NETWORK AND APPLICATION SECURITY

DOI: 10.20535/2411-1031.2018.6.1.153140
УДК 004.056.53::621.391

ІГОР ЯКОВІВ

КІБЕРНЕТИЧНА МОДЕЛЬ APT АТАКИ

Широкомасштабне застосування складних кібератак типу APT відносно критичної інфраструктури стало потужним стимулом для розвитку методів проактивного кіберзахисту. Характерним для APTs є складний набір взаємозв'язаних за часом і простором дій зловмисника. Окремо ці дії можуть не викликати підозр; цільова акція атаки в кіберсегменті об'єкта-жертви готується тривалий час (від декількох місяців до року і більше); сукупність дій зловмисника – це ланцюжок тактик, виконання яких дозволяє досягти мети атаки. Засоби реалізації тактики – різноманітні. Набір тактик і їх сутність залишаються постійними. Більшість відомих моделей APT атак представлені у вигляді вербального опису етапів APT і їх смислового змісту. Недолік таких моделей – неможливість прямого застосування в SIEM через відсутність загальної основи для алгоритмізації дій в рамках етапів атаки. В основі іншої групи моделей різні математичні конструкції, що дозволяють представити масштабні дії зловмисника у вигляді одного складного математичного процесу. Як правило, такі моделі складно зв'язуються з технологічними процесами моніторингу подій в реальному часі. З позицій автоматизації процесів виявлення складних кібератак в першу чергу стоїть завдання розробки моделей APT, які дозволяють алгоритмізувати процес формування індикаторів безпеки на основі аргументованої кореляції подій за часом і простором. Стаття присвячена розробці нової моделі APT на основі кібернетичного підходу. Сутність підходу – відносно комп'ютерів організації-жертви зловмисник регулярно виконує дії із циклу управління. Це дозволяє представити APT атаку у вигляді траєкторії поведінки керованої (кібернетичної) системи. В рамках моделі поведінка кібернетичної системи зловмисника представлена через математичний опис інформаційних процесів управління та ітеративний взаємозв'язок між суміжними фазами (станами) кібернетичної системи. Такий підхід дозволяє в рамках ієрархічної структури моделі: поставити у відповідність етапам відомих вербальних моделей APT атаки набір фаз кібернетичної системи зловмисника; кожній фази поставити у відповідність елементарні події у кіберсегменті організації-жертви, які можуть визначатися сенсорами безпеки. Модель дозволяє представити кожну атаку у вигляді набору взаємопов'язаних характеристик елементарних подій на вузлах мережі ІТС. Такий набір (шаблон APT) може бути застосований в рамках автоматизованого детектування атаки засобами SIEM в системах проактивного кіберзахисту.

Ключові слова: кіберзахист, операційний центр кібербезпеки, вдосконала наполеглива загроза, цільова атака, кібернетична модель, стратегія проактивного захисту, кореляція подій кіберпростору, індикатори безпеки, автоматизоване визначення атаки.

Вступ. Аналіз існуючих практик захисту корпоративних інформаційно-телекомунікаційних систем (ІТС) дозволяє виділити дві стратегії протидії кібератакам: реактивний захист і проактивний (превентивний) захист. Загальною основою для цих стратегій є процеси:

1) спостереження в реальному часі (in real time) за подіями в позначеному сегменті кіберпростору;
2) формування за допомогою сенсорів, збір і нормування інформації про події безпеки в єдиному центрі оперативної обробки;
3) аналіз подій і прийняття рішення про наявність кібератаки;
4) прийняття рішення про протидію атаці і реалізація цього рішення за допомогою актуаторів безпеки (виконавчих пристроїв безпеки).

Для *реактивної стратегії* прийняття рішення про виявлення атаки завершується після її закінчення. Заходи протидії можуть запобігти тільки такій же наступній атаці. Для *проактивного (превентивного) захисту* виявлення атаки має відбутися ще до її завершення. У такому випадку залишається час на реалізацію заходів переривання цієї атаки.

Ключовою частиною сучасних систем кіберзахисту корпоративних ІТС є центри операцій кібербезпеки (the CyberSecurity Operations Center, CSOC або SOC). Такі центри за допомогою операторів і/або засобів управління інформацією і подіями безпеки (Security of Information and Event Management, SIEM) з різним ступенем автоматизації реалізують перераховані вище процеси 1-4. Вітчизняні нормативно-правові документи в сфері захисту інформаційно-телекомунікаційних систем в явному вигляді не визначають і не регламентують процеси захисту в режимі реального часу. Як правило, реалізація в рамках комплексної системи захисту інформації (КСЗІ) заходів захисту від несанкціонованих дій (НСД) здійснюється на основі стратегії *реактивної захисту*. Інформація про події безпеки формується комплексом засобів захисту (КЗЗ) від несанкціонованих дій на основі критеріїв (ознак), які закладені ще на етапі проектування. Реакція (відповідь) на інциденти безпеки, як правило, формується після завершення інциденту.

Широкомасштабне застосування проти національної критичної інфраструктури складних кібератак типу APT (Advanced Persisten Threat, вдосконала стійка загроза) стало потужним стимулом для розвитку методів проактивного захисту на основі SOC. Характерним для 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. Незважаючи на різноманітність засобів, що використовуються в APTs, набір більшості тактик і їх сутність залишаються постійними.

