КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.675
УДК 004.056.5

Цирканюк Діана Андріївна
аспірантка кафедри інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-9422-8617
d.tsyrkaniuk.asp@kubg.edu.ua

Соколов Володимир Юрійович
к.т.н., доцент, доцент кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

МЕТОДИКА РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. Розробка і впровадження комплексу заходів з інформаційної безпеки під час війни є важливим завданням для забезпечення національної безпеки та захисту важливих ресурсів та інформації. В статті проаналізовані різні види інцидентів у сфері інформаційної безпеки, способи їх усунення та відновлення. Продемонстровано механіку розслідування інцидентів інформаційної безпеки на етапах моніторингу, індексації, збору інформації, усунення, відновлення та закриття. У публікації запропонований формалізований опис плану обробки інцидентів у формі стейт-машини, що дозволяє систематизувати та автоматизувати процес реагування на інциденти. На прикладах атак, спрямованих на об'єкти критичної інфраструктури, показано використання цього механізму та визначено заходи, спрямовані на покращення системи інформаційної безпеки, що можуть бути застосовані для захисту державних та комерційних установ та організацій. В результаті, запропоновані рекомендації для успішної протидії кібератакам і забезпечення інформаційної безпеки організації чи держави, включають в себе впровадження інструментів моніторингу та координуватися з урядовими та міжнародними командами реагування. Також, важливо регулярно проводити навчання співробітників та розвивати механізми співпраці з партнерами для ефективного захисту від кібератак. Виконання цих заходів сприяє зміцненню кіберзахисту та зниженню можливих збитків. Подальші дослідження можуть охоплювати розробку нових алгоритмів виявлення загроз, вивчення ефективності заходів інформаційної безпеки державних та комерційних установ та організацій, впровадження систем автоматизованої реакції на інциденти, а також дослідження впливу війни на критичну інфраструктуру та міжнародної співпраці в цій галузі, вивчення можливостей міжнародної співпраці та обміну інформацією в галузі інформаційної безпеки під час конфліктів для спільного захисту національних інтересів.

Ключові слова: кібербезпека; інцидент безпеки; захист інформації; гарантія якості; виявлення помилок; криміналістика; усунення несправностей; фрод.

ВСТУП

Останнім часом стрімко зросло використання кіберпростору в національних конфліктах [1]. Практично кожна галузь змушена впроваджувати нові рішення для захисту від крадіжок, злому та знищення даних. Згідно з дослідженням Accenture Cost of Cybercrime Study, 43% всіх кібератак спрямовані на малий бізнес, причому лише 14% компаній можуть ефективно захистити себе [2].

Станом на 2015 рік кіберзлочинність коштувала компаніям усього світу приблизно 3 трлн доларів. Згідно з прогнозами Cybersecurity Ventures, при темпах зростання 15%, витрати на кіберзлочинність досягнуть 10,5 трлн доларів щорічно до 2025 року [3]. Це підкреслює критичну необхідність у посиленні заходів кібербезпеки на всіх рівнях.

Постановка проблеми. У сучасних умовах, коли інформаційна безпека є критично важливою складовою національної безпеки, розслідування інцидентів інформаційної безпеки стикається з численними викликами. Зростання складності кіберзагроз та збільшення кількості атак вимагають не лише швидкого і ефективного реагування, але й превентивних заходів для запобігання подібним інцидентам у майбутньому. Для цього необхідний комплексний підхід, який включає в себе координацію між різними відомствами, впровадження передових технологій моніторингу та аналізу загроз, а також постійне підвищення кваліфікації фахівців у сфері інформаційної безпеки.

Розробка і впровадження комплексу заходів з інформаційної безпеки під час війни є важливим завданням для забезпечення національної безпеки та захисту важливих ресурсів і інформації.

Аналіз останніх досліджень і публікацій. У попередньому дослідженні [4] було розглянуто профіль потенційного зловмисника, а також причини та процес настання інциденту. Однак, для ефективного розслідування інцидентів необхідно чітко розробити механізми реагування на різні типи атак, які постійно еволюціонують. Зокрема, такі типи атак як фішинг [5] – [7], DoS-атаки [8], [9], DDoS-атаки [6] – [9], SQL-ін’єкції [7], програми-вимагачі [10] та інші [11] – [13] вимагають спеціалізованих методів розслідування та реагування. Сучасні дослідження підкреслюють необхідність постійного оновлення методик для забезпечення адекватної відповіді на нові загрози.

