Ящук Валентина Ігорівна
кандидат економічних наук, доцент, доцент кафедри управління інформаційною безпекою,
Львівський державний університет безпеки життєдіяльності, Україна

Методика забезпечення безпеки інформаційних систем та реагування на кіберінциденти кібербезпековими центрами

Анотація. Досліджено методи та підходи до забезпечення безпеки інформаційних систем та ефективного реагування на кіберінциденти із залученням кібербезпекових центрів. Зокрема, увага зосереджена на аналізі сучасного стану кіберзагроз в Україні та впровадженні передових практик у сфері кібербезпеки. Пропонуються практичні рекомендації організаціям та урядовим структурам щодо підвищення рівня захисту від кіберзагроз та підготовки до реагування на кіберінциденти.

Ключові слова: інформаційна безпека, кіберінцидент; кібербезпековий центр.

У зв'язку зі стрімким розвитком технологій та інформаційної сфери сучасне суспільство стикається зі зростаючою загрозою кібератак та кіберзлочинності. Україна не залишається осторонь цього тренду, і впровадження передових практик у сфері кібербезпеки стає надзвичайно важливим завданням для забезпечення стабільності та безпеки національних інформаційних систем. Методика забезпечення безпеки інформаційних систем, реагування на кіберінциденти кібербезпековими центрами та впровадження передових практик у цій сфері є ключовими аспектами дослідження.

Сьогодні Україна стикається із великою кількістю кіберзагроз, такими як кібератаки на державні установи, критичну інфраструктуру та приватний сектор. Найпоширенішими видами атак є фішинг, злам аккаунтів, вимагання викупу (рансомвер), атаки на мережеві системи тощо. Ці кіберінциденти створюють

загрозу для інформаційної безпеки країни та вимагають великих зусиль для їх запобігання та подолання.

Закон України «Про основні засади забезпечення кібербезпеки України» [1], визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

У Постанові Кабінету Міністрів України «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» [2], що визначено засади функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, які здійснюються щодо об’єктів кіберзахисту, визначених частиною другою статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» [1].

У світовій практиці для різних типів центрів реагування на події інформаційної безпеки використовуються абревіатури SOC та CERT. На думку багатьох дослідників [3-6] SOC та CERT виконують однакове завдання – забезпечують будь-яку реакцію на інциденти.

SOC (Security Operations Center) - це центр забезпечення кібербезпеки, який відповідає за моніторинг, виявлення та реагування на кіберзагрози в реальному часі. У складі SOC можуть працювати спеціалісти з безпеки, аналітики, інженери та інші фахівці, які використовують спеціалізовані інструменти та технології для виявлення та вирішення інцидентів безпеки.

Основними завданнями Центру оперативного управління є консолідація подій з багатьох джерел, проведення певної аналітики та оповіщення уповноважених співробітників про інциденти інформаційної безпеки чи інші події. На основі отриманих даних співробітники центру проводять розслідування, вживають заходів, щоб унеможливити повторення події, мінімізують втрати. Поширена помилкова думка, що термін SOC еквівалентний

SIEM (Security Information and Event Management) з невеликими доповненнями у вигляді постійного штату фахівців, які спостерігають за подіями. Безумовно, SIEM-рішення залишається однією з основних складових центру оперативного управління [3,6-7], але SOC — це сукупність технічних та організаційних заходів, спрямованих на виявлення, аналіз та запобігання інцидентам. Він не може вважатися повноцінним, якщо він не має SLA (Service Level Agreement), що передбачає гарантований час реагування на різні події інформаційної безпеки. Зрілість SOC оцінюється з допомогою методики SOMM (Security Operations Maturity Model), яка складається з п’яти основних рівнів (табл.1).

Таблиця 1

Рівні SOMM (Security Operations Maturity Model)

SOMM-рівень	SOC-опис	Деталізація
Рівень 0	Відсутній	Ключові складові SOC (моніторинг, документування SLA) відсутні.
Рівень 1	Початковий	«Реагування по ситуації» (є моніторинг, немає документованих процесів).
Рівень 2	Базовий	Виконуються всі основні нормативні вимоги з урахуванням актуальних вимог бізнесу. Більшість процесів документовано, переглядається по ситуації.
Рівень 3	Належний	Процеси повністю документовані, регулярно актуалізуються з урахуванням найкращих практик.
Рівень 4	Усвідомлений	Проводиться регулярна оцінка ефективності SOC, виробляється процес для досягнення максимальних ключових показників ефективності бізнесу.
Рівень 5	Максимальний (екстремальний)	Максимальна конкретизація процесів, є план подальшого розвитку SOC.

