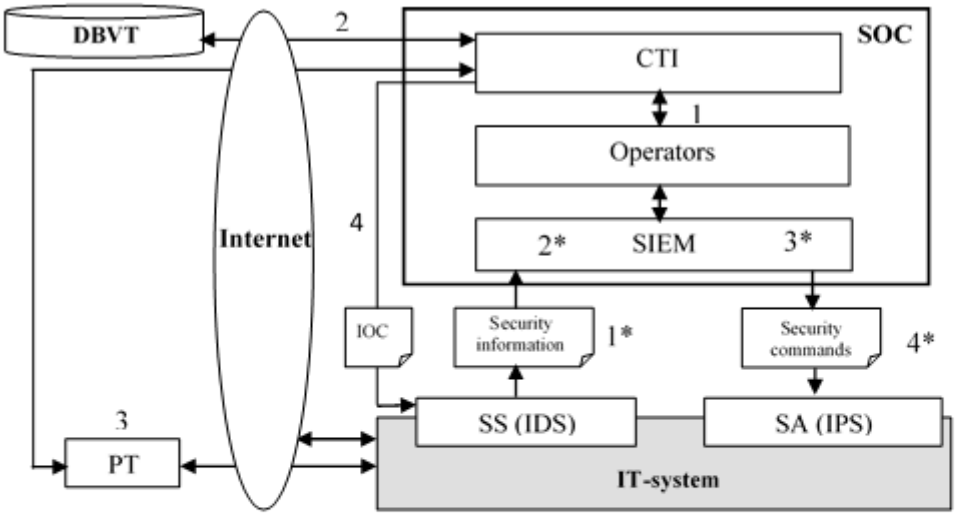
$$PP=\{COPS_i\},\ i=1,\ \ldots,\ I. \qquad (2)$$

де PP – це кінцева множина, що складається з кінцевих підмножин $COPS_i$ (відповідних фаз кібернетичної системи оперативного захисту);

$I(ITS_{i+1}:SOC) = [ITS_i, I(ITS_i:SS), I(ITS_{i+1}:SOC)]$ – підмножина ($COPS_i PP$), що складається з кінцевих бітових наборів (множин). Дві суміжні фази COPS пов'язані між собою системою рівнянь (1); i – номер поточної фази *ITS*, I - кількість фаз управління захистом, $i=1,\ \ldots,\ I$.

За допомогою такої математичної формалізації вдалося представити процеси протидії атакам в системі захисту у вигляді послідовності фаз кібернетичної системи. Кожна фаза – це послідовність регулярно повторюваних дій, які можна назвати *процедурами захисту*. Часові межі кожної фази визначаються моментами детектування подій безпеки. Під новим станом слід розуміти зміни в ITS, що впроваджуються актуаторами безпеки (засобами IDS) на основі команд від SOC (відповідей на події безпеки).

В рамках розробленої моделі (див. рис. 2) представлений формалізований опис взаємодії процесів розвідки кіберзагроз та процесів протидії кібератакам. Процеси розвідки кіберзагроз є первісними для виконання процесів протидії атакам (інформація про IOCs потрібна для сенсорів безпеки (засобів IDS).



Процеси розвідки кіберзагроз (CTI):
1 - визначення характеристик ITS;
2 - визначення всіх актуальних загроз;
3 - визначення актуальних вразливостей ITS (PT)
4 - формування набору індикаторів компрометації для сенсорів ITS

Процеси протидії кібератакам (CD):
1* - спостереження за подіями безпеки ITS;
2* – збір і нормування інформації з сенсорів безпеки про стан безпеки;
3* – аналіз подій і прийняття рішень про наявність атаки;
4* - рішення про протидію атаці і його реалізація

DBVT – бази даних вразливостей і загроз

Рисунок 2 – Модель інформаційних процесів системи кіберзахисту

4. Приклад застосування запропонованих підходів моделювання для розробки засобу автоматизації. Для перевірки конструктивності розроблених засобів формалізації інформаційних процесів системи кіберзахисту та моделей цієї системи було проведено більш детальний аналіз процесу формування індикаторів компрометації на основі результатів тестування на проникнення (відноситься до групи процесів розвідки кіберзагроз).