МЕТОДИКА ДОСЛІДЖЕННЯ

У даній статті проведено аналіз різних типів кібер-атак, а також методів розслідування та реагування на них. Об'єктом дослідження є інциденти інформаційної безпеки, що сталися на державних та приватних підприємствах. Для класифікації інцидентів була розроблена нова методика, яка пройшла апробацію на реальних прикладах інцидентів у державних організаціях критичної інфраструктури.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Класифікація інцидентів безпеки

Забезпечення ефективної підтримки стало невід’ємною складовою операцій підприємств не лише для запитів безпеки. Делегування заявок на підтримку є ключовим аспектом забезпечення безперебійності роботи та задоволення користувачів. З метою забезпечення більш продуктивного технологічного середовища способи передачі запитів (заявок, реквестів, тікетів) службі IT-підтримки можуть бути:

- телефоном (служба підтримки повинна створити запит від імені користувача);
- електронною поштою (служба підтримки повинна створити запит від імені користувача);
- через обраний канал зв’язку, месенджер (служба підтримки повинна створити запит від імені користувача);
- через портал самообслуговування (автоматична реєстрація заявки).

Для забезпечення швидкого та якісного вирішення проблем підприємства можуть використовувати системи автоматизації технічної підтримки, такі як «service desk». У разі виникнення інциденту або підозри на порушення, користувач може подати запит, надавши необхідну інформацію про подію, та стежити за статусом розслідування.

Спеціалісти відповідальні за розслідування можуть використовувати службу підтримки для аналізу докладних відомостей про подію, спільного обговорення стратегій вирішення і ведення відповідних дій. Після завершення розслідування можуть бути збережені всі відомості, знайдені рішення та вжиті заходи безпеки для майбутнього використання та вивчення.

За типологія запити в службу підтримки можна поділити на:

- запит на обслуговування;
- інцидент;
- виявлена проблема (проблеми є першопричинами інцидентів, часто є масовою);
- зміна.

Використання служби підтримки допомагає організувати та систематизувати процес розслідування інцидентів, забезпечуючи ефективну спільну роботу між різними учасниками і збереження важливих даних.

Запити можна створити двома способами:

1. В ручному форматі:
   - від користувача по телефону;
   - від користувача через пошту;
   - від користувача через обраний канал зв’язку, месенджер.
2. Автоматичне створення:
   - через портал самообслуговування (служба підтримки);
   - одинарний запит (очікується конкретна дія);
   - запит за каскадом по дереву (формується кілька заявок);
   - запит від автоматизованої системи (зовнішньої, внутрішньої, гібридної);
   - скрипт (автоматизації).

Аналіз мотивів створення заявок дозволяє докладніше розкрити специфіку об’єктів, що підлягають взаємодії з підтримкою, та визначити наявні тенденції та особливості взаємодії користувачів із службою підтримки на підставі вказаних мотивів. У свою чергу, їх систематизація дозволить визначити вплив на організаційні процеси та вдосконалити підтримку користувачів [14].

Різновиди заявок:

- запит на обслуговування;
- будь-яка явна/неявна проблема;
- автоматично при виявлені аномалії;
- виявлення фроду [4];
- протягом розслідування інцидентів;
- гарантія якості «quality assurance»;
- виявлення помилок «bug bounty»;
- криміналістика «security forensics»;
- усунення несправностей «troubleshooting».

Пріоритизація запитів на потенційні інциденти безпеки

Оскільки ризики інформаційної безпеки і ефективність засобів контролю змінюються в залежності від обставин, організації можуть ранжувати інциденти за наступними критеріями:

- за пріоритетністю;
- за часом реагування;
- за часом виконання запиту;
- за типом запиту (в залежності від типу продукту, вендора, класу загрози).

Головною метою забезпечення інформаційної безпеки є усунення загроз та мінімізація можливих збитків, які можуть виникнути внаслідок реалізації цих загроз [14], [15]. Тому важливим фактором є ранжування інцидентів за пріоритетністю [16]:

- критичний (critical);
- високий (high);
- середній (medium);
- низький (low);
- інформаційний (informational).

Війна в Україні спричинила помітне збільшення застосування шкідливого програмного забезпечення (ПЗ) для видалення даних. Характерною ознакою атак є їх розповсюдження в інших країнах. У 2022 році проти українського провайдера було використане ПЗ AcidRain, яке також було використане в атаках, що відключили практично 6 000 вітряків в Німеччині. Загальна кількість атак за 2022 рік на українські організації була понад дві тисячі (див. рис. 1). З них понад 300 були спрямовані на сектор безпеки й оборони, понад 400 на групи, що впливають на цивільне життя, включаючи комерційний, енергетичний, фінансовий, телекомунікаційний сектори та програмне забезпечення та понад 500 атак проти урядових груп [17].