Усі ці фактори сприяють розвитку конструктивних методів проактивного кіберзахисту від APTs, що робить актуальними дослідження в цій області. Основними напрямками таких досліджень є наступні:

– розробка теоретичних основ кіберпростору, що дозволяють застосувати інструменти математичної формалізації;

– подання з єдиних позицій дій нападника і заходів проактивного захисту у вигляді сукупності інформаційних процесів;

– розробка моделей інформаційних процесів сегмента кіберпростору, що дозволяють представити різні події безпеки у вигляді наборів елементарних подій;

– методи формування нових наборів індикаторів безпеки на основі знань про тактики, техніках і процедурах зловмисника;

– підвищення ефективності процесів формування, збору, нормалізації і аналізу інформації безпеки (індикаторів безпеки) на основі їх автоматизації;

– розробка моделі взаємозв’язку інформаційних процесів розвідки кіберзагроз та проактивного захисту;

– розробка нових методів виявлення APTs за допомогою засобів SIEM на основі застосування нових моделей APTs і способів формування шаблонів APTs.

Стаття присвячена розробці нової моделі APT. Більшість відомих моделей APT атак представлені у вигляді вербального опису етапів APT і їх смислового змісту. Недолік таких моделей – неможливість прямого застосування в SIEM через відсутність загальної основи для алгоритмізації дій в рамках етапів атаки. В основі іншої групи моделей різні математичні конструкції, що дозволяють уявити масштабні дії зловмисника у вигляді одного складного математичного процесу. Як правило, такі моделі не вважаються найкращими: вони складно зв’язуються з технологічними процесами моніторингу подій в реальному часі.

З позицій автоматизації процесів виявлення складних кібератак в першу чергу стоїть завдання розробки таких моделей APT, які дозволяють алгоритмізувати процес формування індикаторів безпеки на основі аргументованої кореляції подій за часом і простором в спостережуваному кіберсегменті.

Аналіз останніх досліджень і публікацій. Існуючі технології виявлення кібератак засновані на процедурах багаторівневого аналізу великого масиву даних про різноманітні поточні події в інформаційно-телекомунікаційній системі (ІТС). Ці дані збираються в електронних журналах подій (англ. *Logs*). Комплекси програм, які реалізують автоматизовані технології аналізу інформації журналів подій, відомі як системи SIEM. Сутність самого аналізу зводиться до кількох процедур:

– інтерпретація даних журналів подій в контексті заданої політики безпеки;
– формування оцінки про стан безпеки (рішення про наявність або відсутність атаки).

У свою чергу, технології автоматизованого аналізу подій засновані на моделях атак. Як правило, така модель складається із:

– вербального опису атаки;
– математичної інтерпретації цього опису;
– набору правил, які пов’язують дані в журналах подій з елементами математичних конструкцій.

Застосування APTs значно ускладнило ситуацію обробки даних SIEM. Основу APT атаки становить комплекс дій, що реалізуються в різних компонентах ІТС на тривалому відрізку часу. З позицій звичайної політики безпеки такі події окремо можуть нести легальний характер. Очевидно, що модель APT атаки повинна дозволяти пов’язувати ці події за часом і простором. Шаблон APT атаки – це набір інформацій про можливі події в кіберсегменті ІТС, що пов’язані різноманітними правилами. Правила визначаються на основі моделі APT. Порівняння такого шаблону і інформації про поточні події становить суть процесу оцінки в рамках SIEM (прийняття рішення про наявність атаки).

Більшість відомих моделей APT атак представлені у вигляді вербального опису етапів атаки і їх смислового змісту [1] - [4]. Переваги таких моделей – вони виділяють загальні закономірності для різних атак:

– всі APT атаки спрямовані на конкретний ресурс ІТС (цільовий ресурс);
– незалежно від відмінності в цілях і засобах всі APTs проходять однакові етапи: зовнішня розвідка; проникнення в систему; доставка засобів впливу; внутрішня розвідка; цільова акція атаки; приховування слідів атаки.

Недолік таких моделей – неможливість прямого застосування в SIEM через відсутність загальної основи для алгоритмізації дій в рамках етапів.

В основі іншої групи моделей лежать різні математичні конструкції, що дозволяють уявити масштабні дії зловмисника у вигляді одного складного процесу. Однак, такі моделі засновані на представленні у вигляді дерева атаки (графа), в якому елементи (гілки, листя) об’єднуються за допомогою логічних елементів AND або OR [5] - [7]. При використанні таких моделей на рівні оцінки в SIEM може використовуватися мурашиний алгоритм оптимізації (AntColony Optimization, ACO). Такі моделі не вважаються найкращими тому, що вони складно зв’язуються з технологічними процесами в кіберсегменті [8]. Інша концептуальна модель, піраміда атаки, дозволяє відобразити траєкторію нападу в різних складових середовищах ІТС [9]. Виділяються моделі, які ідентифікують атаку на ранніх етапах і прогнозують її розвиток за допомогою прихованої марківської моделі (Hidden Markov Model, HMM) [10]. Практичне застування таких моделей обмежене низкою невизначеностей прихованих станів і складністю реалізації алгоритму Вітербі (Viterby algorithm), що дозволяє визначати стани процесу (тобто, детектувати атаку).

Метою статті є розроблення моделі APT атаки, яка дозволить:

– представити етапи атаки, описані вербальним чином, у вигляді комплексу процедур, які можливо реалізувати автоматизованими процесами;

– представляти дії зловмисника у вигляді комплексу подій, що можливо відображати в різних журналах подій інформацією від сенсорів безпеки;

– описувати взаємозв'язок подій за просторам (по пристроям кіберсегменту) і за часом.

Виклад основного матеріалу дослідження.