Тестування на проникнення є складовою частиною CTI, одним з основних завдань якої є визначення індикаторів компрометації (Indicators of Compromise, IOC) для сенсорів системи кіберзахисту корпоративної ITS. Це тестування є санкціонованою імітацією кібератаки на IT-систему, що виконується для оцінювання реального стану безпеки. Зазвичай тестування починається із ідентифікації цільової системи і визначення конкретної мети. Потім здійснюється збір з різних джерел інформації про ITS, її аналіз і приймається рішення про засоби і заходи досягнення мети тестування. Тестування може проводитися за концепцією "white box" (замовник надає всю інформацію про яка надає інформацію про ITS), або за концепцією "black box" (оператор тестування самостійно отримує необхідну інформацію). Існує також концепція "gray box" – комбінація двох перших концепцій [6]. Про проблеми безпеки, які виявляє тестування на проникнення, аудитор повідомляє власнику системи. Звіти про тести на проникнення можуть також оцінювати потенційні впливи на організацію та пропонувати заходи протидії, щоб зменшити ризики.

Тестування на проникнення може застосовуватися як основний засіб незалежного аудиту рівня кібербезпеки. У цьому разі він, як правило, застосовує концепцію "black box". Ми розглядаємо тестування у рамках забезпечення процесів оперативного кіберзахисту. Для цього застосовуються концепція "white box" або "gray box".

З метою визначення процесу, що необхідно автоматизувати, було проведено подальший аналіз застосування тестування на проникнення в рамках CTI. Для цього спочатку було визначено переліки процедур (функцій) і інформацій, що застосовуються у рамках формування набору індикаторів компрометації (див. табл. 1).

Результати аналізу інформаційного процесу формування переліку індикаторів компрометації.

Таблиця 1 – Формування набору індикторів компроментації

№	Назва процедури (функції)	Назва інформації, що застосовується
1	Визначення характеристик ITS (F1)	Перелік характеристик (ListA)
2	Формування тексту запиту до бази даних вразливостей і отримання доступу до актуальних вразливостей (F2)	Веб-запит (WRV), перелік актуальних вразливостей (ListV)
3	Отримання переліку потенційних вразливостей ITS (F3)	Перелік характеристик (ListA), перелік актуальних вразливостей (ListV), перелік потенційних вразливостей ITS (ListV*)
5	Отримання доступу до переліку актуальних експлойтів на відповідної базі даних (F4)	Веб-запит (WRE), перелік відомих експлойтів (ListE)
6	Пошук експлойтів, що відповідають переліку актуальних вразливостей ITS (F5)	ListV*, ListE, перелік експлойтів для тестування ITS (ListE*)
7	Застосування експлойтів до ITS в рамках тестування на проникнення та отримання відповідей на їх дії (F6)	ListE*, набір експлойтів для PT, набір актуальних загроз для ITS (ListT*)
8	Формування переліку (F7) актуальних для ITS індикаторів компрометації	перелік існуючих загроз для ITS (ListT*), перелік відомих індикаторів компрометації (ListIOC), перелік актуальних для ITS індикаторів компрометації (ListIOC*)

Відомості табл. 1 дозволяють провести подальшу графічну формалізацію інформаційного процес формування індикаторів компрометації (ListIOC) на основі характеристик ITS (ListA) і представити його у вигляді інформаційно-функціональної структури (Мал.3). Всі означені функції (F1-F7) виконує оператор безпеки. Структура дозволяє виділити функції, що у подальшому будуть автоматизовані. Було визначено функції F2-F5 (межі процесу автоматизації означені пунктиром на мал.3).