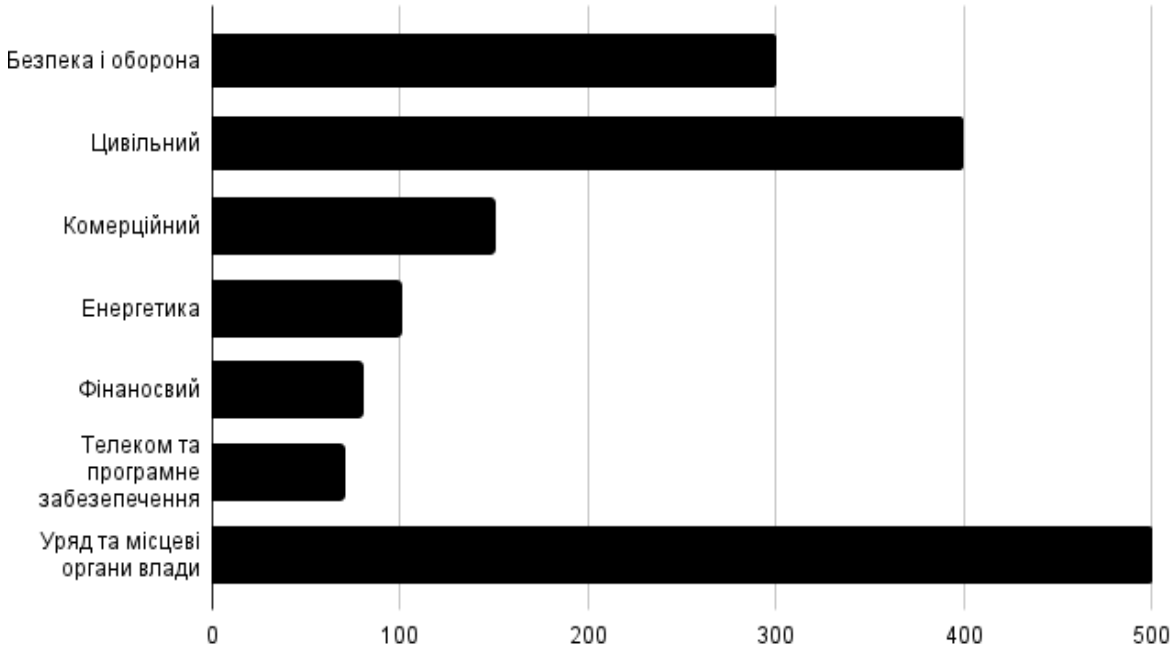

Рис. 1. Кількість кібератак за секторами в Україні у 2022 році

У 2023 році кібератаки змінили своє спрямування (рис. 2) зі сфери оборони на сектори комерції, енергетики, фінансів, телекомунікацій та державного управління [18].

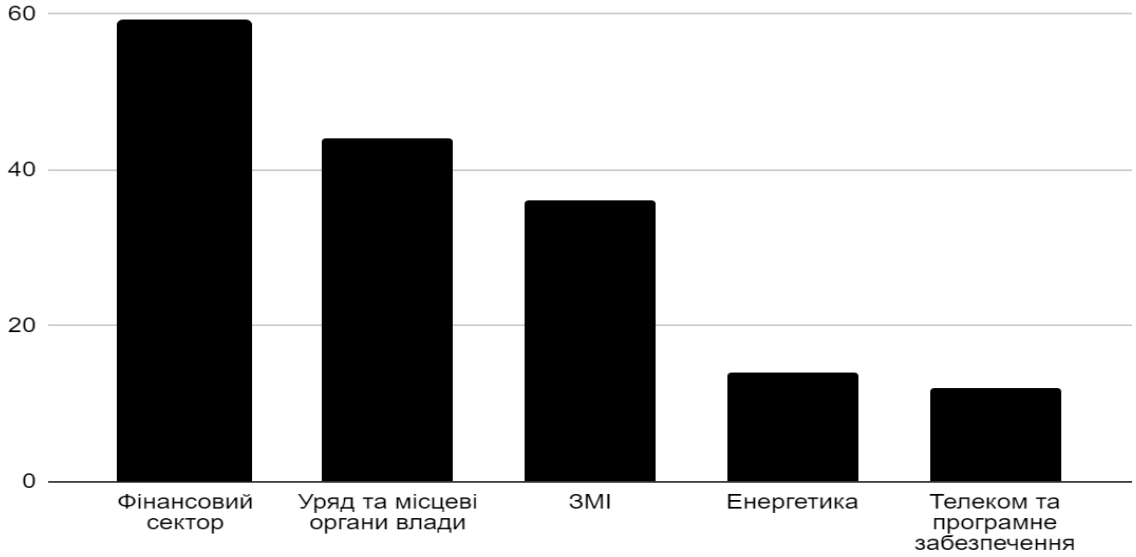

Рис. 2. Розподіл активності проросійських хакерських угруповань за другий квартал 2023 року в процентах

До найпоширеніших типів інцидентів інформаційної безпеки можна віднести наступні [4], [8]:

- аномальна поведінка облікових записів привілейованих користувачів;
- неавторизовані інсайдери намагаються отримати доступ до серверів і даних;
- аномалії у вихідному мережевому трафіку;
- трафік, надісланий до невідомих мереж або з невідомих місць;
- надмірне споживання ресурсів апаратного забезпечення;
- неавторизовані (непогоджені) зміни в конфігурації;
- виявлення прихованих файлів;
- несподівані, аномальні зміни на системах, з обліковими записами;
- аномальна робота браузера;
- підозрілі записи реєстру.

Розслідування та процес реагування наведено в табл. 1.

