NETWORK AND APPLICATION SECURITY

DOI: 10.20535/2411-1031.2018.6.2.153490
УДК 004.056.5

АРТЕМ ЖИЛІН,
МИКОЛА ХУДИНЦЕВ,
МАКСИМ ЛІТВІНОВ

ФУНКЦІОНАЛЬНА МОДЕЛЬ СИТУАЦІЙНОГО ЦЕНТРУ КІБЕРЗАХИСТУ

У загальному випадку питання побудови центрів кіберзахисту зводяться до побудови SOC, основною функцією якого є моніторинг й аналіз кіберзахисту та реагування на кіберінциденти онлайн. В зазначеному підході не завжди приділяється увага етапам попередження вторгнень й усунення наслідків кібератак. Існуючі дослідження показують можливість розширення функції SOC, але вони не формалізовані й не описані з точки зору функцій, що покладаються на такий Ситуаційний центр кіберзахисту. Метою даної роботи визначено аналіз наявних моделей забезпечення кібербезпеки й побудова функціональної моделі сучасного центру кіберзахисту. Для досягнення поставленої мети в статті проводились дослідження моделей аналізу кібератак з позиції дослідника (Діамантова модель та Q Модель), реалізації кібератак з позиції атакуючого (Модель Cyber Kill-Chain) та моделей, що враховують більш широкий спектр аналітичних підходів (Адаптивна модель безпеки). Ґрунтуючись на потребах в даних для аналізу кібератак, враховуючи етапи проведення кібератак та беручи за основу архітектуру Адаптивної системи безпеки визначено функції забезпечення кіберзахисту до, під час та після проведення кібератак. Результати аналізу вибраних моделей дозволили також запропонувати Організаційну модель ситуаційного центру кіберзахисту, визначити його складові та сформулювати основні функції. Так запропоновано реалізувати побудову Ситуаційного центру кіберзахисту шляхом впровадження Підрозділу розвідки кіберзагроз, Підрозділу моніторингу та управління інцидентами безпеки та Команди реагування на кіберінциденти. В зазначеній моделі показано зв'язки між структурами та потоки інформації, що між ними циркулює. На основі вимог нотацій IDEF представлено функціональну модель рівнів A-0 та A0. Визначено головну функцію центру кіберзахисту, вхідні та вихідні дані, а також ресурси, що використовуються при функціонуванні центру, та обмеження, в умовах яких центр діє. Представлені нотації графічно відображають результати функціонального аналізу центру кіберзахисту й дають змогу сформувати вимоги до його складових, а в подальшій декомпозиції – сформувати організаційну структуру кожного підрозділу й розробити функціональні обов'язки кожного співробітника.

Ключові слова: діамантова модель, Q Модель, Cyber Kill-Chain, адаптивна модель кібербезпеки, ситуаційний центр кіберзахисту, індикатори компрометації, кіберінцидент, функціональна модель, IDEF.

Постановка проблеми. Активний розвиток універсальності комунікацій, конвергенції мереж, поширення мобільних платформ, соціальних мереж та додатків віддаленого використання призвели до того, що втрачається поняття периметру захисту, внаслідок чого змінюється не лише ландшафт загроз, але й розпорошуються зусилля захисту, знижується його ефективність. В той же час зловмисники, які заподіювали незначної шкоди, поступилися місцем сучасній кіберзлочинності – витонченій, добре фінансованій і здатній викликати тривалі збої в роботі компаній і державних установ. Атаки, що вони реалізують, стали не тільки менш помітними, тривалішими у часі, але і все частіше мають направлену дію, здатні накопичувати мережеві ресурси для збільшення радіусу дії на майбутнє. Це

пов’язано, в першу чергу, з активною комерціалізацією «хакерства» та підтримкою його на державних рівнях. Тобто змінилися мотиви зловмисників і підходи до реалізації кібератак [1].

В свою чергу більшість систем захисту націлені на моніторинг мережі або кінцевих пристроїв й блокування шкідливого програмного забезпечення в точці входу. Ці інструменти одразу ж сканують файли або мережевий трафік на наявність загроз, як правило, використовуючи сигнатурний метод. Якщо ж шкідливе програмне забезпечення доставляється до місця призначення частинами, або воно модифікується, стаючи шкідливим після потрапляння до пристрою, то дані технології виявлення вже не зможуть помітити наступні дії з розгортання атаки. При цьому нові атаки не можна назвати одномоментними: вони тривають довго і вимагають постійної уваги. Тобто традиційні методи захисту, що використовуються в підрозділах забезпечення кіберзахисту, метою яких є лише виявлення і блокування атак в точці входу, більше не ефективні. Тому **актуальним** стає розроблення нової моделі центру кіберзахисту, в якій враховується весь період атаки, максимальний спектр підходів до оцінки загроз та арсенал можливостей інших споріднених видів діяльності (кіберрозвідки, кіберконтррозвідки, кібероборони).

Аналіз останніх досліджень і публікацій. Сучасні публікації [2], [3] показують, що в більшості випадків питання побудови центрів кіберзахисту зводяться до побудови SOC (Cybersecurity Operations Center – Центр управління кібербезпекою). В той же час в [4], [5] показана можливість розширення функції SOC за рахунок введення етапів розвідки загроз та реагування та кіберінциденти, але запропонований підхід не формалізований й не описаний з точки зору функцій, що покладаються на такий центр кіберзахисту.

Тому **метою** даної роботи є аналіз моделей в сфері кібербезпеки й побудова функціональної моделі сучасного центру кіберзахисту.

Виклад основного матеріалу дослідження. Ситуаційний центр кіберзахисту повинен не тільки реагувати на атаки, що тривають, а й здійснювати превентивні заходи щодо попередження кібератак та проводити оброблення й ретроспективний аналіз кіберінцидентів. Окрім цього, при побудові центру кіберзахисту необхідно враховувати не лише етапи реалізації кібератак, але й весь спектр підходів до їх аналізу і синтезу, а також максимальний арсенал можливостей інших споріднених видів діяльності. Слід зауважити, що аналіз принципових відмінностей між суб’єктами кіберзахисту, кіберконтррозвідки, кібероборони, кіберрозвідки тощо виходить за межі даного наукового дослідження та може мати дискусійний характер. Проте автори вважають достатнім для досягнення поставленої мети дослідження врахувати (але не обмежуватись) такі тези:

– по-перше, є суттєвою відмінність між денотатами, які вживає законодавець відносно законодавчого тлумачення понять “кібербезпека” (захищеність, стан захищеності) та “кіберзахисту”, “кібероборона” (сукупність заходів, діяльність). Позначена відмінність впливає на підходи до визначення (оцінки) обсягу цих понять, а також дозволяє якісніше підійти до інтерпретації їх зв’язку (кореляції) з поняттями “кіберзагрозам”, “вразливість”;

– по-друге, є значною відмінність між сукупністю цілей, законних повноважень та похідних від них специфічних методів та засобів діяльності суб’єктів розвідки, контрозвідки, поліції, військових підрозділів або комерційних структур. Позначена відмінність обґрунтовується системними загрозами, на протидію яким в Україні вже сформовані інституції, організаційні структури та відповідне правове поле.

Серед формалізованих моделей аналізу кібератак найбільшої уваги заслуговують Діамантова модель (Diamond Model) [6] та Q Модель (Q Model) [7].

Діамантова модель представляє нову концепцію аналізу вторгнень, побудовану аналітиками кібербезпеки. Модель встановлює, що основний «атомний елемент» будь-якої діяльності зі вторгнення чи кіберінцидент, складається з чотирьох основних функцій: зловмисника, інфраструктури, спроможності та жертви (див. рис. 1). При виявлені події автоматизовано або за допомогою аналітиків заповнюються вершини моделі. Вершини пов'язані ребрами й виділяють природні зв’язки між функціями. Проходячи по ребрах та вершинах, аналітики виявляють більше інформації про операції зловмисника та виявляють нові спроможності, інфраструктуру та жертв.