Для уточнення змісту дій, що буде виконувати програма автоматизації, додатково за допомогою базових засобів теорії множин була проведена математична формалізація. Завдяки цьому ситуацію визначення експлойтів для на проникнення конкретної ITS можливо представити наступним чином:

$ListE_S=\{e_i\}$ – множина актуальних експлойтів для тестування системи S;

e– окремий експлойт (елемент множини); $i=1,I$ – номер експлойту;

I – кількість експлойтів (потужність множини);

множина актуальних експлойтів $ListE_S$ формується розвідкою кіберзагроз (CTI):

$$ListE_S = F_{CTI}(ListV, ListE, ListA_S), \quad (4)$$

де $ListV =\{v_j\}$ – множина актуальних вразливостей ($ListV$), v_j – окрема вразливість, $j=1,J$ – номер вразливості;

$ListE =\{e_k\}$ – множина актуальних відомих експлойтів ($ListE$);

множина $ListE_S$ є підмножиною $ListE$;

$ListA_S=\{a_k\}$ – множина характеристик ІТ-системи, a_k – окрема характеристика, $k=1,K$ – номер характеристики;

$F_{CTI}(.)$ – оператор визначення експлойтів, що реалізується процесами розвідки кіберзагроз.

Всі зазначені множини – це кінцеві множини, потужність яких змінюється з:

- зміною апаратного і програмного забезпечення ITS;
- розширенням знань про вразливості інформаційних технологій;
- розвитком заходів і засобів застосування вразиливостей.

Результати проведеного аналізу на основі графічної і математичної формалізації процесів кіберзахисту (моделі: рис. 1, 2, 3; табл. 1; формули (1) – (4)) дозволяють визначить сутність автоматизації обраного процесу:

1) автоматизується процес визначення переліку актуальних експлойтів для проведення тестування заданої ІТ- системи;

2) програмний засіб автоматизації активізується або оператором безпеки, або автоматично за визначеним часом;

3) в коді програми автоматизації зазначені:

характеристики ІТ- системи;

адреси баз даних вразливостей, експлойтів і загроз;

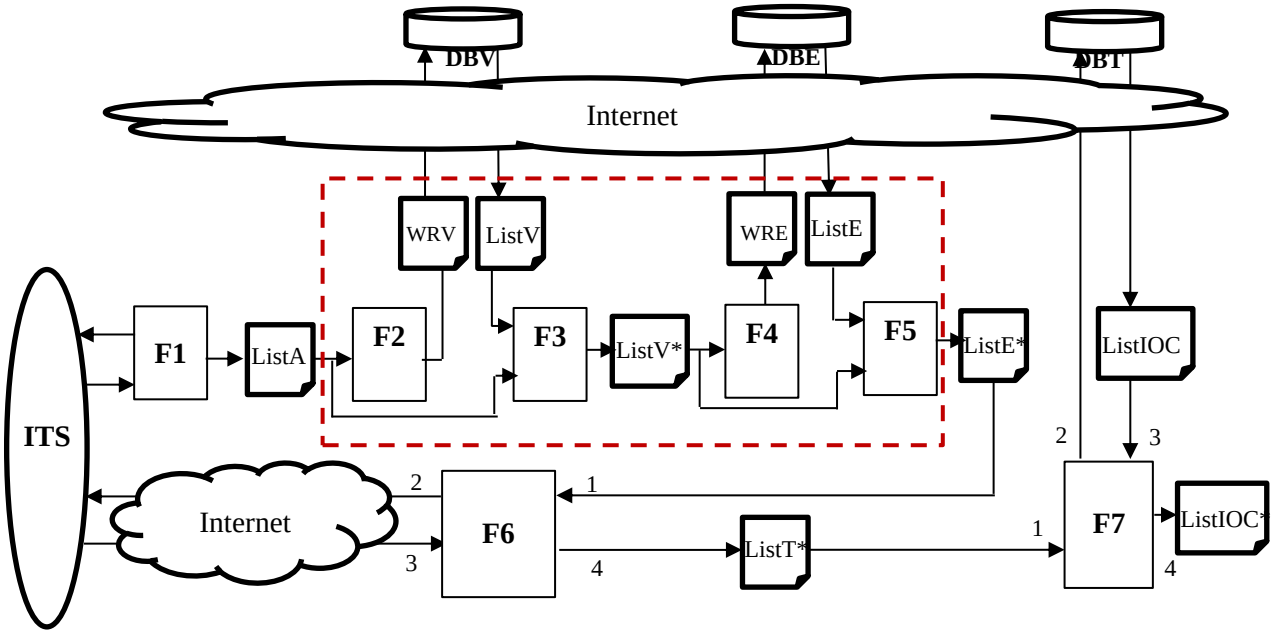
4) в ході виконання програми послідовно здійснюється звернення до баз даних вразливостей, експлойтів і загроз;