Таблиця 1

Розслідування та реагування поширених типів атак

Назва атаки/ інцидент	Деталізації	Валідаційні параметри	Джерело інформації	Усунення та відновлення
Програми-вимагачі «ransomware» [7], [10]	Зловмисник використовує програми-вимагачі для шифрування або отримання інформації жертви з метою отримання викупу.	Виявлення зашифрованих файлів або повідомлення з вимогою викупу. Зміна розширення файлів на незрозумілі або	OS Logs, AV Logs, Account Logs, Network traffic	Ізолювання системи від мережі для запобігання поширенню. Запуск антивірусного ПЗ для виявлення та видалення шкідливого ПЗ. Використання резервних копій для відновлення шифрованих даних, заміна паролів паролі.

		вимоги до введення ключа. Перешкоди в доступі до файлів чи системи.		
Спеціалізована стійка загроза «advanced persistent threats» [8]	Довготривала та високорівнева кіберзагроза, що складається з високоорганізованої групи зловмисників, які завдовжки часу спрямовано та систематично ведуть атаки на конкретну ціль з метою викрадення чутливої інформації.	Довготривалі підозрілі активності у мережі або системі. Неочікувані втрати даних або інформації. Підозрілі вхідні та вихідні мережеві з'єднання.	Network traffic, Access Logs, OS Logs, зв'язок із власником сервера/службами підтримки	Ізолювання зараженої системи в мережі, виявлення та видалення шкідливого ПЗ. Оцінка мережевої архітектури та рівня захисту. Виконання аудиту безпеки та вдосконалення моніторингу для виявлення подібних загроз.
Атака відмовою в обслуговуванні «denial-of-service (DoS)» [6], [8], [9]	Спроба перевантаження системи або мережі, щоб завадити її нормальному функціонуванню та доступу користувачів.	Періоди зниження продуктивності або недоступності системи. Висока витратність ресурсів під час навантаження на сервер.	OS Logs, Firewall Logs, Network traffic	Блокування зловмисницького трафіку. Створення обмеження на частоту запитів для попередження атак. Оцінка впливу атаки на систему та вживання заходів для запобігання подібним атакам у майбутньому.
Розподілена атака відмовою в обслуговуванні «distributed denial-of-service (DDoS)» [9], [7], [19]	Спроба перевантаження комп'ютерної системи або мережі шляхом одночасної активності великої кількості зловмисників, з метою призупинити нормальну роботу цієї системи.	Відчутні перешкоди у роботі мережі або сервісу. Велика кількість незвичайних запитів або активності на сервері.	OS Logs, Firewall Logs, Network traffic	Виявлення та блокування зловмисницького трафіку. Звернення до служби хостингу для допомоги в розсіюванні атаки. Перегляд архітектури мережі та інфраструктури для покращення стійкості до атак DDoS.
Вторгнення методом підбору «brute forcing» [7]	Зловмисник намагається вгадати пароль, намагаючись ввести кілька різних паролів	Багатократні невдачі при вході під одним обліковим записом. Неочікувана активність або незвичайний	Active Directory Logs, Application Logs, OS Logs, зв'язок із користувачем	Усунення: Блокування доступу до системи. Зміна паролів для підозрілих облікових записів. Зміна всіх паролів, встановлення двофакторної автентифікації для додаткового захисту.

		обсяг вхідних запитів.		
Мережа ботів «botnets»	Зловмисники використовують сервер-жертву для здійснення DDOS-атак або інших шкідливих дій	Необґрунтована активність на комп'ютерах або в мережі. Підозрілі мережеві з'єднання до відомих центрів керування.	Network traffic, OS Logs, зв'язок із власником сервер, зв'язок із службою підтримки	Визначення джерела інфікування, блокування облікового запису, видалення шкідливого ПЗ із систем. Зміна паролів, перевірка системи на аномальну активність.
Виведення даних «data exfiltration»	Нелегальний вивід чутливої або конфіденційної інформації з комп'ютерної системи чи мережі без дозволу власника.	Неавторизовані надходження даних або файлів до недовірливих серверів. Зміни в обсягах передачі даних або активності на мережі.	Network traffic, OS Logs, Proxy Logs	Виявлення способів виведення даних та блокування доступу. Перегляд системи на наявність шкідливого ПЗ та забезпечення безпеки мережі. Використання резервних копій для відновлення втрачених даних, заміна паролів.
Скомпрометований обліковий запис «compromised account»	Ситуація, коли зловмисники здобули доступ до облікового запису користувача (зазвичай шляхом використання краденого пароля чи інших методів) і можуть використовувати цей доступ для незаконних дій.	Невідома активність або вхід під обліковим записом з незвичайних регіонів. Зміни в персональних налаштуваннях облікового запису.	Active Directory Logs, OS Logs, Network traffic, зв'язок із користувачем для уточнень	Блокування доступу, зміна паролів для облікових записів. Визначення способу компрометації та видалення вразливості. Зміна всіх паролів, оновлення облікових записів та встановлення двофакторної автентифікації.
Фішингова атака «phishing» [5] – [7]	Атака, під час якої зловмисники намагаються обманом вивести чутливу інформацію від користувачів шляхом вигляду, ніби вони комунікують з надійним джерелом.	Надходження підозрілих або підроблених електронних листів. Посилання на ненадійні веб-сайти або вимоги ввести особисту інформацію.	Email Headers, URL Analysis, User Reports, Web Server Logs, DNS Records	Розпізнавання та блокування небезпечні листи та посилання. Повідомлення співробітників про можливу загрозу. Навчання співробітників про фішинг та вимоги безпеки.
SQL-ін'єкція «SQL injection» [7]	Техніка атаки, під час якої зловмисники вводять	Аномальні запити, що містять SQL-код, які можуть	Database Logs, Web Application Logs,	Виправлення вразливостей в програмному коді, що дозволяли SQL-ін'єкції. Аудит для виявлення інших вразливих