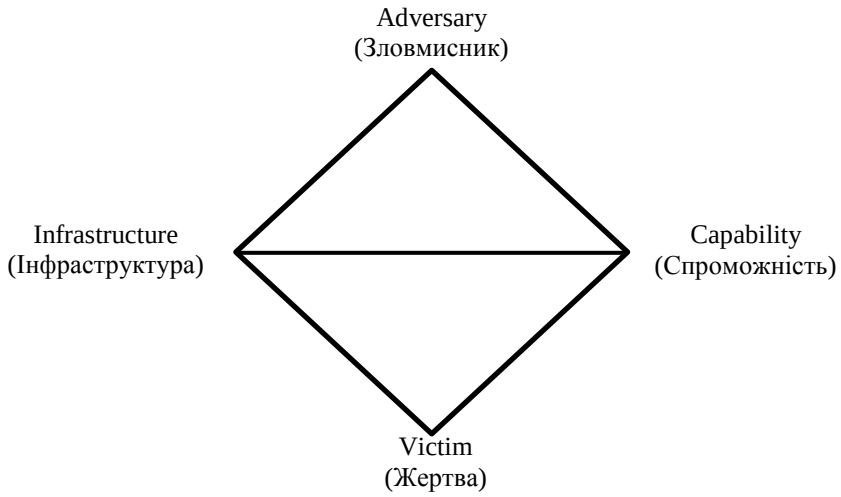

Рисунок 1 – Діамантова модель аналізу вторгнень [6]

Модель також визначає додаткові мета-функції для підтримки конструкцій вищого рівня. До мета-функцій відносяться часовий штамп (як початок, так і кінець), етап, результат, напрямок, методологія та ресурси. Ці елементи вносять вклад в фундаментальну та всеосяжну модель вторгнення, побудовану навколо аналітичних процесів. Вона фіксує основні поняття аналізу вторгнень та суперечливих операцій, одночасно дозволяючи гнучким чином розширювати та охоплювати нові ідеї та концепції.

Ця модель встановлює наукові принципи та застосовує формальні методи до аналізу вторгнень, зокрема вимірювання, тестування та порівняння, що забезпечує комплексну методику документування, синтезу та кореляції процесів під час діяльності дослідника вторгнень. Цей науковий підхід і простота дають покращення аналітичної ефективності, продуктивності та точності. Зрештою, Діамантова модель забезпечує можливості інтеграції розвідки вразливостей в режимі реального часу для захисту мереж, автоматизації і кореляції подій, їх класифікації за рівнем впевненості в кампаніях протистояння, прогнозування суперечливих операцій при плануванні, у розробки стратегій зменшення ігрових витрат.

Зазначимо переваги Діамантової моделі:

– дозволяє використовувати контекстні і взаємозалежні індикатори, що покращують обмін інформацією про кіберзагрози і розширює діапазон застосовності індикаторів;

– підвищує аналітичну точність, забезпечуючи генерацію гіпотез, документування та тестування, тим самим підвищує контрольованість аналітичного процесу;

– підтримує курс розробки дій, планування та стратегії пом'якшення наслідків, легко інтегруючись практично з будь-яким планом;

– визначає різницю в отриманих даних через фазовий підхід та включення вимог зовнішніх ресурсів як основної мета-функції;

– підтримує характеристику подій у режимі реального часу шляхом картографування аналітичного процесу на добре зрозумілу класифікацію та дослідження виявлення вторгнень;

– встановлює основи онтологій, таксономій, методик кіберзахисту та протоколів обміну розвідувальною інформацією про загрози, а також управління знаннями.

Q Модель дозволяє визначити атрибути кібератаки для з’ясування питання того, чи є кіберінцидент кіберзлочином. На рівні тактики модель допомагає аналітикам вирішувати весь спектр відповідних питань, інтегрувати як технічну, так і нетехнічну інформацію в конкуруючі гіпотези, допомагає критично мислити та провести результативне розслідування. Підхід включає в себе перехід до більш складних питань на нижчих рівнях їх конкертизації, включаючи детальні технічні питання, а також більш широкі, більш аналітичні операційні питання при підвищенні рівня конкретизації.

Стратегічно модель допомагає уточнити та продемонструвати сутність процесу атрибуції для зовнішньої презентації у відповідній оціночній мові. Цей підхід має на меті допомогти сформувати та обгрунтувати політичні судження про серйозні наслідки, робити належні висновки на високому рівні абстрагування.

Представлена в [7] модель є описовою й складається з трьох частин (див. рис. 2). Перша частина концептуальна: вона вводить розуміння атрибуції як процесу, описуючи модель в загальних рисах та вводячи кілька критичних відмінностей. Друга частина є емпіричною: вона ілюструє різні етапи процесу атрибуції в динаміці. У третій частині описується комунікація потенціалів та обмежень атрибуції й перетворення висновків у дію.

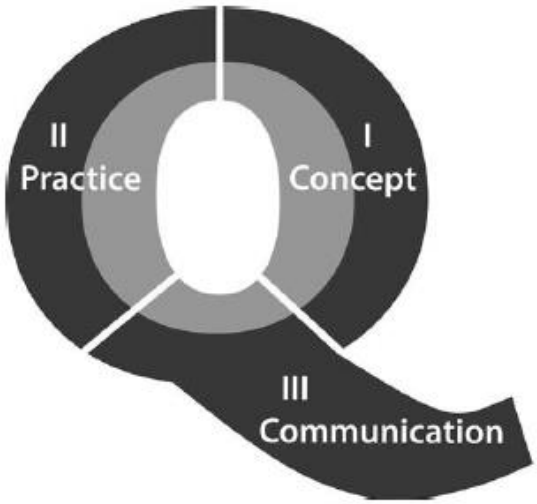

Рисунок 2 – Частини Q моделі [7]

Ці частини моделі можна назвати своєрідними рівнями, на яких проводиться атрибуція кібератаки. На кожному рівні атрибуції є свій дискретний аналітичний виклик, який спирається на конкретні вхідні дані та спеціальні знання та висвітлює окремий аспект успішної атрибуції. Аналіз на кожному рівні повинен бути інформативним та закінченим. Хоча процес атрибуції, як правило, має початок і кінець, цикл не обов'язково відповідає певному послідовному чи хронологічному порядку, оскільки гіпотези стикаються з новими деталями, а нові деталі породжують нові гіпотези. Тим не менше, рівні являють собою окремі завдання, які, хоча й взаємопов'язані, розглядаються окремо.

Результатом атрибуції будуть індикатори компрометації та нові знання про механізм, цілі, засоби тощо. Але вони будуть різнитися в залежності від рівня розгляду: стратегічний, операційний чи тактико-технічний. Атрибуція на тактико-технічному рівні полягає в розумінні інциденту в першу чергу в його технічних аспектах – “Як?”. Операційний рівень – розуміння архітектури високого рівня атаки та профілю атакуючого – “Що?”. На стратегічному рівні метою є розуміння, хто відповідає за атаку, оцінку мети, обґрунтування мотиву нападу, значення наслідків для нападника, тобто – “Хто і Чому?”. При чому атрибуція на рівнях є пов’язаною. Так визначення атрибутів на тактичному рівні (IP- адреса, заголовок електронного листа, тощо) може допомогти у визначені атрибутів операційного й стратегічного рівнів (мета угруповань й країн).

Оскільки інформація надходить від технічного до операційного та стратегічного рівнів, вона повинна бути синтезована. Так, первинний технічний аналіз може, залежно від інциденту, дати детальну інформацію про конкретні вторгнення і в цьому полягає його користь для дослідника. Проте відсутність належного синтезу таких даних на тактичному рівні, висока щільність технічних криміналістичних артефактів може призвести до інформаційного шуму й завадити атрибуції на операційному та стратегічному рівнях. Таким чином, по мірі того, як інформація переходить від технічного до оперативного й стратегічного рівнів, інтерпретація результатів аналітики дозволяє досягти більш

концентрованих, лаконічних та виважених висновків. Разом з тим, невизначеність атрибутивних тверджень, швидше за все, зростатиме, коли аналіз переходить від технічного до політичного. Технічні атрибути можуть бути вузькоспеціалізованими та конкретними. Конкуруючі операційні гіпотези можуть грунтуватись на трудомісткій спеціалізованій криміналістичній експертизі, але не повністю підтверджуватись іншими наявними технічними та нетехнічними фактологічними даними. На стратегічному рівні висновки ще більше віддаляються від артефактів, і можуть містити певну кількість припущень та оціночних суджень.

Кінцевою метою атрибуції в *Q* моделі є визначення організації чи уряду, а не окремих осіб. Але за рахунок маркування, уніфікації та геотегів окремі індикатори можуть бути потужними доказовими зв'язками між артефактами та організаціями.

Розглянуті Діамантова модель та *Q* модель застосовуються тільки для аналізу кібератак (для їх формалізації) з метою надання відповіді на питання хто, навіщо і яким чином реалізував кібератаку, надають індикатори компрометації кібератак для подальшої кримінально-технічної експертизи, політично та економічно значимих висновків, дипломатичних заяв тощо. Проте якісна інтерпретація всієї інформації про кібератаки не може здійснюватись без врахування динаміки їх протікання, враховувати етапи проведення кібератак.