5) на основі отриманих відомостей про всі актуальні вразливості, експлойти і загрози автоматично формується перелік тих експлойтів, що дозволяють виявити за допомогою тестування на проникнення існуючі загрози ІТ- системи;

6) перелік експлойтів і їх характеристик надається візуально оператору безпеки.

За результатами проведених досліджень для реалізації обраного способу автоматизації на основі мови програмування Python було розроблено програму, що працює за веб-технологією та виконує наступні задачі:

- встановлення з'єднання із Національною базою даних вразливостей (NVD);
- пошук та завантаження CVE List із актуальними кібервразливостями;
- аналіз завантаженої інформації та здійснення вибірки CVE-IDs;
- відбір ста найновіших вразливостей;
- підбір існуючих експлойтів для актуальних кібервразливостей;
- збір та представлення інформації про експлойти актуальних кібервразливостей.



DBV – база даних вразливостей
DBE - база даних експлойтів
DBE - база даних загроз
WRV – веб-запит до DBV
WRE – веб-запит до DBE
WRT – веб-запит до DBT

ListA – перелік характеристик ITS
ListV – перелік відомих вразливостей
ListV* – перелік потенційних вразливостей ITS
ListE – перелік відомих експлойтів
ListE* – перелік експлойтів для тестування ITS
ListT* - перелік існуючих загроз для ITS (за результатами тестування)
ListIOC – перелік відомих індикаторів компрометації
ListIOC* – перелік актуальних для ITS індикаторів компрометації

Рисунок 3 – Модель (інформаційно-функціональна структура) процесу формування переліку актуальних індикаторів компрометації для ITS на основі процедури тестування на проникнення

Такий функціонал програмного продукту дає змогу оператору тестування на проникнення своєчасно отримувати інформацію про актуальні кіберзагрози у вигляді переліку експлойтів, які у подальшому буде застосовано для проведення тестування на проникнення. У такий спосіб оператор зможе перевіряти цільову інформаційну систему або веб-ресурс на предмет наявності у них найновіших вразливостей, які можуть бути використані зловмисником для проведення кібератаки на систему або проникнення у неї.

Програмний продукт складається із трьох модулів: imp.py, par.py та утиліти SearchSploit. Модуль imp.py забезпечує з'єднання із веб-сторінкою Національної бази даних вразливостей (NVD) і подальший пошук та завантаження CVE List до директорії за шляхом /home/user/nvd/. Модуль par.py здійснює аналіз CVE List та запис його вмісту до текстового файлу, після цього здійснює вибірку CVE-IDs та запис із неї ста останніх до окремого файлу. Потім здійснює запис CVE-IDs до масиву, а також запис вмісту файлу CwE_2018.txt до асоціативного масиву. Далі порівнюються елементи першого масиву з ключами другого. Однакові записуються до файлу. Після цього визначаються ідентифікатори експлойтів та за допомогою утиліти SearchSploit забезпечується їх візуалізація.

Перевірку працездатності програмного продукту було проведено у середовищі віртуальних машин на хості під управлінням OS Parrot Security (цільова ITS). За результатами перевірки час формування переліку актуальних для ITS експлойтів за допомогою запропонованого продукту зменшується:

з 20 до 32 хвилин (оператор: 30 операцій збору інформації у різний час дня);

до 5 до 8 хвилин (засіб автоматизації: 30 запусків програми у різний час дня).

Висновки. 1. Стратегія проактивного кіберзахисту потребує зменшення рівня людського фактору за рахунок впровадження засобів автоматизації, що знижують час визначення подій безпеки, формування та реалізації відповіді на вторгнення у кіберпростір.