	шкідливі SQL-запити в веб-додаток з метою отримання несанкціонованого доступу до бази даних.	змінювати або розкривати дані.	Network Traffic Analysis, Input Validation and Sanitization Reports	точок. Оновлення ПЗ, для запобігання SQL-ін'єкціям, перевірка бази даних на несанкціоновану активність.
Міжсайтовий скриптінг «cross-site scripting (XSS)» [7]	Тип атаки, під час якої зловмисники вставляють шкідливий код у веб-сайт, що виконується на боці клієнта, з метою отримання доступу до даних користувачів.	Аномальна активність. Неочікувані втрати даних або інформації.	Web Server Logs, Browser Console Logs, User Reports, Code Reviews, Input Validation and Sanitization Reports	Виправлення вразливостей у веб-додатку, що дозволяли XSS. Фільтрування та екранування введення даних. Перевірка код веб-додатка на наявність вразливостей, виправлення. Реалізація системи контролю та валідації даних.
Атака «Людина посередині» «man-in-the-middle» [7]	Атака, під час якої зловмисники вступають між двома сторонами комунікації з метою перехоплення чи зміни передачі даних.	Неочікувана зміна або перенаправлення мережевих з'єднань. Наявність підозрілих прослуховувачів у мережі.	Network Traffic Analysis, Certificate Authorities Logs, Firewall/Router Logs, Endpoint Security Logs	Захист мережі шляхом використання шифрування трафіку та сертифікатів безпеки. Відстеження та блокування підозрілих мережевих з'єднань. Оновлення сертифікатів, зміна паролів, аудит систем на вразливості, розробка план захисту від подібних атак.
Соціальна інженерія «social engineering» [4], [5]	Маніпулювання та обман користувачів з метою отримання конфіденційної інформації або здійснення інших шкідливих дій.	Неочікувані запити або прохання від невідомих осіб. Дії або заяви, які викликають сумнів чи вимагають конфіденційної інформації.	Інтерв'ю з користувачами, звіти про інциденти, записи електронної пошти та спілкування, відеозаписи та відеоспостереження	Навчання співробітників, розробка процедури підтвердження ідентифікації.
Незапрошене завантаження «drive-by download» [7]	Зловмисник без попередження чи дозволу користувача автоматично завантажує шкідливе ПЗ або код на його комп'ютер чи пристрій.	Автоматичне завантаження інфікованого ПЗ або вірусів при відвідуванні підозрілих веб-сайтів або взаємодії з ними.	Web Server Logs, Browser History and Downloads, Network Traffic Analysis, Malware Analysis Reports	Оновлення браузерів, встановлення блокування небезпечних вмістів. Перевірка веб-сайтів на вразливості та потенційно шкідливі скрипти. Відновлення системи з резервних копій, перегляд налаштування безпеки браузера.

Події в Україні показали, як ці типи атак можуть бути використані для погіршення роботи критичної інфраструктури та послуг для підтримки більших цілей війни.

План реагування на інциденти

План реагування забезпечує комплексний підхід до інцидентів, описуючи кроки реагування та способи обробки подій таким чином, щоб скоротити час відновлення, мінімізувати витрати та зменшити збитки. У ньому має бути чітко визначено групу реагування, включно з їхніми ролями та обов'язками, протоколами, політиками та перед ким команда повинна звітувати.

Після інциденту група реагування повинна оцінити реакцію, вивчити способи запобігання повторенню інциденту та визначити шляхи вдосконалення плану реагування на кібер інцидент відповідно до інциденту [20].

В рамках розробленої стейт-машини (рис. 3) представлений формалізований опис плану обробки інцидентів.