Моделлю, яку зазвичай використовують для виокремлення етапів проведення кібератак, є запропонована корпорацією Lockheed Martin, як частина моделі Intelligence Driven Defense, модель **Cyber Kill-Chain** [8]. Ця модель визначає типовий порядок дій зловмисника для досягнення поставлених цілей. Так, для досягнення успіху зловмисник повинен пройти усі вісім етапів (див. рис. 3).

Рисунок 3 – Модель Cyber Kill-Chain

Дамо пояснення кожного етапу:

1. Розвідка. Цей етап може бути визначений як фаза вибору мети, виявлення особливостей організації, специфічних вимог в даній галузі, вибір технологій, вивчення активності компанії в соцмережах або через розсилки. По суті, зловмисник намагається знайти точки входу в систему організації, отримати відповіді на питання: Які методи атаки будуть працювати?, Де, що або хто є найслабшим елементом захисту?, Як вдасться діяти непомітно та результативно?.

2. Озброєння. Підбір інструментарію, створення експлойтів, оснащення шкідливим вмістом файлу (наприклад, PDF або MS Office) або іншого контенту, який повинен бути прочитаний/відкритий жертвою.

3. Доставка. Донесення шкідливого контенту до жертви, використовуючи для цього e-mail, web-сайти або USB-флешки.

4. Зараження. Запуск шкідливого коду, використовуючи наявні на цільовому комп’ютері уразливості, з подальшим його зараженням.

5. Інсталяція. Відкриття віддаленого доступу для непомітного управління і поновлення шкідливого коду, додавання функціональних модулів.

6. Отримання управління. Отримання оновлень з новим функціоналом ззовні, а також управляючих команд для досягнення поставлених цілей.

7. Виконання дій. Збір і крадіжка даних, шифрування файлів, перехоплення управління, підміна даних та інші завдання, які можуть стояти перед порушником.

8. Знищення слідів. Після успішно виконаної атаки, зловмиснику необхідно знищити сліди своєї активності.

В класичній роботі [8] представлено сім етапів. Восьмий етап “знищення слідів” пропонується більшістю спеціалістів в сфері кібербезпеки як логічний й за замовчуванням застосовується як доповнення до класичної моделі. Зрозуміло, що зловмисник не обов’язково повинен дотримуватися проходження усіх наведених кроків, але ефективність його діяльності при цьому може знизитись. Доречно припустити, що чим раніше системи захисту виявлять спрямовані зловмисні дії, тим більш ефективно працює вся система захисту. Блокування зловмисника на будь-якому етапі розриває весь ланцюжок атаки. Приклад застосування моделі Cyber Kill-Chain для побудови системи кібербезпеки наведено в [9]. В статті пропонується впровадження засобів захисту (міжмережеві екрани, системи виявлення вторгнень, антивірусне програмне забезпечення, тощо) від кібератак відносно кожного етапу моделі. Наведені засоби захисту класифікуються на засоби виявлення, нейтралізації, розірвання з’єднань, зниження втрат та введення в оману зловмисників з урахуванням особливостей атаки на кожному етапі. Але [8] - [9] не відповідає на питання, що робити, коли атака виявилася успішною, також не враховує підготовчий етап кібератаки, тобто у моделі не приділяється достатня увага попередженню вторгнень.

В той же час в [10] аналітиками компанії Gartner було запропоновано архітектуру **Адаптивної системи безпеки** для захисту від просунутих атак. Представлена архітектура зміщує точку зору на захист від «реакції на інцидент» до «безперервного контролю». Вона складається з чотирьох категорій компетенцій високого рівня та з 12 категорій можливостей (див. рис. 4). Названі компоненти архітектури повинні працювати інтелектуально разом як інтегрована, адаптивна система, яка безпосередньо втілює повноцінний процес захисту від сучасних загроз. Постійний моніторинг та аналітика є основою архітектури адаптивного захисту.

Рисунок 4 – Адаптивна модель безпеки з компетенціями та можливостями

Згідно з [10] архітектура адаптивної системи безпеки має наступні компетенції захисту:

1. Можливість “**Запобігання**” описує набір політик, продуктів та процесів, які застосовуються для запобігання успішної атаки. Основна мета цієї категорії полягає в тому, щоб попередньо зменшити вразливість системи, виявити можливі техніки, технології та процедури реалізації кібератак, перш ніж вони розпочнуться.

2. Можливість "**Виявлення**" призначена для пошуку атак, які «уникнули» запобігання. Основною метою цієї категорії є зменшення часу існування (присутності) загроз в мережі та, таким чином, зниження потенційного збитку, який вони можуть заподіяти. Можливості детектування мають вважатись критичними, оскільки до цього спонукає ризик-орієнтований підхід: необхідно відноситись до критичних даних так, нібито вони вже скомпрометовані.

3. Можливість "**Ретроспективне дослідження**" – знання та засоби, необхідні для використання даних, виявлених під час детектування (внутрішніми або зовнішніми акторами), з метою проведення криміналістичного аналізу накопичених раніше даних та аналізу основних причин кіберінциденту, а також напрацювання нових запобіжних заходів, щоб уникнути майбутніх кіберінцидентів.

4. Можливість "**Прогнозування**" дозволяє організації вивчати накопичені дані у кореляції з відомостями, отриманими ззовні (надані організаціями, що здійснюють розвідку кіберзагроз, вразливості, розкриті «білими хакерами» в результаті пентесту, інциденти та атаки, що відбулись в сторонніх організаціях зі схожими елементами захисту або споріднені за родом діяльності, афілійовані або які є постачальниками довірених послуг), щоб активно передбачати нові типи атак, а також активно наповнювати системи евристичного аналізу, що використовують штучний інтелект як основу для самонавчання.

Автори наголошують на системності методологічного підходу, який реалізується при "безперервному контролі": при впровадженні адаптивної моделі необхідно розробити та усвідомити політики, розуміти контекст інформації, об'єднувати відомості і дані з різних джерел, проводити розвідку кіберзагроз, розуміти вразливості своїх систем та використовувати підтримку постачальників платформ захисту [10].

Окрім наведених чотирьох компетенцій захисту автори виділяють дванадцять категорій можливостей: системи укріплення та ізоляції, переадресація нападників, запобігання інцидентам, виявлення інцидентів, підтвердження та визначення пріоритетності ризику, стримування інцидентів, розслідування та судово-технічна експертиза, зміна моделі, відновлення та внесення змін, базові системи, передбачення атак, проактивний аналіз впливу. Кінцевою метою є системна інтеграція вказаних можливостей для побудови захисту, який буде більш адаптивним та інтелектуальним в цілому. При цьому адаптивна архітектура захисту продовжуватиме функціонувати упродовж всього життєвого циклу нападу: до, під час та після атаки.

Отже, ґрунтуючись на потребах у даних для аналізу кібератак, враховуючи етапи проведення кібератак та беручи за основу архітектуру «Адаптивної системи безпеки» можливо визначити основні **функції забезпечення кіберзахисту до, під час та після проведення кібератак:**

До: оцінити свою інформаційно-телекомунікаційну систему та систему кіберзахисту; дізнатися про противника й його методи (соціальна та технічна складова), виявити можливі техніки, тактики та процедури нападу.

Під час: ідентифікувати інциденти, блокувати поширення кібератаки, зафіксувати слідову картину.

Після: локалізувати атаку, оцінити нанесену шкоду, усунути вразливості, відновити систему.

Дамо деталізоване пояснення виділеним функціям.

До атаки. Для результативної протидії зловмисникам є потреба в адекватній системі кіберзахисту, яка не лише аналізує поточну ситуацію, а й здійснює ретроспективний аналіз та прогнозування можливих атак. На практиці часто виникає ситуація, коли організація протистоїть зловмисникам, які знають про її інфраструктуру більше, ніж фахівці, що її захищають. Спеціалістам із інформаційної безпеки необхідно виявляти вразливі місця інфраструктури, враховуючи попередні атаки. Щоб правильно налаштувати засоби захисту, їм необхідно добре розбиратися в тому, що вони намагаються захистити та від чого. Тобто потрібно знати структуру своєї мережі, її недоліки та можливі атаки на неї. Інколи

організації намагаються здійснювати окремі заходи із арсеналу розвідки або контррозвідки, що отримали назву "конкурентна розвідка". Але такий підхід не завжди раціональний та ефективний через специфіку організації і проведення розвідувальних заходів, що потребують не лише спеціальних знань, програмного забезпечення, відповідного досвіду, а й спеціальних повноважень, що забезпечують законність подібних заходів, вказаних відповідно у Законах України "Про розвідувальні органи", "Про контрозвідувальну діяльність", "Про оперативно-розшукову діяльність" та Кримінальному процесуальному кодексі України. Отже з позиції спеціаліста у сфері кіберзахисту, який дотримується законодавства, намагання дізнатися про противника та його методи без провадження повноцінної розвідувальної, контррозвідувальної або оперативно-розшукової діяльності може виявитись неефективним, а із застосуванням таких методів – незаконним.