2. Отримано нові графічні та математичні моделі інформаційних процесів системи кіберзахисту та їх зв'язку між собою. В основі розробки застосовано атрибутивно-трансферний підхід до сутності інформації та базова модель інформаційних процесів кібернетичної системи. Моделі орієнтовані на розробку засобів автоматизації для системи проактивного кіберзахисту.

3. Визначено дві групи інформаційних процесів захисту: процеси розвідки кіберзагроз, процеси протидії кібератакам. Обов'язковою умовою ефективної протидії кібератакам є застосування сенсорами безпеки набору актуальних індикаторів компрометації, які формуються циклом процесів розвідки кіберзагроз.

4. Процеси протидії кібератакам пов'язані в циклі управління безпекою системи інформаційних технології. Отримано графічну та математичну моделі траєкторії поведінки системи проактивного кіберзахисту.

5. Розроблені засоби графічної та математичної формалізації можливо застосовувати в рамках ієрархічної декомпозиції інформаційних процесів, яка дозволяє з загальних позицій описувати їх з необхідною ступеню деталізації у вигляді двійкових наборів (файлів, трафіків, обчислювальних процесів).

6. З метою перевірки розроблених засобів проведено детальний аналіз процесу формування індикаторів компрометації на основі результатів тестування на проникнення (один з процесів розвідки кіберзагроз). За результатами розроблено засіб автоматизації, що скорочує час пошуку даних про актуальні експлойти для тестування на проникнення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] E. Şeker, "Use of Artificial Intelligence Techniques", *Applications in Cyber Defense. NATO CCD COE Tallinn, Estonia*. [Online]. Available: https://www.researchgate.net/publication/333674372_Use_of_Artificial_Intelligence_Techniques_Applications_in_Cyber_Defense. Accessed on: July 17, 2019.

[2] P. Poputa-Clean. "Automated Defense". *Using Threat Intelligence to Augment Security*. [Online]. Available: https://www.sans.org/reading-room/whitepapers/threats/automated-defense-threat-intelligence-augment-35692. Accessed on: July 17, 2019.

[3] "Being Smart About Cyber Threat Intelligence". [Online]. Available: http://www.fusionppt.com/blog-post/smart-cyber-threat-intelligence/. Accessed on: July 17, 2019.

[4] D. Bianco, "The Defense Chain". [Online]. Available: http://detect-respond.blogspot.com/2014/10/the-defense-chain.html. Accessed on: July 17, 2019.

[5] D. Bianco, "The Pyramid of Pain". [Online]. Available: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html. Accessed on: July 17, 2019.

[6] C. Zimmerman, "Ten Strategies of a World-Class Cybersecurity Operations Center". [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf. Accessed on: July 17, 2019.

[7] N. MacDonald, and P. Firstbrook, "Designing an Adaptive Security Architecture for Protection From Advanced Attacks". [Online]. Available: https://www.gartner.com/en/documents/2665515/designing-an-adaptive-security-architecture-for-protecti. Accessed on: July 17, 2019.

[8] И.Б. Яковив, "Канал связи с позиций атрибутивно-трансфертной сущности информации", *Information Technology and Security*, vol. 1, iss. 2 (2), pp. 84-96, 2012.

[9] И.Б. Яковив, "Базовая модель информационных процессов управления и критерии безопасности кибернетической системы", *Information Technology and Security*, vol. 3, iss. 1 (3), pp. 68-74, 2015.

Стаття надійшла до редакції 03.09.2019.

REFERENCE

[1] E. Şeker, "Use of Artificial Intelligence Techniques", *Applications in Cyber Defense. NATO CCD COE Tallinn, Estonia*. [Online]. Available: https://www.researchgate.net/publication/333674372_Use_of_Artificial_Intelligence_Techniques_Applications_in_Cyber_Defense. Accessed on: July 17, 2019.