Методика SOMM (Situational Method Engineering) використовується для створення методологій інформаційних систем, а також для визначення та адаптації підходів у конкретних ситуаціях. SOMM включає різні рівні, які дозволяють описати процес розробки методології. Ось кілька типових рівнів SOMM. Рівень метамоделі - найвищий рівень SOMM, де описується загальна структура та концепції методології. Метамодель визначає основні конструктивні елементи, їхні взаємозв'язки та основні принципи розробки методологій. На Рівні моделей концептуалізації визначаються конкретні моделі, які використовуються для представлення потреб, вимог та специфікацій стосовно інформаційних

систем. Ці моделі допомагають уточнити структуру та функціональність системи. На Рівні моделей процесів описуються процеси, які використовуються для розробки та впровадження інформаційних систем на основі визначених моделей концептуалізації. Найнижчим рівнем SOMM є Рівень моделей методології. На цьому рівні конкретизуються кроки, техніки та інструменти, які використовуються під час реалізації процесів розробки інформаційних систем. Кожен з цих рівнів дозволяє уточнити та деталізувати процес створення методології залежно від потреб та умов конкретного проекту чи організації.

При створенні SOC зазвичай уникають суто технічного розуміння завдання, що включає тільки встановлення та налаштування SIEM, а звертають увагу на організаційні моменти: документування найбільш очевидних процесів та формалізації вимог на відповідність будь-яким стандартам (як внутрішнім, так і зовнішнім), складання SLA та інші. Добре налаштовану та підтримувану SIEM-систему (якщо в службі безпеки існують регламенти реагування на інциденти) теоретично можна вважати SOC першого рівня. Однак зараз таких впроваджень, які працюють на повну силу, у нашій країні є порівняно небагато (рис.1).