1. Корпоративна інформаційно-телекомунікаційна система і APT атака. Одна з особливостей APTs, яка відрізняє їх від звичайних (простих) кібератак, – це спрямованість на конкретні ресурси корпоративних ІТС (наприклад: державних, комерційних). При цьому виділяють такі основні цілі:

1) отримання критичної конфіденційної інформації корпорації, що оброблюється в ІТС;

2) несанкціоноване управління технічними пристроями (системами), що підключені до ІТС;

3) порушення роботи ІТС, що призводить до припинення бізнес-процесів корпорації або значного зниження їх результативності.

Для поглибленого аналізу процесів в рамках APTs необхідно більш детально розібратися зі структурою корпоративної ІТС. У сегменті її кіберпростору можна виділити наступні компоненти (див. рис. 1):

1) комп'ютерна мережа корпорації (КМК);

2) користувачі ІТС (співробітники корпорації, технічні пристрої або системи, які використовують сервіси ІТС);

3) інформаційні ресурси у вигляді даних, які можуть перетворюватися процесорами комп'ютерів, зберігається в різних пристроях пам'яті або передаватися по мережі між комп'терами;

4) набір інформаційних сервісів з обробки даних, якими можу скористатися користувачі в своїх інтересах;

5) інформаційні відносини між користувачами ІТС, які представляють сукупність інформаційного продукту і відповідного сервісу, що формує цей продукт на основі вихідних даних від користувача. Вимоги до інформаційного продукту задаються інтересами користувача.

У свою чергу КМК складається з:

1) електронних комп'ютерних пристроїв, що дозволяють зберігати, перетворювати і передавати/приймати дані від інших комп'ютерів (далі – кінцеві вузли мережі, КВМ);

2) електронних комутаційних пристроїв, що дозволяють перемикати потоки даних між різними кінцевими вузлами мережі (далі – проміжні вузли мережі, ПВМ; комутатори, маршрутизатори і шлюзи);

3) фізичних середовищ поширення електронних сигналів (ФСП), що з'єднують кінцеві і проміжні вузли між собою в єдину мережу (дротові, кабельні або оптоволоконні лінії, різноманітні радіолінії).

Обмін даними між кінцевими вузлами мережі здійснюється шляхом передачі електронних сигналів за маршрутом (послідовність проміжних вузлів і ФСП між ними). Елементи сигналів відповідають двійковим одиницям (бітам). Дані об'єднуються в пакети. Кожен пакет в своєму заголовку містить унікальні адреси вузла призначення і вузла відправника. Маршрут доставки пакета формується на основі адреси призначення шляхом комутації послідовності ФСП відповідними проміжними вузлами.

Кожна мережа характеризується кількістю вузлів (кінцевих і проміжних) і конфігурацією зв'язків між ними на основі ФСП. Як правило, таку характеристику називають топологією мережі. Її можна представити у вигляді графа, в якому вершини відповідають вузлам мережі, а ребра – ФСП між вузлами. Графічно у спрощеному вигляді склад і структуру корпоративної ITS можна представити схемою на рис. 1.

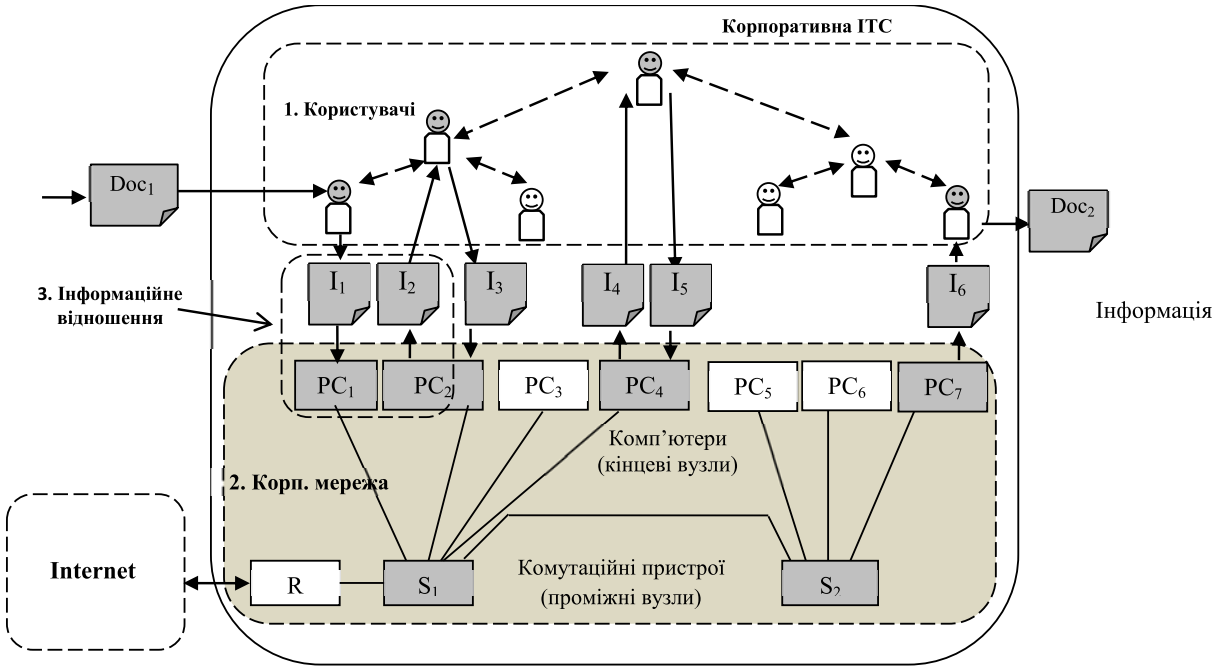

Рисунок 1 – Типова структура корпоративної ІТС і технологія обробки інформації

Для більш повного розуміння сутності APT атаки також доцільно конкретизувати сутність обробки інформації в ІТС. Інформаційні сервіси в КВМ реалізуються за допомогою обчислювальних процесів. Під таким процесом розуміють сукупність програми, яка виконується процесором комп'ютера, і задіяних при цьому його ресурсів (сегменти пам'яті даних і програм, вміст різних регістрів процесора, ресурси операційної системи, периферійні апаратні засоби комп'ютера та інше). Процеси кінцевих вузлів мережі запускаються або операційними системами, або авторизованими користувачами.