Разом з тим, зосередження зусиль на оцінці власної інформаційно-телекомунікаційної системи замість постійного стеження за противником, на нашу думку, виглядає більш раціональним. Як з юридичної, так і практичної точок зору, отримання (набуття) нових знань про реальні або потенційні загрози і вразливості можливо і доцільно здійснювати за рахунок актуальних знань довідкового характеру, які формуються за рахунок вже виявлених атак на інші інфраструктури, в інших галузях, інших країнах тощо. Типовими джерелами таких знань, наприклад, є збір та аналіз відкритих даних, а також відомостей, які набули поширення без відома власника (розпорядника) в результаті небажаних дій третіх осіб, недбалості самого власника (розпорядника) чи афілійованих з ним осіб, або внаслідок дії непереборної сили.

Безумовно більш якісним джерелом нових знань про реальні або потенційні загрози і вразливості є дані організацій, що здійснюють професійну розвідку кіберзагроз. Рішення, які побудовані такими компаніями, як правило, базуються на телеметричній інформації, яка зібрана з багатьох джерел і видів телекомунікаційних пристроїв, попередньо опрацьована та підготовлена до впровадження в захисні системи.

Крім цього, продовжують набувати популярності різні проекти типу Bug Bounty, які дозволяють отримати упереджувальну інформацію про якість захисту конкретного підприємства, яке заздалегідь погодилось щодо тестування на проникнення (пентест). Вразливості, розкриті "білими хакерами" в результаті пентесту, включаючи й так звані елементи соціального інжинірингу, дають змогу виявити можливі техніки, тактики та процедури потенційної кібератаки, а відповідно підготуватись та вжити заходів пом'якшення наслідків, якщо уникнути атаки все ж таки не вдасться (резервування ресурсів, критичних даних, логування подій критично важливих систем тощо).

Під час атаки. Сучасні атаки розподілені в часі та просторі, але традиційні засоби захисту можуть виявити атаку тільки в один момент часу та можуть детектуватись лише на мережевому пристрої на основі сигнатурного методу. Сьогодні потрібна інфраструктура кіберзахисту, яка збирає і аналізує дані зі всієї мережі та кінцевих пристроїв, а також дозволяє обмінюватись даними з глобальними системами моніторингу. Це дозволить виявляти кібератаки на ранніх стадіях, зокрема діяльність з прихованого зондування мереж, фішингові розсилки, початок застосування заздалегідь створеної хакерами кримінальної інфраструктури тощо. Після ідентифікації інциденту як кібератаки, головним завданням кіберзахисту є локалізація атакованої частини мережі або пристрою та блокування поширення атаки в часі та просторі. В умовах кризової ситуації, система кіберзахисту повинна мати ефективні можливості оперування журналами подій, кореляції даних з різних джерел у об'єктно-орієнтованому графічному інтерфейсі, спрощеному для сприйняття людиною, масового автоматизованого застосування правил та політик кіберзахисту, динамічного керування сегментами мереж та користувачами, їх оповіщення тощо. Але одним із найважливіших завдань, яким часто нехтують, є, на нашу думку, забезпечення безперервної спостережності, що не лише створює доказову базу на випадок юридичних суперечок, але й фіксує слідову картину кіберінциденту для подальшої "роботи над помилками", а також дозволяє спрогнозувати розвиток подальших подій. .

Після атаки. Завершення активної фази кібератаки супроводжується настанням бажаних для атакуючого наслідків або різкою зміною тактики, яка викликана ефективними заходами захисту. Швидкість реагування на етапі завершення або тимчасового припинення кібератаки відіграє ключову роль у розвитку подальших подій і залежить від плану «Б» кожної зі сторін. Проте значну роль відіграє й налагоджена взаємодія з іншими суб'єктами кібербезпеки, особливо силовими підрозділами, які уповноважені законом на проведення активних заходів протидії не лише в рамках периметру захисту та повноважень атакованого об'єкту, але й контратакувальних заходів, спрямованих на нейтралізацію атакуючої сторони в цілому, в тому числі на «її території». Отримання допомоги, консультацій з боку кіберполіції, а у випадку просунутих атак типу APT – і з боку підрозділів кіберконтррозвідки (кібероборони), а також завдяки власній інфраструктурі, здатній безперервно збирати й аналізувати дані, команди реагування на кіберінциденти повинні мати змогу швидко визначати вразливості, що призвели до несанкціонованого втручання, знаходити первинну точку та час компрометації системи, усувати виявлені вразливості та відновлювати пошкоджену інфраструктуру.

Таким чином, за спеціалізацією діяльності з кіберзахисту структурно вимальовується потреба у підрозділах:

– розвідки кіберзагроз (ПРКЗ), що у повсякденній діяльності зосереджені на отриманні (набутті) нових знань про реальні або потенційні загрози і вразливості;

– моніторингу та управління інцидентами безпеки (ПМУІБ), які у повсякденній діяльності концентруються на виявленні інцидентів, оцінці поточного стану кіберзахисту та кореляції телеметричних даних з іншими потоками даних;

– команди реагування на кіберінциденти (КРКІ), які в режимі постійної готовності очікують детектування кібератаки, та, за умови настання такої ситуації, мобілізують сили і засоби інших підрозділів кіберзахисту, координують свою діяльність із зовнішніми структурами кіберконтррозвідки, кібероборони, кіберрозвідки.

Слід зазначити, що розвідку кіберзагроз, попри зовнішню схожість окремих засобів і методів, автори пропонують не ототожнювати зі спеціальним видом діяльності у розумінні Закону України "Про розвідувальні органи України". За текстом даної роботи пропонується розуміти зазначений термін як ініціативну, неоголошену заздалегідь діяльність з отримання (набуття) нових знань про реальні або потенційні кіберзагрози і вразливості, здобутих в результаті збору та аналізу відкритих даних, а також відомостей, які набули поширення без відома власника (розпорядника) в результаті небажаних дій третіх осіб, недбалості самого власника (розпорядника) чи афілійованих з ним осіб, або внаслідок дії непереборної сили.

Також, адаптивна модель інформаційної безпеки **вимагає** від сучасних технологій захисту, забезпечення спостережності мережі, орієнтацію на загрози і базування на платформі. Розкриємо ці вимоги.

Спостережність: адміністратори мереж, серверів, а також фахівці підрозділу кіберзахисту повинні відслідковувати все, що відбувається в мережі, на її інформаційних ресурсах, в системах віртуалізації, кінцевих пристроях. Це вимагає поєднання ширини і глибини. Аспект ширини відповідає за можливість збирати дані по усіх напрямках потенційних атак, що охоплює мережу, кінцеві пристрої, поштові та веб-шлюзи, мобільні пристрої, віртуальні і хмарні середовища. Аспект глибини дає можливість співвідносити ці відомості і застосовувати їх, щоб вивчити контекст проблеми, знайти краще рішення і виконати дії як вручну, так і автоматично.

Орієнтація на загрозу: сучасні мережі працюють всюди, де знаходяться співробітники і дані. Незважаючи на значні зусилля, фахівці з кіберзахисту не завжди встигають за зловмисниками, які атакують з нових напрямків. Для скорочення радіуса атаки необхідні спеціальні політики і засоби контролю, однак загрози проникають в мережу. Тому технології захисту повинні бути націлені на виявлення, аналіз і усунення загроз. Орієнтація на загрози означає думати як зловмисник, спиратися на спостережність мережі і контекст для адаптації

до змін середовища і знаходити спосіб захисту від загрози. Нове шкідливе програмне забезпечення і атаки нульового дня вимагають постійного вдосконалення захисту. З цією метою необхідний безперервний збір даних хмарної аналітики, які передаються в усі системи безпеки для підвищення їх ефективності.