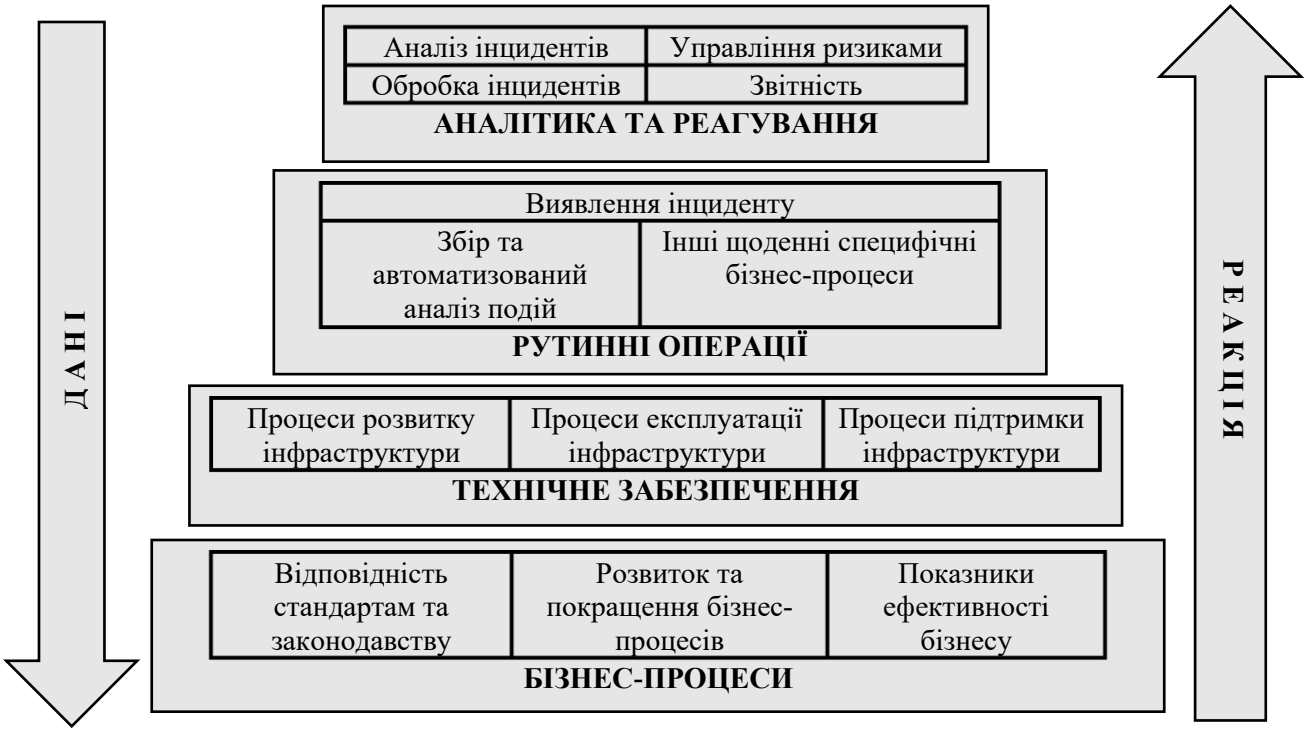

Рис. 1. Основні процеси, необхідні для функціонування повноцінного SOC

Умовами існування успішного SOC можна вважати сукупність наступних систем та нормативних документів: впроваджена та налагоджена система класу SIEM та Help-Desk для організації призначення завдань групі реагування та контролю виконання завдань; розроблені угоди SLA; регламенти реагування на типові інциденти; метрики ефективності. На даний момент в Україні є декілька організацій, які надають SOC як послугу. Слід зазначити, що далеко не всі потенційні клієнти користуються нею через побоювання витоку своїх даних або подій інформаційної безпеки, пракнучи будувати власні центри реагування.

CERT (Computer Emergency Response Team) - це команда, яка відповідає за реагування на кіберінциденти та вирішення комп'ютерних екстрених ситуацій. Їхнє завдання полягає у виявленні, аналізі та вирішенні кібератак, виявленні інформаційних загроз та розробці заходів для їх запобігання. CERT може бути внутрішньою командою в організації або зовнішньою службою, яка надає послуги з реагування на інциденти в інших компаніях або урядових органах.

Іноді Computer Emergency Response набуває значення Комп'ютерної команди безпеки з реагування на інциденти - CSIRT (Computer Security Incident Response Team). Слово «команда» часто замінюється словом «центр». Образно кажучи, CERT/CSIRT — це МНС у цифровому світі, до основних завдань якого входять збирання інформації про події інформаційної безпеки, їх класифікація та нейтралізація. Прикладом таких CERT є Computer Emergency Response Team of Ukraine [9,10]. Команда функціонує у складі Держспецзв'язку та займається питаннями запобігання, виявлення та усунення наслідків кіберінцидентів.

У кожному CERT окреслюється коло відповідальності. Наприклад, обробка лише інцидентів, спрямованих на державні інформаційні системи, або тих подій інформаційної безпеки, які пов'язані із фінансовою сферою. Також різняться й способи отримання даних: прямий зв'язок із громадськістю через електронну пошту або телефон, автоматизований збір інформації з відкритих джерел за допомогою спеціалізованих засобів, запуск «своїх» SOC та підключення до існуючих. З метою вдосконалення процесів нейтралізації інцидентів і виявлених вразливостей, об'єднуються кілька CERT і оброблені

результати аналізу одного центру передаються в CERT, що спеціалізується на даному напрямку. Один із результатів роботи таких центрів — формування рекомендацій щодо мінімізації ризику або регламентів дій у разі виникнення подій інформаційної безпеки, які можуть використовуватися при обробці аналогічних інцидентів у SOC.

Таким чином, часто CERT є «вищим» по відношенню до SOC, але його наявність зовсім не є обов'язковою. З технічної точки зору основою CERT в більшості випадків є SOC, але «кадри вирішують все». Щоб називатися CERT/CSIRT, потрібно мати команду аналітиків, які мають експертні знання в галузі виявлення та нейтралізації подій інформаційної безпеки, що знаходяться у сфері інтересів даного CERT. Це дозволяє вчасно виявляти та нейтралізувати інциденти, складаючи бази даних загроз, характерних для спрямування роботи CERT. Крім цього, фахівці можуть брати участь у процесі ліквідації виявлених центром подій інформаційної безпеки або через надання консультаційної, методичної та іншої підтримки, або через передачу даних у відповідні державні органи, що займаються кібербезпекою. CERT - це, швидше, прерогатива дуже великих спеціалізованих компаній, які бажають підвищити оперативність реагування на власні інциденти інформаційної безпеки і продають аналітику дрібнішим організаціям, або державного центру реагування на загрози, спрямованого на їхню мінімізацію в межах галузі або напряму.

Існують такі міжнародні об'єднання CERT, як FIRST і Trusted Introducer, офіційне включення до яких стало дуже ефективним показником довіри. Створення CERT особливо актуальне для державної галузі або напряму, де шкода від проігнорованої загрози може мати сильний негативний вплив. Виключно для потреб навіть великої компанії подібні роботи економічного сенсу не мають, вимагаючи великих витрат без подальших гарантій про повернення вкладень (показник ROI близький до нуля). Окремим складним завданням стає технічний запуск SOC, що входить до складу CERT. Для представників великого бізнесу вартість створення такого центру може перевищити рівень прибутку від основної діяльності компанії. У цьому випадку краще звернутися за допомогою

до інтегратора і побудувати SOC, який має прийнятну вартість та термін окупності, або віддати його на аутсорсинг, щоб позбавитися витрат на утримання. Експертів теж простіше взяти на аутсорсинг із метою зниження витрат на персонал. У такий спосіб можна вирішити задачу підключення до CERT спеціалізованих організацій, для яких це є основним видом діяльності. За вказаного сценарію доведеться ділитися частиною зібраної вашим SOC інформації з центром CERT, але організація отримає прийнятний рівень безпеки за доступною ціною.