[2] P. Poputa-Clean. "Automated Defense". *Using Threat Intelligence to Augment Security*. [Online]. Available: https://www.sans.org/reading-room/whitepapers/threats/automated-defense-threat-intelligence-augment-35692. Accessed on: July 17, 2019.

[3] "Being Smart About Cyber Threat Intelligence". [Online]. Available: http://www.fusionppt.com/blog-post/smart-cyber-threat-intelligence/. Accessed on: July 17, 2019.

[4] D. Bianco, "The Defense Chain". [Online]. Available: http://detect-respond.blogspot.com/2014/10/the-defense-chain.html. Accessed on: July 17, 2019.

[5] D. Bianco, "The Pyramid of Pain". [Online]. Available: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html. Accessed on: July 17, 2019.

[6] C. Zimmerman, "Ten Strategies of a World-Class Cybersecurity Operations Center". [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf. Accessed on: July 17, 2019.

[7] N. MacDonald, and P. Firstbrook, "Designing an Adaptive Security Architecture for Protection From Advanced Attacks". [Online]. Available: https://www.gartner.com/en/documents/2665515/designing-an-adaptive-security-architecture-for-protecti. Accessed on: July 17, 2019.

[8] I. Yakoviv, "Communication channel from positions of the attributive-transfer entity of information", *Information Technology and Security*, vol. 1, iss. 2 (2), pp. 84-96, 2012.

[9] I. Yakoviv, "The base model of informational processes of management and safety criteria for cybernetic systems", *Information Technology and Security*, vol. 3, iss. 1 (3), pp. 68-74, 2015.

IHOR YAKOVIV

BASIC MODEL OF INFORMATION PROCESSES AND BEHAVIOR OF A CYBER DEFENSE SYSTEM

Increasing the complexity and intensity of cyberattacks makes the actual task of implementing a proactive strategy for protecting information technology systems. Such a strategy is associated with tight time limits on making decisions on assessing the current situation and making appropriate decisions even before the interruption of a cyber attack. These limitations significantly narrow the scope of the use of expert assessment methods. There is a growing need for the widespread use of automation tools that will significantly reduce the time for determining security events, and for formulating and implementing a decision on countering the invasion of information technology systems cyberspace. A feature of such tools is a significant level of intellectualization, which is adequate to the level of competence of cybersecurity operators. The basic component of the procedure for developing automation tools is the formation of a process model of the object of research. Based on this modem, using the well-known technological platforms, the corresponding software code is generated. Known means of a formalized description of business processes make it possible to form models of information processes. The term "information" is widely used, but its essence is not disclosed. This, in turn, leads to a number of uncertainties regarding the properties of these processes (composition, structure, functions, organization, etc.). The lack of a constructive definition of the term "information" greatly complicates the analysis of cyber defense processes. In cyberspace, security events and security information are procedures for processing, storing and transmitting data (bit sets). Under these conditions, it is difficult to unambiguously express the semantic connection between the dangerous event in ITS, the information objects reflecting this event, and cyber defense processes using existing modeling tools. The problem of "information

uncertainties” in modeling a cyber defense system significantly narrows the range of processes that can be algorithmized with the aim of creating means for their automation. The solution to this problem is relevant for the sphere of automation of proactive cyber defense system processes In order to increase the efficiency of the process of developing automation tools for modern cyber defense systems, a new model of such a system has been developed based on an attribute-transfer approach to the essence of information and a basic model of information processes for managing a cyber system. Within the framework of this model, the IT system is a management object, the security of which is controlled by a set of coordinated cyber protection information processes. This set of processes is connected by a control cycle. The sequence of cycles is the trajectory of the cyber defense system. Corresponding graphic and mathematical models of behavior are developed. Using them, a decomposition of one of the cyber threat intelligence processes was carried out and an appropriate automation tool was developed.

Keywords: proactive cyber defense, automation problems, the nature of information, information management processes, cycles and behavior of a cyber defense system.

Яковів Ігор Богданович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і застосування автоматизованих інформаційних систем та технологій, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна.

ORCID: 0000-0001-7432-898X.

E-mail: iyakov52@gmail.com.

Yakoviv Ihor, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.