У рамках ІТС з метою реалізації завдань, що стоять перед корпорацією, можуть бути реалізовані різні автоматизовані технології обробки інформації. Кожна з таких технологій являє сукупність:

– користувачів, що пов'язані функціональними обов'язками і ієрархією підлеглості;
– інформаційних ресурсів ІТС (файли, бази даних, бази знань, веб-сайти та інше);
– інформаційних сервісів (обмін інформацією, розповсюдження інформації, перетворення даних, зберігання даних та інше);
– комп'ютерів, що реалізують інформаційні сервіси за допомогою наборів своїх обчислювальних процесів;
– інформаційних відносин між користувачами ІТС (тобто, сукупність: вхідна інформація від користувача; визначений сервіс; інформаційний продукт на виході сервісу).

Сукупність дій над інформацією, що реалізується за допомогою користувачів і сервісів комп'ютерної мережі, складають технологію обробки інформації (ТОІ).

Представлена вище деталізація дозволяє уточнити суть дій зловмисника в рамках APT атаки. Після визначення корпоративної ІТС 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 ІТС з різноманітних джерел поза нею.

Етап 2. Проникнення в ІТС. На основі інформації зовнішньої розвідки приймається рішення про засоби і способи запуску несанкціонованих процесів в одному з КВМ ІТС. За допомогою комп'ютера зловмисника здійснюється реалізація рішення шляхом направлення через Інтернет необхідних даних. На основі прийнятих повідомлень запускаються процеси, які встановлюється прихований канал віддаленого управління КВМ.

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 приймається рішення про засоби і способи реалізації цільового впливу. За допомогою прихованого каналу управління критичним кінцевим вузлом 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 та інше).

Етап 6. Приховування слідів атаки. За допомогою несанкціонованих процесів на всіх кінцевих вузлах стираються дані, які були пов'язані з атакою.

2. APT атака і поведінка кібернетичної системи. В рамках вище представленої вербальної моделі APT атаки на корпоративну ІТС можна виділити загальну для всіх її різновидів послідовність дій, яка регулярно повторюється на всіх етапах:

- отримання зловмисником інформації про стан компонентів корпоративної ІТС;
- прийняття рішення про подальші дії;
- реалізація несанкціонованих дій в ІТС доставленими або штатними засобами;
- отримання інформації про результати цих дій (несанкціонованого впливу).

Такий регулярний порядок дій дозволяє представити APT атаку у вигляді траєкторії поведінки керованої (кібернетичної) системи. У такій системі, назвемо її кібернетичної системою APT атаки (CyberSystem of APT, CSoA), можна виділити наступні компоненти:

- об'єкт управління (Management Object, MO) – це може бути комп'ютер, комутаційне обладнання мережі, обчислювальні процеси в цих пристроях, або будь-які інформаційні ресурси (файли, бази даних та інше);
- підсистема управління (Control SubSystem, CSS), яка складається з:
- центру управління (Control Center, CC) – зловмисник і його комп'ютер;
- сенсора (sensor, S) і актуатора (actuator, A) – це процеси комп'ютерів, які відповідають за передачу інформації про стан об'єкта управління і прийому інформації про керуючий вплив;
- прямого і зворотного каналу зв'язку (*Forward Link, FL; Return Link*, *RL*) – це комп'ютерна мережа Internet, що забезпечує обмін інформацією між центром управління CC і об'єктом управління MO.

У рамках задачі автоматизації технології виявлення APT атаки CSoA необхідно представити у вигляді такої моделі кібернетичної системи, яка дозволяє описати її поведінку за допомогою математичних конструкцій. З цією метою обрано базову модель інформаційного процесу управління [11]. Вона заснована на атрибутивно-трансферному представленні суті інформації і представляє процеси кібернетичної системи у вигляді сукупності різних інформацій та операцій з цією інформацією. На відміну від інших моделей тут інформація та її зміст (семантика) позначаються в явному вигляді. Крім цього кожен інформаційний об'єкт може бути описаний за допомогою математичної мови теорії множин. Також за допомогою моделі може бути представлена траєкторія поведінки кібернетичної системи через математичний опис взаємозв'язку її суміжних фаз (станів) кібернетичної системи.

При розробці моделі CSoA використовувалося ряд тверджень, які дозволили спростити графічний і математичний опис ситуації:

– будь-які характеристики та стан кінцевого вузла комп'ютерної мережі можна представити у вигляді кінцевої множини двійкових одиниць (бітів);

– інформація про будь-який стан будь-якого кінцевого вузла, яка передається через мережу до будь-якого іншого вузлу, може бути представлена також множиною бітів, як і сам стан;

– роль сенсора кібернетичної системи в комп'ютері виконує обчислювальний процес, який передає інформацію про стан комп'ютера через мережу за вказаною адресою;

– роль актуатора кібернетичної системи в комп'ютері виконує процес, який на основі прийнятих команд запускає нові процеси, що виконують необхідні дії.