Основна різниця між SOC (Security Operations Center) та CERT (Computer Emergency Response Team) полягає у їхніх функціях, завданнях та методах роботи та наведена в табл. 2.

Таблиця 2

Порівняльна характеристика SOC (Security Operations Center) та CERT (Computer Emergency Response Team)

Критерій	SOC	CERT
Функції	відповідає за постійний моніторинг систем безпеки, виявлення загроз та інцидентів у реальному часі, а також за їхню первинну обробку.	спеціалізується на реагуванні на кіберінциденти, вирішенні кризових ситуацій, аналізі виявлених загроз та розробці стратегій та методів їхнього вирішення.
Область діяльності	зазвичай орієнтований на постійне моніторинг внутрішніх мереж та систем організації або компанії.	може бути внутрішньою чи зовнішньою командою, яка відповідає за реагування на інциденти в різних організаціях або галузях.
Час реакції	реагує на події в реальному часі, намагаючись виявити та припинити загрози якнайшвидше.	може бути активований після виявлення серйозних кіберінцидентів для проведення розслідування та реагування на них.
Аналіз інцидентів	зазвичай використовує автоматизовані системи та методи для виявлення та аналізу загроз.	зазвичай використовує більш ретельний аналіз та дослідження для визначення походження та масштабу кіберінцидентів

Хоча обидва типи організацій мають спільну мету - забезпечення безпеки інформаційних систем, їхні функції та методи роботи відрізняються залежно від специфіки завдань, які вони виконують.

Отже, в процесі дослідження проаналізовано методи та підходи до забезпечення безпеки інформаційних систем та ефективного реагування на кіберінциденти з використанням кібербезпекових центрів. Результати дослідження показали, що сучасний стан кіберзагроз в Україні вимагає негайних заходів для підвищення рівня кібербезпеки.

Важливо враховувати, що ефективний захист від загроз потребує комплексного підходу, який включає в себе не лише захист інформаційних систем, але й швидке та якісне реагування на кіберінциденти. Залучення кібербезпекових центрів є ключовим елементом в цьому процесі, оскільки вони забезпечують постійний моніторинг кіберпростору та оперативну відповідь на потенційні загрози.

Враховуючи викладене вище можна сформувати практичні рекомендації щодо підвищення екфективності інформаційної безпеки, зокрема, розробка та впровадження стратегічних планів кібербезпеки на рівні організацій та урядових структур; посилення співпраці між сектором кібербезпеки та приватним сектором для обміну інформацією та взаємодії у вирішенні кіберзагроз; підвищення кваліфікації фахівців з кібербезпеки через навчання та сертифікацію; перевірка та оновлення захисту інформаційних систем у відповідності з сучасними кіберзагрозами; розширення мережі кібербезпекових центрів та підвищення їхньої ефективності та доступності для всіх зацікавлених сторін. Ці заходи допоможуть покращити рівень захисту від кіберзагроз та забезпечити ефективне реагування на кіберінциденти в Україні.

Список джерел:

1. Про основні засади забезпечення кібербезпеки: Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
2. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова Кабінету Міністрів України від 23.12.2020 №1295 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text.

3. Логойда Я. Дослідження використання SIEM-систем в менеджменті інформаційної безпеки / Я. Логойда, В. Ящук, Н. Фединець // Інформаційна безпека та інформаційні технології: збірник тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 30 листопада 2023 року. Львів, ЛДУ БЖД, 2023, С.111-114.
4. Про Кібербезпеку: Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19.
5. Доктрина інформаційної безпеки України: [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/documents/472017-21374
6. Ориник С. Система управління інцидентами інформаційної безпеки / С. Ориник, В. Ящук, М. Навитка // Інформаційна безпека та інформаційні технології: збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. – Львів: Растр-7, 2022. – С.36-39.
7. Тичина Ю. Модель системи управління інцидентами інформаційної безпеки / Ю. Тичина, В. Ящук, О. Полотай // Інформаційна безпека та інформаційні технології: збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. – Львів: Растр-7, 2022. – С.108-111.
8. Про захист інформації в інформаційно-комунікаційних системах: Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
9. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/3475-15#Text.
10. Computer Emergency Response Team of Ukraine [Електронний ресурс]. Режим доступу: https://cert.gov.ua/