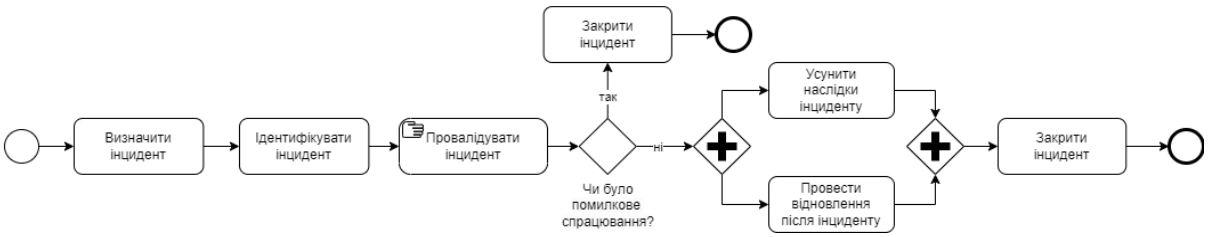

Рис. 3. Стейт-машина розслідування інцидентів

Механіка розслідування інцидентів завжди складається з однакових етапів, незалежно від розмірів організації та специфіки її інформаційної системи:

1. Промоніторино інцидент інформаційної безпеки:
   - аномальний мережевий трафік; спроби несанкціонованого доступу;
   - аномальні дії зі сторони користувача;
   - виявлене зловмисне ПЗ тощо.

Використовуючи наступні типи рішень: SIEM, IDS/IPS, EDR/XDR тощо. Створено запис інциденту та призначено інцидент відповідному члену групи.

2. Інцидент проіндексовано та розпочато збір інформації:
   - дата та час події; про уражені системи та дані;
   - про потенційного зловмисника;
   - будь-які інші логи, докази.

Відповідно до класифікації інциденту, визначено рівень пріоритету та серйозності.

3. Інцидент проаналізовано:
   - причини інциденту;
   - масштаб інциденту;
   - розмір збитків;
   - стан уражених систем і даних; потенційні цілі зловмисника.
4. Спрацювання виявилось помилковим, інцидент закрито та задокументовано для подальшого використання.
5. Спрацювання не виявилось помилковим, інцидент стримано. А саме, негайно вжито заходів, щоб локалізувати інцидент і запобігти подальшим збиткам:
   - від'єднано уражені системи від мережі;
   - завершено скомпрометовані служби;
   - ізольовано системи, кінцеві точки;
   - заблоковано IP-адреси та домени тощо.

6. Вжито заходи для одночасного усунення першопричини інциденту: виправлено вразливості, видалено зловмисне ПЗ та змінено скомпрометовані облікові дані.
7. Паралельно відновлено нормальну роботу: системи було підключено до мережі, дані відновлено із резервних копій, системи та програми успішно протестовано. Таким чином, забезпечена безперервність бізнес-процесів під час виконання необхідних відновлювальних заходів.
8. Інцидент закрито та зроблено висновки: задокументовано інцидент, включаючи причину, вплив і кроки, вжиті для його вирішення. Проведено аудит процесу реагування на інциденти [13], [21], переглянуто та оновлено (покращено) процеси управління інцидентами.

Приклади реалізації механізму

Розберемо застосування даного механізму на прикладі нещодавніх атак, що здійснювались на об'єкти критичної інфраструктури.

Інцидент 1: Скомпрометований обліковий запис співробітника

Першою була стадія дослідження. Цю атаку проводили з нещодавно тимчасово окупованої росіянами української території. Хакери використали для розвідки скомпрометований обліковий запис співробітника компанії. І на першому етапі намагалися скомпрометувати й інші облікові записи співробітників [22].

07.03.2022 близько 20:00 виявлено інцидент:

- виявлено використання HackTool:Win32/DumpLSASS, спроби дампування процесу LSASS;
- використання Mimikatz (утиліта для перехоплення паролів на Windows);
- зафіксована успішна авторизація на VPN;
- зловмисник спробував створити політику в домені, яка спрямовувалася на масове видалення файлів.

Вжито наступні заходи: блокування скомпроментованого облікового запису та зміна пароля. Запущено розслідування. Внаслідок атаки були скомпрометовані активи: комп'ютерну мережу, сервери, робочі станції, мережевий ресурс та здійснено спробу створити політику для масового видалення файлів у домені. Атака відбулася в неробочий час.

Інцидент 2: Вторгнення та атаки

Другим етапом стала атака, під час якої хакери намагались вивести з ладу обладнання та сервіси компанії, а також отримати контроль над мережею та обладнанням. Були вчинені спроби змінити паролі від облікових записів працівників компанії, обладнання, фаєрволів [22]. Обидва інциденти відбувались у нічний час, що одразу видавало аномальну кількість подій:

- 26.03.2022 близько 20:00 виявлено SMB-атаку на один з серверів з дампуванням процесу LSASS та зламано обліковий запис одного з співробітників, що призвело до доступу до корпоративної пошти;
- 26.03.2022 о 20:40 зафіксовано атаку hands-on-keyboard за допомогою набору інструментів Impacket на одній з кінцевих точок адміністратора. Для усунення о 21:09 було заблоковано скомпроментований обліковий запис адміністратора;
- 26.03.2022 о 21:20 виявлено спробу підключення по протоколу SSH на одну з IP-адрес, для усунення обліковий запис одразу було заблоковано;

- 26.03.2022 о 21:32 зафіксовано віддалене виконання коду на домені за допомогою WMI;
- 26.03.2022 о 21:57 зловмисниками було виконано скрипт для зміни паролів всіх користувачів домену, у відповідь було закрито доступ до VPN;
- наступного дня близько 14:00 встановлено, що адміністратори мережі втратили доступ до мережевого обладнання та змінено паролі всіх локальних адміністраторів;
- 27.03.2022 близько 14:35 Для усунення інциденту було прийнято рішення фізично вимкнути мережеве обладнання.