Дані твердження дозволяють спростити початкову модель [11] і представити графічно дві суміжні фази CSA у вигляді наступної структури (див. рис. 2).

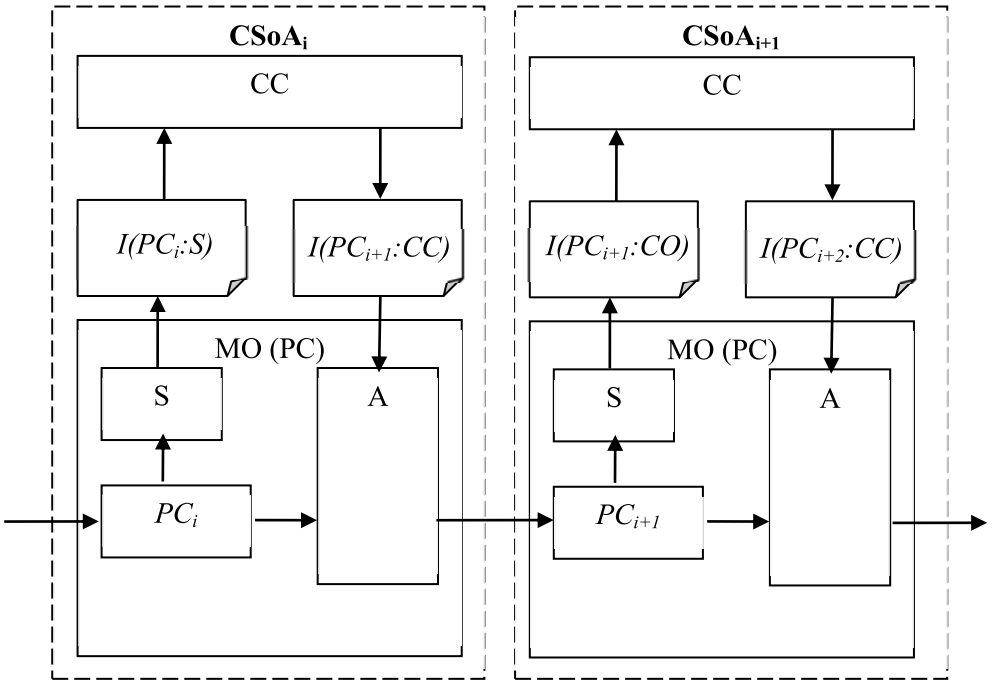

Рисунок 2 – Графічна модель кібернетичної системи APT атаки (CyberSystem of APT, CSoA)

У рамках моделі 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 $I(PC_{i+1}{:}CO)$. Далі ця інформація пересилається до *CO*, де прийняте рішення реалізується за допомогою актуатора *A*: об'єкт управління переходить в наступний стан PC_{i+1}.

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

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

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

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

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

Отримані результати графічної і математичної формалізації *CSA* дозволяють математично представити всю APT атаку у вигляді множини:

$$APT = \{CSoA_i\}, i = 1,..,I, \quad (2)$$

де APT – це кінцева множина, що складається з кінцевих підмножин $CSoA_i$ (відповідних фаз 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 фаз *CSoA* пов'язані між собою системою рівнянь (1);

i – номер поточної фази *CSA*, I - кількість фаз APT атаки, $i = 1,..,I$.

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 рис. 3.

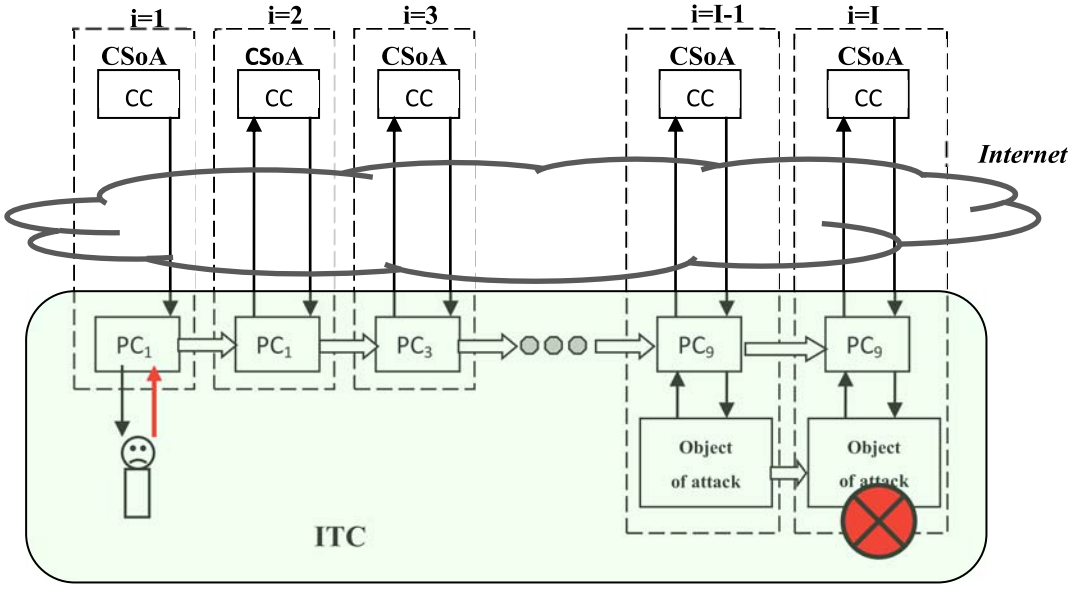

Рисунок 3 – Графічне представлення кібернетичної моделі APT атаки

На рис. 3 в рамках фази 1 ($CSoA_1$) відображено застосування зловмисником прийому "фішинг" (англ. phishing). Тобто, провокування користувача системи на дії, що порушують вимоги політики безпеки.