Базування на платформі: кібербезпека не обмежується мережею і вимагає інтегрованої системи гнучких і відкритих платформ, які охоплюють мережу, пристрої та хмари. Ці платформи повинні бути розширюваними, масштабованими і централізованими, щоб забезпечити уніфіковані політики і засоби управління. Тобто, вони повинні відповідати масштабу атак. Для цього необхідно перейти від пристроїв точкового захисту до сучасної платформи сервісів та додатків, що масштабуються і легко розгортаються. Підхід на базі платформи не тільки підсилює систему кіберзахисту, усуваючи вразливості і недоліки, але також дозволяє швидше виявити загрозу і визначити захисні дії.

Ґрунтуючись на особливостях досліджених моделей, на основі різних потреб до кіберзахисту до, підчас та після атаки, а також на визначених функціях пропонується організаційна модель ситуаційного центру кіберзахисту (див. рис. 5).

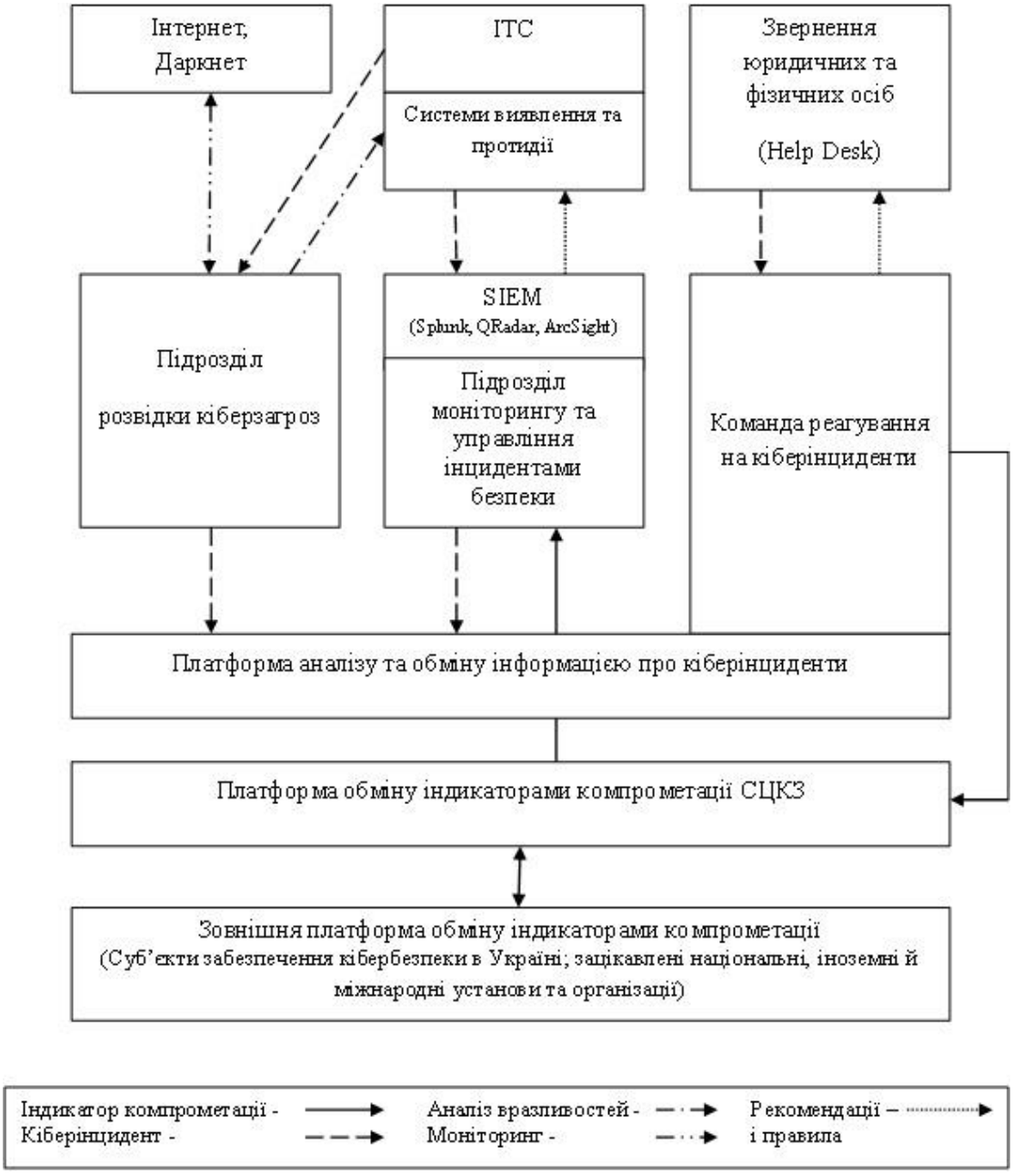

Рисунок 5 – Організаційна модель ситуаційного центру кіберзахисту

Отже, можна стверджувати, що основною діяльністю підрозділу розвідки кіберзагроз в рамках СЦКЗ буде регулярний і систематичний збір інформації про кіберзагрози та кібервразливості з різних джерел, а також її подальший аналіз для розуміння поточних і потенційних кібератак, що можуть загрожувати організації, покращення і збагачення бази знань про кіберзагрози й її поширення між суб'єктами кіберзахисту. В загальному випадку можна виділити два рівні проведення розвідки кіберзагроз – стратегічний і тактичний (або "технічний") [11]. Вони сильно відрізняються і за результатами, і за способами використання цих результатів.

Під час стратегічної розвідки мають добуватися аналітичні дані про тенденції загроз в світі з подальшою метою вироблення стратегії розвитку систем забезпечення інформаційної безпеки. Вихідними даними цього типу розвідки є публікації та різні звітні документи. Основними користувачами є фахівці в сфері кібербезпеки. Інформація доставляється до користувачів на протязі днів-місяців. Ця інформація є актуальною на протязі року і більше. У разі недостатності даних, можливе висунення та формулювання гіпотез, але вони повинні бути обґрунтованими та періодично перевірятись. Основна мета – планування та прийняття рішень. Тактична ж розвідка має надавати дані про атакуючих (інструменти, тактики, техніки і процедури, які використовують порушники), дані про індикатори компрометації, про поточні та прогнозовані атаки, одержані шляхом відстеження нових векторів загроз, способів компрометації інформаційних процесів та ін. Основними вихідними даними даної розвідки є набори правил, параметри налаштування. Ця інформація має сприйматися машиною або людиною спільно з машиною. Доставка до користувача також має відбуватися за секунди-хвилини. Період корисності інформації, дуже короткий, до появи нової вразливості або нового методу експлуатації. При цьому введені правила зазвичай залишаються в системах захисту. Припущення – неможливі, оскільки машини не розуміють нечітких інструкцій. Основна мета – виявлення та розставлення пріоритетів загроз для більш швидкого реагування на них.

ПРКЗ також має відповідати за проведення перевірки на вразливість своїх систем та мереж (Penetration testing) та проактивного пошуку й виявлення загроз, які не виявляються традиційними методами захисту (Threat Hunting). Підсумовуючі, в ПРКЗ можна виділити такі основні функції: розвідка та збір даних про вразливості і загрози, аналітика, обмін даними, оперативне оповіщення.

В свою чергу, підрозділ моніторингу та управління інцидентами безпеки являє собою інфраструктуру, основою якої є команда інформаційної безпеки, що відповідає за моніторинг та аналіз стану безпеки організації на постійній основі. Метою ПМУІБ має бути виявлення, аналіз та реагування на інциденти, пов'язані з кібербезпекою, використовуючи комбінацію технологічних рішень. Як правило, в команді ПМУІБ можуть працювати аналітики безпеки та інженери, а також менеджери, які здійснюють нагляд за кібербезпекою. Співробітники ПМУІБ повинні тісно співпрацюють з командами реагування на кіберінциденти, щоб забезпечити швидке вирішення питань безпеки. ПМУІБ проводять моніторинг та аналіз активності в мережах, серверах, кінцевих точках, базах даних, програмах, веб-сайтах та інших системах, шукаючи аномальну діяльність, яка може свідчити про інцидент безпеки. Цей підрозділ відповідає за те, щоб потенційні загрози були правильно ідентифіковані, проаналізовані, виявлені, розслідувані та повідомлені. Належне функціонування підрозділу залежить від використання SIEM системи. З її допомогою проводять моніторинг та аналіз інформації яка надходить з об'єктів критичної інфраструктури. Вона проводить збір, кореляцію та аналіз подій, відповідає за моніторинг та контроль інформаційної безпеки, управління файлам логіювання, пошук та оцінку вразливостей [2].