Наслідки атаки: недоступність служб IT-інфраструктури, заблоковано віддалений доступ, недоступність електронної пошти та додатків для спільного використання файлів, скомпрометовані сервери, робочі станції, мережевий ресурс.

Для безперервного надання послуг військовим та критичній інфраструктурі під час виконання необхідних відновлювальних заходів було обмежено доступ для користувачів та бізнесу [22], [23].

РЕКОМЕНДАЦІЇ ДЛЯ УСПІШНОЇ ПРОТИДІЇ АТАКАМ

1. Необхідно впроваджувати новітні (інноваційні) інструменти моніторингу слідуючи кращим практикам у цій області.

2. Має бути розроблений план щодо швидкої локалізації інциденту (ізоляція уражених систем, вимкнення скомпрометованих облікових записів чи серверів, блокування зловмисного мережевого трафіку тощо), забезпечуючи безперервність бізнес-процесів під час виконання необхідних відновлювальних заходів. Таким чином протягом розслідування інциденту, команда реагування має паралельно відновлювати нормальну роботу систем відповідно до завчасно розробленого плану відновлення.

3. Рекомендуємо координуватися з фахівцями CERT-UA, це урядова команда реагування на комп’ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв’язку та захисту інформації України, та іншими стейкхолдерами задля покращення безпеки інформаційного простору України (формування атрибутів інцидентів, превентивних дій зі сторони держави, спільного розслідування інцидентів тощо).

4. Необхідно дотримуватися протоколу збереження та логування всіх подій задля підвищення ефективності процесу розслідування інцидентів.

5. Після закриття інциденту має бути проведений аудит процесу реагування на інциденти з метою використання досвід для підвищення кіберстійкості компанії та держави в цілому.

6. Рекомендується на регулярній основі організовувати навчальні заходити щодо найкращих практик в інформаційній безпеці для співробітників, адже саме від них залежить безпека всієї організації.

7. За можливістю залучати зовнішніх партнерів (стейкхолдерів), які можуть запропонувати додаткову експертизу та ресурси під час складних інцидентів.

8. Розвивати механізми співпраці з іншими державними органами, агентствами безпеки, а також з міжнародними партнерами для обміну інформацією, спільної розробки стратегій та спільного реагування на загрози.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В статті проаналізовані різні класифікації інцидентів інформаційної безпеки, шляхи усунення та відновлення. Продемонстровано механіку розслідування інцидентів інформаційної безпеки на етапах моніторингу, індексації, збору інформації, усунення, відновлення та закриття. В публікації запропонований формалізований опис плану обробки інцидентів у формі стейт-машини, що дозволяє систематизувати та автоматизувати процес реагування на інциденти.

На прикладах атак, спрямованих на об'єкти критичної інфраструктури, показано застосування цього механізму та визначено заходи, спрямовані на покращення системи інформаційної безпеки, які можуть бути використані для захисту державних та комерційних установ та організацій.

В результаті, запропоновані рекомендації для успішної протидії кібератакам і забезпечення інформаційної безпеки організації чи держави, необхідно впроваджувати інструменти моніторингу та координуватися з урядовими та міжнародними командами реагування. Також, важливо регулярно проводити навчання співробітників та розвивати механізми співпраці з партнерами для ефективного захисту від кібератак. Виконання цих заходів сприяє забезпеченню надійного кіберзахисту та зменшенню можливих збитків.