За допомогою запропонованої моделі можливо:

– кожен етап вербальної моделі представити у вигляді однієї або декількох фаз кібернетичної системи;

– кожну фазу представити у вигляді конкретних подій (процедур атаки), що можуть бути зафіксовані на конкретних пристроях корпоративної ІТС;

– кожну процедуру атаки пов'язати із елементарними подіями або набором елементарних подій в ІТС.

Можливо розглядати два види елементарної події:

1) обчислювальний процес вузла мережі;

2) послідовність даних, якими обмінюються обчислювальні процеси вузлів мережі (трафік між процесами вузлів мережі).

З одного боку кожна елементарна подія пов'язана із набором індивідуальних характеристик конкретного вузла (вузлів) 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.

З іншого боку кожна елементарна подія може бути процедурою інформаційного процесу управління кібернетичної системи зловмисника. Відповідно до запропонованої моделі це дозволяє представити дії зловмисника не тільки у вигляді вербального опису в рамках етапів APT, а й у вигляді послідовності фаз кібернетичної системи. У свою чергу кожна послідовність фаз може бути подана у вигляді послідовності елементарних подій із конкретними характеристиками. Таким чином, кожну APT можливо представити у вигляді набору взаємопов'язаних характеристик елементарних подій на вузлах мережі ІТС. Такий набір є шаблоном APT, що може застосовуватися в рамках автоматизованого детектування атаки засобами SIEM.

3. Кібернетична модель і шаблон APT атаки. Одержана модель дозволяє розробити наступну ієрархічну структуру шаблона для APT атаки (див. табл.1).

Таблиця 1 – Ієрархічна структура шаблону APT

I. Етапи атаки	**1 Проникнення**								**2 Доставка засобів впливу**				…	**N Цільова акція атаки**					
II. Фази атаки	1.1			1.2		1.3			2.1		2.2			N.1		N.2		N.3	
III. Процедури атаки	1.1.1	…	1.1.5	1.2.1	1.2.2	1.3.1	…	1.3.4	2.1.1	2.1.2	2.2.1	2.2.2		N.1.1	N.1.2	…	…	…	N.3.4

Рівень 1 структури відображає послідовність етапів APT, що описуються вербальним чином.

Рівень 2 відображає послідовність фаз атаки ($CSoA_i$), що відповідають стану кібернетичної системи. Кожна фаза пов'язана із конкретним вузлом корпоративної мережі (комп'ютери і комутаційні пристрої).

Рівень 3 представляє послідовність станів фаз кібернетичної системи, тобто сукупність PC_i, $I(PC_i:S)$ і $I(PC_{i+1}:CC)$. Кожна така компонента відповідає елементарній події і може представлятися у вигляді набору даних (індикатор події). Кожний індикатор має свою комірку в шаблоні. Шаблон пов'язує всі індикатори за кібернетичним простором і часом.

Для визначення APT необов'язково заповнювати всі комірки шаблону (повний набір індикаторів подій). За деяких умовах достатньо обмежиться тільки набором індикаторів подій, що відповідають деяким фазам атаки (неповний набір подій). Не обов'язково фази можуть бути суміжними.

Надана структура шаблону відповідає "класичній" кібернетичній моделі APT. Для атак, що мають свої особливості (відсутність каналу управління; відсутність зворотного зв'язку; відсутність етапу внутрішньої розвідки та інше) необхідно формувати свої структури шаблонів на основі базової структури.

На основі доступних матеріалів про APT атаку на ПАТ "Прикарпаттяобленерго" в грудні 2015 року (міжнародна назва атаки – BlackOut) складено фрагменти шаблону атаки для етапів "Проникнення" і "Внутрішня розвідка". В рамках експерименту на комп'ютерному макеті застосування цих фрагментів дозволило виявити відповідні несанкціоновані дії "зловмисника".

Висновки. На основі кібернетичного підходу розроблено модель APT атаки. Сутність підходу – відносно комп'ютерів організації-жертви зловмисник регулярно виконує дії із циклу управління. Це дозволяє представити APT атаку у вигляді траєкторії поведінки керованої (кібернетичної) системи. В рамках моделі поведінка кібернетичної системи зловмисника представлена через математичний опис інформаційних процесів управління і ітеративний взаємозв'язок між суміжними фазами (станами) кібернетичної системи. Такий підхід дозволяє в рамках ієрархічної структури моделі:

– поставити у відповідність етапам відомих вербальних моделей APT атаки набір фаз кібернетичної системи зловмисника;

– кожній фази поставити у відповідність елементарні події у кіберсегменті організації-жертви, які можуть визначатися сенсорами безпеки.

Таким чином, за допомогою моделі кожну APT можливо представити у вигляді набору взаємопов'язаних характеристик елементарних подій на вузлах мережі ІТС. Такий набір є шаблоном APT, що може застосовуватися в рамках автоматизованого детектування атаки засобами SIEM в системах проактивного кіберзахисту.

Працездатність моделі перевірено в рамках експерименту на комп'ютерному макеті. Застосування фрагментів шаблону для атаки на ПАТ "Прикарпаттяобленерго" (грудень 2015 року, міжнародна назва – BlackOut) дозволило виявити відповідні несанкціоновані дії "зловмисника" на етапах "Проникнення" і "Внутрішня розвідка".