Команда реагування на кіберінциденти – група експертів в області кібербезпеки, основним обов'язком якої є реагування на інциденти комп'ютерної та кібербезпеки. Ця команда також може надавати необхідні сервіси для обробки інцидентів та підтримки своїх клієнтів у процесі відновлення після виявлення вразливостей в системах безпеки. Більшість КРКІ також надають профілактичні та освітні послуги для своїх клієнтів. На основі

Платформи аналізу та обміну інформацією про кіберінциденти відбувається аналіз отриманих кіберінцидентів та створюються рекомендації щодо усунення вразливостей в програмному забезпеченні і обладнанні, інформування користувачів про поширення шкідливого програмного забезпечення, формування індикатори компрометації систем [12], [13]. В цілому в КРКІ виділяють групи функцій реагування, профілактики, опрацювання артефактів, управління якістю систем безпеки.

Загальним компонентом, який може об'єднувати центри кіберзахисту суб'єктів забезпечення кібербезпеки в Україні, а також зацікавлених національних, іноземних й міжнародних установ та організацій є Зовнішня платформа обміну індикаторами компрометації. Вона призначена для створення простого і зручного формату опису кіберінцидентів та обміну ними між зазначеними організаціями з метою вдосконалення контрзаходів, що використовуються для протидії кібератакам, їх виявлення та запобігання.

Ґрунтуючись на представленій організаційній моделі сучасного центру кіберзахисту (СЦКЗ) й на виділених функціях його складових, представимо функціональну модель цього центру в нотаціях IDEF [14] рівня А-0 (див. рис. 6).

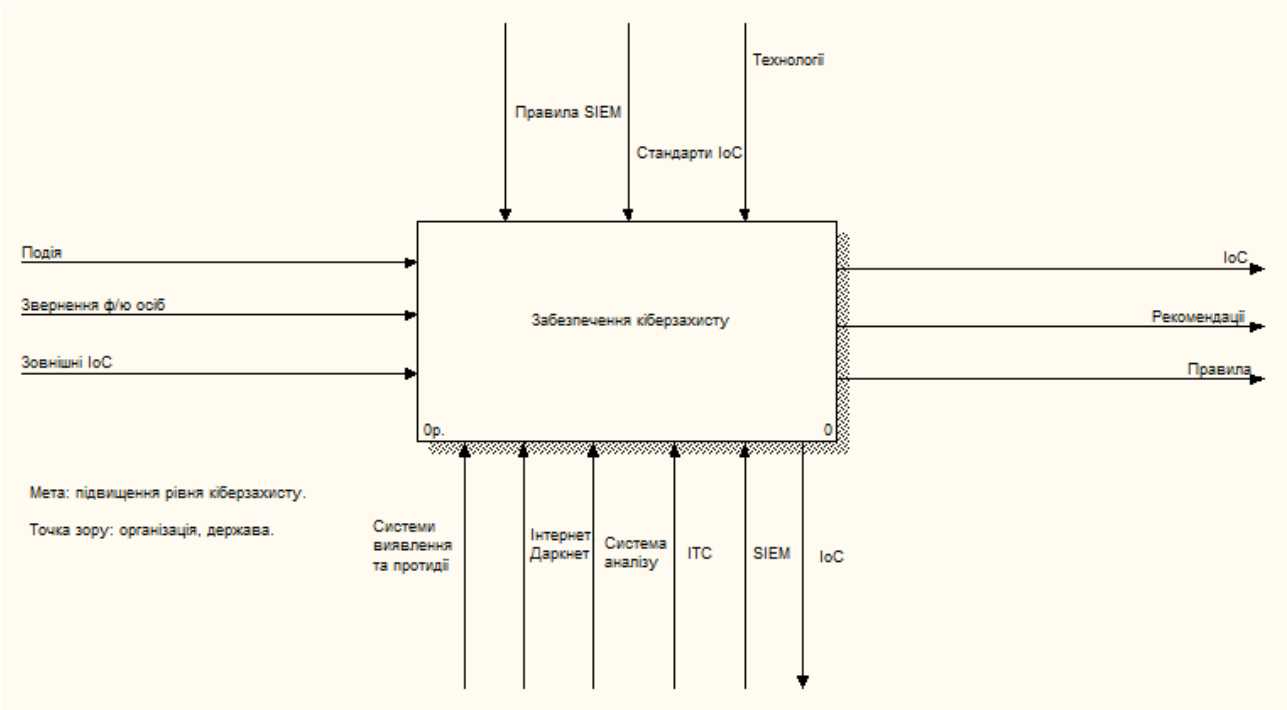

Рисунок 6 – Функціональна модель ситуаційного центру кіберзахисту в нотації IDEF0

Основною функцією СЦКЗ є забезпечення кіберзахисту держави, організації, тощо. Метою ж функціонування цього центру є підвищення рівня кіберзахисту. Вхідними даними, що необхідні для виконання зазначеної функції є певна подія, що відбувається в ІТС держави або організації; звернення фізичних або юридичних осіб щодо підозри або виявлення кібератаки; індикатори компрометації (IoC), що надходять з інших платформ обміну індикаторами. Для забезпечення виконання зазначеної функції на основі вхідних даних використовуються певні ресурси, а саме: системи виявлення та протидії, які функціонують в ІТС держави (організації), сама ІТС, Інтернет та Даркнет як неіндексована частина Інтернету, системи аналізу, що використовуються для аналізу добутих та виявлених кіберінцидентів, SIEM системи для пошуку кореляції між різними подіями в мережі з метою виявлення кібератак. Індикатори компрометації слугують тим ресурсом, що надаються іншим споживачам. В той же час СЦКЗ функціонує в умовах обмежень, які являють собою налаштовані правила SIEM, стандарти опису IoC та технологій, що використовуються для забезпечення кіберзахисту. Результатом функціонування СЦКЗ будуть правила конфігурації,

що можна застосувати до систем виявлення та протидії кібератакам, рекомендації щодо протидії кібератакам та усунення їх наслідків, а також індикатори компрометації, які формуються в наслідок оброблення кіберінцидентів.

З метою деталізації функціональної моделі виконаємо декомпозицію рівня А-0 до рівня А0 (див. рис. 7).

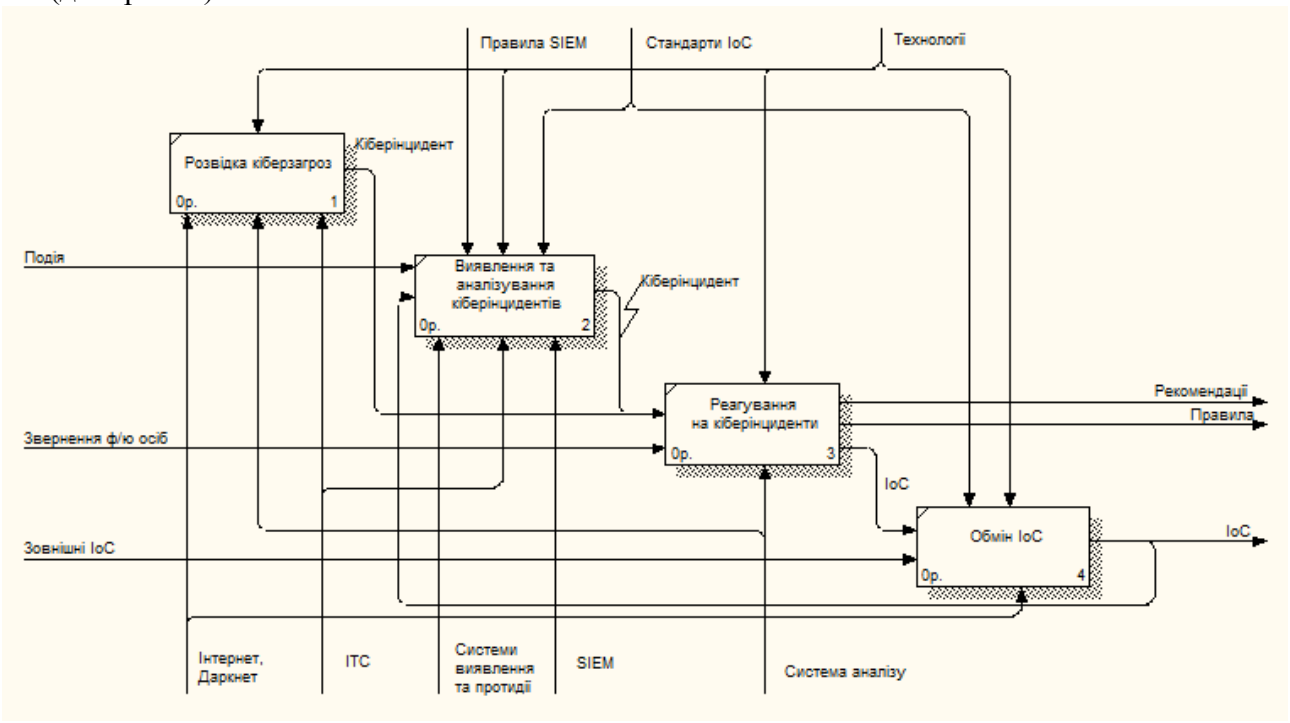

Рисунок 7 – Декомпозиція функціональної моделі ситуаційного центру кіберзахисту в нотаціях IDEF0