У перспективах подальших досліджень планується на основі запропонованої моделі розробити:

– методи визначення індикаторів компрометації (Indicators of Compromise, IoC) для системи моніторингу;

– методи збору і аналізу інформації про події безпеки;

– порядок визначення кібервторгнень;

– порядок визначення 0day APT (атаки "нулевого дня");

– порядок прийняття рішення про підготовку відповіді на вторгнення і його реалізація.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] P. Chen, and L. Desmet, and C. Huygens, "A study on Advanced Persistent Threats", in Proc. *15th IFIP TC 6/TC 11 International on Conference Communications and Multimedia Security*, Aveiro, Portugal, 2014, pp. 63-72. doi: 10.1007/978-3-662-44885-4_5.

[2] E. M. Hutchins, M. J. Clopperty, and R. M. Amin, "Intelligence-Driven Computer Network Defense", Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation, 2009. [Online]. Available: https://www.lockheedmartin.com/.content/dam/lockheed/data/corporate/documents/ LM-White-Paper-Intel-Driven-Defense.pdf.

[3] "Mandiant M-Trends: The Advanced Persistent Threat". Mandiant, 2010. [Online]. Available: https://wikileaks.org/hbgary-emails//fileid/27714/8307.

[4] D. Whitehead, K. Owens, D. Gammel, and J. Smith, "Schweitzer. Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies". Engineering Laboratories, Inc. Published in Wide-Area Protection and Control Systems: A Collection of Technical Papers Representing Modern Solutions", in *Proc. 70th Annual Conference for Protective Relay Engineers, 2017.* [Online]. Available: https://doi.org/10.1109/CPRE.2017.8090056. doi: 10.1109/CPRE.2017.8090056.

[5] S. Camtepe, and B. Yener, “Modeling and detection of complex attacks”, in. *Proc. 3th International Conference on Security and Privacy in Communications Networks and the Workshops*, Nice, 2007. pp. 234-243.
doi: 10.1109/SECCOM.2007.4550338.

[6] F. Arnold, H. Hermanns, R. Pulungan, and M. Stoelinga, “Time-dependent analysis of attacks”, *Principles of Security and Trust, Lecture Notes in Computer Scienc*e, vol. 8414, pp. 285-305, 2014. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-54792-8_16.
doi: 10.1007/978-3-642-54792-8_16.

[7] O. Flåten, and M. Lund, “How good are attack trees for modelling advanced cyber threats?”, in Proc. Norwegian Information Security Conference, Fredrikstad, 2014, pp. 1-4.

[8] J. Navarro, V. Legrand, and al., “HuMA: A multi-layer framework for threat analysis in a heterogeneous log environment”, in *Proc. International Symposium on Foundations and Practice of Security*, Schiltigheim, 2015. [Online]. Available: http://fps2017.loria.fr/wp-content/uploads/2017/10/08.pdf.

[9] P. Giura, and W. Wang, “Using large scale distributed computing to unveil advanced persistent threats”, *SCIENCE,* no. 1 (3), pp. 93-105, 2013.

[10] Z. Cui, I. Herwono, P. Kearney, “Multi-stage attack modeling”, in *Proc. of Cyberpatterns,* Abingdon, 2013, pp. 78-89.

[11] I. 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.

Стаття надійшла до редакції 6 лютого 2018 року.

REFERENCE

[1] P. Chen, and L. Desmet, and C. Huygens, “A study on Advanced Persistent Threats”, in Proc. *15th IFIP TC 6/TC 11 International on Conference Communications and Multimedia Security*, Aveiro, Portugal, 2014, pp. 63-72.
doi: 10.1007/978-3-662-44885-4_5.

[2] E. M. Hutchins, M. J. Clopperty, and R. M. Amin, “Intelligence-Driven Computer Network Defense”, Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation, 2009. [Online]. Available: https://www.lockheedmartin.com/ content/dam/lockheed/data/corporate/documents/ LM-White-Paper-Intel-Driven-Defense.pdf.

[3] “Mandiant M-Trends: The Advanced Persistent Threat”. Mandiant, 2010. [Online]. Available: https://wikileaks.org/hbgary-emails//fileid/27714/8307

[4] D. Whitehead, K. Owens, D. Gammel, and J. Smith, “Schweitzer. Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies”. Engineering Laboratories, Inc. Published in Wide-Area Protection and Control Systems: A Collection of Technical Papers Representing Modern Solutions”, in *Proc. 70th Annual Conference for Protective Relay Engineers, 2017.* [Online]. Available: https://doi.org/10.1109/CPRE.2017.8090056.
doi: 10.1109/CPRE.2017.8090056.

[5] S. Camtepe, and B. Yener, “Modeling and detection of complex attacks”, in. *Proc. 3th International Conference on Security and Privacy in Communications Networks and the Workshops*, Nice, 2007. pp. 234-243.
doi: 10.1109/SECCOM.2007.4550338.

[6] F. Arnold, H. Hermanns, R. Pulungan, and M. Stoelinga, “Time-dependent analysis of attacks”, *Principles of Security and Trust, Lecture Notes in Computer Scienc*e, vol. 8414, pp. 285-305, 2014. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-54792-8_16.
doi: 10.1007/978-3-642-54792-8_16.

[7] O. Flåten, and M. Lund, “How good are attack trees for modelling advanced cyber threats?”, in Proc. Norwegian Information Security Conference, Fredrikstad, 2014, pp. 1-4.

[8] J. Navarro, V. Legrand, and al., “HuMA: A multi-layer framework for threat analysis in a heterogeneous log environment”, in *Proc. International Symposium on Foundations and Practice of Security*, Schiltigheim, 2015. [Online]. Available: http://fps2017.loria.fr/wp-content/uploads/2017/10/08.pdf
[9] P. Giura, and W. Wang, “Using large scale distributed computing to unveil advanced persistent threats”, *SCIENCE,* no. 1 (3), pp. 93-105, 2013.
[10] Z. Cui, I. Herwono, P. Kearney, “Multi-stage attack modeling”, in *Proc. of Cyberpatterns,* Abingdon, 2013, pp. 78-89.
[11] I. 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.

ИГОРЬ ЯКОВИВ

КИБЕРНЕТИЧЕСКАЯ МОДЕЛЬ APT АТАКИ

Широкомасштабное применение сложных кибератак типа APT относительно критической инфраструктуры стало мощным стимулом для развития методов проактивной киберзащиты. Характерным для APTs является сложный набор взаимосвязанных по времени и пространству действий злоумышленника. Отдельно действия могут не вызывать подозрений; целевая акция атаки в киберсегменте объекта-жертвы готовится длительное время (от нескольких месяцев до года и более); совокупность действий злоумышленника – это цепочка тактик, выполнение которых позволяет достичь цели атаки. Средства реализации тактик – разнообразны. Набор тактик и их сущность остаются постоянными. Большинство известных моделей APT атак представлены в виде вербального описания этапов APT и их смыслового содержания. Недостаток таких моделей – невозможность прямого применения в SIEM-за отсутствия общей основы для алгоритмизации действий в рамках этапов атаки. В основе другой группы моделей разные математические конструкции, позволяющие представить масштабные действия злоумышленника в виде одного сложного математического процесса. Как правило, такие модели сложно связывать с технологическими процессами мониторинга событий в реальном времени. С позиций автоматизации процессов обнаружения атак в первую очередь стоит задача разработки таких моделей APT, которые позволяют алгоритмизировать процесс формирования индикаторов безопасности на основе аргументированной корреляции событий по времени и пространству. Статья посвящена разработке новой модели APT на основе кибернетического подхода. Сущность подхода – относительно компьютеров организации-жертвы злоумышленник регулярно выполняет действия из цикла управления. Это позволяет представить APT атаку в виде траектории поведения управляемой (кибернетической) системы. В рамках модели поведение кибернетической системы злоумышленника была представлено через математическое описание информационных процессов управления и итеративную взаимосвязь между смежными фазами (состояниями) кибернетической системы. Такой подход позволяет в рамках иерархической структуры модели: вербальным этапам атаки поставить в соответствие набор фаз кибернетической системы злоумышленника; каждой фазе поставить в соответствие элементарные события в киберсегменте организации-жертвы, которые могут определяться сенсорами безопасности. Модель позволяет представить каждую атаку в виде набора взаимосвязанных характеристик элементарных событий на узлах компьютерной сети. Такой набор (шаблон APT) может быть применен в рамках автоматизированного детектирования атаки средствами SIEM в системах проактивной киберзащиты.

Ключевые слова: киберзащита, операционный центр кибербезопасности, усовершенствованная стойкая угроза, целевая атака, кибернетическая модель, стратегия проактивной защиты, корреляция событий киберпространства, индикаторы безопасности, автоматизированное определение атаки.

IHOR YAKOVIV

CYBERNETIC MODEL OF THE ADVANCED PERSISTEN THREAT

The widespread use of sophisticated cyberattacks such as Advanced Persisten Threat with regard to critical infrastructure has become a powerful incentive for the development of proactive cyber defense techniques. Typical for APTs are a complex action set of malicious actor that are related time and space. Separately, these actions may not cause suspicion; targeted attack actions on the cyber segment of the victim object is being prepared for a long time (from a few months to a year or more); a set of actions of the intruder are a chain of tactics, the execution of which allows to achieve the purpose of the attack. Means of implementing tactics are varied. The set of tactics and their essence remain constant. Most of the known models of APT attacks are presented in the form of a verbal description of the stages of the APT and their semantic content. The disadvantage of such models is the impossibility of direct application in the SIEM due to the lack of a common basis for the algorithmization of actions during the attack stages. At the base of another group of models are different mathematical constructions that allow one to represent large-scale actions of an attacker in the form of one complex mathematical process. As a rule, such models are difficult to associate with technological processes for monitoring events in real time. From the standpoint of automating the detection of attacks, the first task is to develop such APT models that allow you to algorithmize the process of generating compromise indicators based on a reasoned correlation of events over time and space. The article is devoted to the development of a new model of APT based on a cybernetic approach. This allows you to imagine an attack in the form of a behavior trajectory of a controlled (cybernetic) system. Within the framework of the model, the behavior of the attacker cybernetic system was presented through a mathematical description of information management processes and the iterative relationship between adjacent phases (states) of the cybernetic system. This approach allows the attack to be presented in the form of a hierarchical structure: the upper level is a sequence of verbal stages of an attack; the middle level is a sequence of phases of the cybernetic system; lower level is a sequence of control loop procedures. Procedures are elementary events (transmitted data and computational processes) that are detected by security sensors at the nodes of a computer network. The model allows us to represent each attack as a set of interrelated characteristics of elementary events at the nodes of a computer network. Such a set (APT pattern) can be applied within the framework of automated attack detection using SIEM tools in proactive cyber defense systems.

Keywords: cyber defense, cybersecurity operation center, advanced persistent threat, targeted attack, cybernetic model, proactive defense strategy, correlation of cyberspace events, indicators of compromise, automated attack detection.

Ігор Богданович Яковів, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та 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.

Игорь Богданович Яковив, кандидат технических наук, доцент, доцент кафедры кибербезопасности и применения автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

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