На рівні А0 функція забезпечення кіберзахисту буде мати чотири складові функції – розвідка кіберзагроз, виявлення та аналізування кіберінцидентів, реагування на кіберінциденти та обмін IoC. З рисунку 7 видно що є вхідними та вихідними даними зазначених функцій та які ресурси та обмеження використовуються. При цьому слід зазначити, що вихідними даними функцій розвідки кіберзагроз й виявлення та аналізування кіберінцидентів є сам кіберінцидент, який становиться вхідними даними для функції реагування на кіберінциденти. Взагалі, представлена функціональна модель ситуаційного центру кіберзахисту в нотаціях IDEF рівня А0 (див. рис. 7) уточнює організаційну модель СЦКЗ (див. рис. 5) й може бути використана для функціонального аналізу СЦКЗ з метою декомпозиції й формування організаційної структури кожного підрозділу й розроблення функціональних обов'язків кожного співробітника.

Висновки. Сучасні цілеспрямовані атаки, що здійснювалися останнім часом, показали не спроможність стандартних засобів й методів захисту протистояти їм. Це зумовлено тим, що ці засоби напрямлені лише на виявлення та блокування атак в точці входу в систему. Тому в статті вирішувалася актуальна задача розроблення нової моделі центру кіберзахисту, в якій враховується весь період атаки.

Аналіз публікацій показав необхідність врахування всього періоду атаки: до, під час, після. Але відсутність функціональної моделі ситуаційного центру кіберзахисту, що б спиралася на зазначені етапи спонукала до аналізу найбільш вагомих формалізованих моделей аналізу кібератак, реалізації кібератак та моделі, що враховують весь період атаки. Так серед формалізованих моделей аналізу кібератак було проаналізовано Діамантову модель (Diamond Model) та Q Модель (Q Model). Діамантова модель встановлює основний атомний елемент будь-якої діяльності вторгнення, події, що складається з чотирьох основних функцій: зловмисника, інфраструктури, спроможності та жертви, які утворюють умовний

“діамант”. При виявлені події автоматизовано або за допомогою аналітиків заповнюються вершини моделі. Вершини пов'язані ребрами й виділяють природні зв'язки між функціями. Проходячи по ребрах та вершинах, аналітики виявляють більше інформації про операції зловмисника та виявляють нові спроможності, інфраструктуру та жертв. Q Модель дозволяє визначити атрибути кібератаки для встановлення чи є кіберінцидент кіберзлочином. Тактично модель допомагає аналітикам вирішувати весь спектр відповідних питань, допомагає критично мислити та провести розслідування. Практично модель допомагає інтегрувати як технічну, так і нетехнічну інформацію в конкуруючі гіпотези. Розглянуті Діамантова модель та Q Модель застосовуються тільки для аналізу кібератак, для їх формалізації з метою надання відповіді на питання хто, навіщо і яким чином реалізував кібератаку, надають індикатори компрометації кібератак для подальшої кримінально-технічної експертизи, але вони не відображають етапів проведення кібератак.

Такою моделлю, яка враховує етапи проведення кібератак, є модель Cyber Kill-Chain. Ця модель визначає порядок дій зловмисника для досягнення поставлених цілей й містить в собі 8 етапів: розвідка, озброєння, доставка, зараження, інсталяція, отримання управління, виконання дій, знищення слідів. Але модель Cyber Kill-Chain не відповідає на питання, що робити, коли атака виявилася успішною, також не приділяє уваги попередженню вторгнень.

В той же час архітектура Адаптивної системи безпеки для захисту від просунутих атак зміщує точку зору на захист від “реакції на інцидент” до “безперервного контролю”. Вона складається з чотирьох категорій компетенцій високого рівня (запобігання, виявлення, ретроспектива та прогнозування) та з 12 категорій можливостей (системи укріплення та ізоляції, переадресація нападників, запобігання інцидентам, виявлення інцидентів, підтвердження та визначення пріоритетності ризику, стримування інцидентів, розслідування та судово-технічна експертиза, зміна моделі, відновлення та внесення змін, базові системи, передбачення атак, проактивний аналіз впливу). Адаптивна архітектура захисту працює протягом всього життєвого циклу нападу: до, під час та після атаки.

Ґрунтуючись на потребах в даних для аналізу кібератак, враховуючи етапи проведення кібератак та беручи за основу архітектуру Адаптивної системи безпеки було визначено функції забезпечення кібербезпеки до, під час та після проведення кібератак. Також було запропоновано операційно реалізувати ці етапи шляхом побудови Підрозділу розвідки кіберзагроз, Підрозділу моніторингу та управління інцидентами безпеки та Команди реагування на кіберінциденти. В статті визначено основні функції та вимоги до цих складових ситуаційного центру кіберзахисту. Показано їх функціональну залежність.

На основі вимог нотацій IDEF було представлено функціональну модель рівнів A-0 та A0. Визначено головну функцію ситуаційного центру кіберзахисту, вхідні та вихідні дані, а також ресурси, що використовуються при функціонуванні центру, та обмеження, в умовах яких центр діє. Представлені нотації графічно відображають результати функціонального аналізу ситуаційного центру кіберзахисту й дають змогу сформувати вимоги до складових цього центру, а в подальшій декомпозиції сформувати організаційну структуру кожного підрозділу й розробити функціональні обов’язки кожного співробітника.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Річний звіт з інформаційної безпеки. Cisco 2018. [Електронний ресурс]. Доступно: www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf.

[2] C. Zimmerman. *Ten Strategies of a World-Class Cybersecurity Operations Center*. The MITRE Corporation, 2014.

[3] J. Muniz, G. McIntyre, and N. AlFardan. *Security Operations Center*. Cisco Press, 2016.

[4] M. Sanders, “How to Get the Most Value out of Your MSSP and Security Operations” [Online]. Available: https://securityintelligence.com/how-to-get-the-most-value-out-of-your-mssp-and-security-operations.

[5] Adaptive Cybersecurity Model for the Protection of Industrial Objects [Online]. Available: https://www.kaspersky.ru/blog/ics-asa/4455.

[6] S. Caltagirone, A. Pendergast, and C. Betz, “Diamond Model of Intrusion Analysis”, Center for Cyber Threat Intelligence and Threat Research, Hanover, MD, Technical Report ADA586960, 05 July 2013.
[7] T. Rid, and B. Buchanan, “Attributing Cyber Attacks”, *The Journal of Strategic Studies*, vol. 38, no. 1-2, pp. 4-37, 2015.
doi: 10.1080/01402390.2014.977382.
[8] E. M. Hutchins, M. J. Clopperty, and R. M. Amin, Ph.D. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation, 2010.
[9] I. Tarnowski, “How to use cyber kill chain model to build cybersecurity?”, *European Journal of Higher Education IT* [Online]. Available: http://www.eunis.org/download/TNC2017/TNC17-IreneuszTarnowski-cybersecurity.pdf.
[10] N. MacDonald, and P. Firstbrook, *Designing an Adaptive Security Architecture for Protection From Advanced Attacks*. Gartner, 2014.
[11] National Institute of Standards and Technology. (Okt. 31, 2016). *NIST SP 800-150. Guide to Cyber Threat Information Sharing*, 2014.
doi: 10.6028/NIST.SP.800-150.
[12] H. Bronk, M. Thorbruegge, and M. Hakkaja. *CSIRT Setting up Guide*, 2006.
[13] Nippon CSIRT Association. CSIRT Starter Kit, 2016.
[14] C. Feldmann. *The Practical Guide to Business Process Reengineering Using IDEF0*. Dorset House Publishing, New York, 1998.

Стаття надішла в редакцію 18 вересня 2018 року.

REFERENCE

[1] Annual report on information security. Cisco 2018. [Online]. Available: www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf.
[2] C. Zimmerman. *Ten Strategies of a World-Class Cybersecurity Operations Center*. The MITRE Corporation, 2014.
[3] J. Muniz, G. McIntyre, and N. AlFardan. *Security Operations Center*. Cisco Press, 2016.
[4] M. Sanders, “How to Get the Most Value out of Your MSSP and Security Operations” [Online]. Available: https://securityintelligence.com/how-to-get-the-most-value-out-of-your-mssp-and-security-operations.
[5] Модель адаптивної кібербезпеки для захисту промислових об’єктів [Електронний ресурс]. Доступно: https://www.kaspersky.ru/blog/ics-asa/4455.
[6] S. Caltagirone, A. Pendergast, and C. Betz, “Diamond Model of Intrusion Analysis”, Center for Cyber Threat Intelligence and Threat Research, Hanover, MD, Technical Report ADA586960, 05 July 2013.
[7] T. Rid, and B. Buchanan, “Attributing Cyber Attacks”, *The Journal of Strategic Studies*, vol. 38, no. 1-2, pp. 4-37, 2015.
doi: 10.1080/01402390.2014.977382.
[8] E. M. Hutchins, M. J. Clopperty, and R. M. Amin, Ph.D. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation, 2010.
[9] I. Tarnowski, “How to use cyber kill chain model to build cybersecurity?”, *European Journal of Higher Education IT* [Online]. Available: http://www.eunis.org/download/TNC2017/TNC17-IreneuszTarnowski-cybersecurity.pdf.
[10] N. MacDonald, and P. Firstbrook, *Designing an Adaptive Security Architecture for Protection From Advanced Attacks*. Gartner, 2014.
[11] National Institute of Standards and Technology. (Okt. 31, 2016). *NIST SP 800-150. Guide to Cyber Threat Information Sharing*, 2014.
doi: 10.6028/NIST.SP.800-150.

[12] H. Bronk, M. Thorbruegge, and M. Hakkaja. *CSIRT Setting up Guide*, 2006.
[13] Nippon CSIRT Association. CSIRT Starter Kit, 2016.
[14] C. Feldmann. *The Practical Guide to Business Process Reengineering Using IDEF0*. Dorset House Publishing, New York, 1998.

АРТЕМ ЖИЛИН,
НИКОЛАЙ ХУДЫНЦЕВ,
МАКСИМ ЛИТВИНОВ

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ СИТУАЦИОННОГО ЦЕНТРА КИБЕРЗАЩИТЫ

В общем случае вопросы построения центров киберзащиты сводятся к построению SOC, основной функцией которого является мониторинг и анализ киберугроз и реагирования на киберинциденты онлайн. В указанном подходе не всегда уделяется внимание этапам предотвращения вторжений и устранения последствий кибератак. Существующие исследования показывают возможность расширения функции SOC, но они не формализованы и не описаны с точки зрения функций, возлагаемых на такой Ситуационный центр киберзащиты (далее - СЦКЗ). Целью данной работы было определено анализ существующих моделей обеспечения кибербезопасности и построение функциональной модели ситуационного центра киберзащиты. Для достижения поставленной цели в статье проводились исследование моделей анализа кибератак с позиции исследователя (Бриллиантовая модель и Q Модель), реализации кибератак с позиции атакующего (Модель Cyber Kill-Chain) и моделей, учитывающих более широкий спектр аналитических подходов (Адаптивная модель безопасности). Основываясь на потребностях в данных для анализа кибератак, учитывая этапы проведения кибератак и основываясь на архитектуре адаптивной системы безопасности определены функции обеспечения киберзащиты до, во время и после кибератак. Результаты анализа выбранных моделей позволили предложить Организационную модель ситуационного центра киберзащиты, определить его составляющие и сформулировать основные функции. Так предлагается реализовать построение СЦКЗ путем создания Подразделения разведки киберугроз, Подразделения мониторинга и управления инцидентами безопасности и Команды реагирования на киберинциденты. В указанной модели показано связи между структурами и потоки информации, которые между ними циркулирует. На основе требований нотаций IDEF представлено функциональную модель. Определены главная функция центра киберзащиты, входные и выходные данные, а также ресурсы, используемые при функционировании центра, и ограничения, в условиях которых центр действует. Представленные нотации графически отображают результаты функционального анализа центра киберзащиты и позволяют сформировать требования к его составляющим, а в дальнейшей декомпозиции - сформировать организационную структуру каждого подразделения и разработать функциональные обязанности каждого сотрудника.

Ключевые слова: Бриллиантовая модель, Q Модель, Cyber Kill-Chain, Адаптивная модель кибербезопасности, ситуационный центр киберзащиты, индикаторы компрометации, киберинцидент, функциональная модель, IDEF.

ARTEM ZHYLIN,
MYKOLA HUDYNCEV,
MAKSYM LITVINOV

FUNCTIONAL MODEL OF CYBERSECURITY SITUATION CENTER

In general, the issue of building cybersecurity centers mainly stands for building a SOC which main function is monitoring and analyzing cybercrime questions and responding to cyber incidents online. The approach, mentioned above, implies insufficient attention to the stages of intrusions` prevention and the elimination of cyber attacks` outcomes. Conducted investigations represent the possibility of SOCs` functions expanding , but they are not formalized and described in terms of functions, which rely on such Cybersecurity Situation Center (hereinafter referred to as the CSSC). The

aim of this work is to analyze the existing cybersecurity models and build a functional model of modern cyberprotection center. The article reviews cyberattacks` analyzing models from the position of a researcher (Diamond Model and Q Model), the implementation of cyberattacks from the position of an attacker (Model Cyber Kill-Chain) and models with a wider range of analytical approaches (Adaptive Safety Model) to achieve this goal. The functions of cyberprotection before, during and after cyberattacks have been determined taking into consideration data needs for cyberattack analysis, understanding of cyberattacks` realization stages and the Adaptive Security System`s architecture. The results of the selected models` analysis allow to suggest a new organizational model of a modern cyberprotection center as well as define it`s components and formulate main functions. The implementation of the CSSC is proposed to be realized through the construction of Cybercrime Intelligence Unit, Monitoring and Incident Security Control Unit and Cyber Incident Response Team. The mentioned model represents logical links between structures and information streams which circulate between them. The presented functional model of A-0 and A0 levels is based on the IDEF notations` requirements. The main cyberprotection center`s function, input and output data as well as the resources used in the process of center functioning , main restrictions under which the modern center operates are determined. The presented notations display the visualisations which demonstrate the results of the cyberprotection center`s functional analysis. They also give an opportunity to determine requirements for the center`s components, form the organizational structure of each unit and establish each employee`s functional responsibilities in subsequent decomposition.

Keywords: Diamond Model, Q Model, Cyber Kill-Chain, Adaptive Cybersecurity Model, Cybersecurity Situation Center, Compromise Indicators, cyber incident, functional model, IDEF.

Артем Вікторович Жилін, кандидат технічних наук, доцент кафедри Захисту державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0002-4959-612X.

E-mail: zhylinartem@gmail.com.

Микола Миколайович Худинцев, кандидат фізико-математичних наук, доцент, перший заступник начальника Державного центру кіберзахисту, Київ, Україна.

ORCID: 0000-0001-9659-2984.

E-mail: dckz_hmm@dsszzi.gov.ua.

Максим Юрійович Літвінов, кандидат юридичних наук, начальник Ситуаційного центру забезпечення кібербезпеки, Київ, Україна.

ORCID: 0000-0001-6093-1366.

E-mail: htcu@ssu.gov.ua.

Артем Викторович Жилин, кандидат технических наук, доцент кафедры Защиты государственных информационных ресурсов, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Николай Николаевич Худынцев, кандидат физико-математических наук, доцент, первый заместитель начальника Государственного центра киберзащиты, Киев, Украина.

Максим Юрьевич Литвинов, кандидат юридических наук, начальник Ситуационного центра обеспечения кибербезопасности, Киев, Украина.

Artem Zhylin, candidate of technical sciences, associate professor of state information resources security academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Mykola Hudyncev, candidate of physical and mathematical sciences, associate professor, first deputy head of State Centre of Cyberdefence, Kyiv, Ukraine.

Maksym Litvinov, candidate of juridical sciences, head of the Cybersecurity Situation Center, Kyiv, Ukraine.