Подальші дослідження будуть спрямовані на розробку нових алгоритмів виявлення загроз, вивчення ефективності заходів інформаційної безпеки державних та комерційних установ та організацій, впровадження систем автоматизованої реакції на інциденти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dohtieva, I., & Shyian, A. (2023). Analysis of the Effectiveness of the Security Incident Response Team Under Intensity Cyber-Attack Increasing. In *Mathematical Modeling and Simulation of Systems, Lecture Notes in Networks and Systems, 667*, 183–197. https://doi.org/10.1007/978-3-031-30251-0_15
2. Embroker. (2023). *2023 Must-Know Cyber Attack Statistics and Trends*. https://www.embroker.com/blog/cyber-attack-statistics/
3. Globe Newswire. (2022). *Cybercrime to Cost the World $10.5 Trillion Annually by 2025.* https://www.globenewswire.com/news-release
4. Tsyrkaniuk, D., et al. (2021). Method of marketplace legitimate user and attacker profiling. *Cybersecurity: Education, Science, Technique, 2(14),* 50–67. https://doi.org/10.28925/2663-4023.2021.14.5067
5. Sokolov, V., & Kurbanmuradov, D. (2018). The Method of Combating Social Engineering at the Objects of Information Activity. *Cybersecurity: Education, Science, Technique*, *1*, 6–16. https://doi.org/10.28925/2663-4023.2018.1.616
6. CrowdStrike. (2023). *10 most common types of cyber attacks.* https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/
7. DNSstuff. (2023). *Types of Cyber Security Attacks.* https://www.dnsstuff.com/types-of-cyber-security-attacks
8. TechTarget. (2023). *10 types of security incidents and how to handle them*. https://www.techtarget.com/searchsecurity/feature/10-types-of-security-incidents-and-how-to-handle-them
9. Hulak, H., et al. (2020). Cryptovirology: Security Threats to Guaranteed Information Systems and Measures to Combat Encryption Viruses. *Cybersecurity: Education, Science, Technique, 2(10),* 6–28. https://doi.org/10.28925/2663-4023.2020.10.628
10. Zhao, Y. (2021). Application of Machine Learning in Network Security Situational Awareness. In *Proceedings of the 2021 World Conference on Computing and Communication Technologies (WCCCT)*. https://doi.org/10.1109/WCCCT52091.2021.00015
11. Sriram, G. S. (2022). Security Challenges of Big Data Computing. *International Research Journal of Modernization in Engineering Technology and Science, 4(1),* 1164–1171. https://doi.org/10.0202/DATA.2022708702

12. Xu, W., et al. (2022). Research on Network Security Situational Awareness based on Crawler Algorithm. *Security and Communication Networks II, 3188(2)*, 1–9. https://doi.org/10.1155/2022/3639174
13. Roy, Y. V., Mazur, N. P., & Skladannyi, P. M. (2018). Audit of Information Security is the Basis of Effective Protection of the Enterprise. *Cybersecurity: Education, Science, Technique, 1(1)*, 86–93. https://doi.org/10.28925/2663-4023.2018.1.8693
14. Kyrychok, R., et al. (2021). Rules for the Implementation of Exploits during an Active Analysis of the Corporate Networks' Security based on a Fuzzy Assessment of the Quality of the Vulnerability Validation Mechanism. *Cybersecurity: Education, Science, Technique, 2(14)*, 148–157. https://doi.org/10.28925/2663-4023.2021.14.148157
15. Politico. (2023). *Russia's cyberattacks aim to 'terrorize' Ukrainians.* https://www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561
16. *Information technology — Security techniques — Information security risk management.* (2022). (ISO/IEC 27005:2022)
17. State Special Communications and Information Protection Service of Ukraine. (2023). *War in Ukraine pulse of cyber defense.*
18. State Service for Special Communications and Information Protection of Ukraine. (2023) *The number of information security events in the "Malicious software code".* https://cip.gov.ua/ua/news/kilkist-podii-informaciinoyi-bezpeki-u-kategoryi-shkidlivii-programnii-kod-zrosla-u-95-8-raza-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz
19. Security Investigation. (2023). *Incident Response for Common Attack Types.* https://www.socinvestigation.com/incident-response-for-common-attack-types
20. Buriachok, V., Sokolov, P., & Skladannyi P. (2019). Security Rating Metrics for Distributed Wireless Systems. In: *8th International Conference on "Mathematics. Information Technologies. Education" (MoMLeT&DS), vol. 2386*, 222–233.
21. Kipchuk, F., et al. (2021). Assessing Approaches of IT Infrastructure Audit. In: *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PICST)*, 213–217. https://doi.org/10.1109/picst54195.2021.9772181
22. State Special Communications and Information Protection Service of Ukraine. (2022). *Cyber Attack on Ukrtelecom on March 28.* https://cip.gov.ua/ua/news/kiberataka-na-ukrtelekom-28-bereznya-detali
23. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Diana Tsyrkaniuk
PhD Student of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-9422-8617
d.tsyrkaniuk.asp@kubg.edu.ua

Volodymyr Sokolov
PhD, Associate Professor, Associate Professor of the Department of
Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

METHODOLOGY FOR INVESTIGATING INFORMATION SECURITY INCIDENTS

Abstract. The development and implementation of a comprehensive information security strategy during times of war are critical tasks for ensuring national security and protecting vital resources and information. The article analyzes various types of incidents in the field of information security, their mitigation, and recovery methods. It demonstrates the mechanics of investigating information security incidents at stages such as monitoring, indexing, data collection, mitigation, recovery, and closure. The publication presents a formalized description of an incident-handling plan in the form of a state machine, enabling the systematization and automation of the incident response process. Using examples of attacks targeting critical infrastructure, it illustrates the application of this mechanism and identifies measures aimed at enhancing the information security system, which can be employed to protect both governmental and commercial institutions and organizations. As a result, the recommended strategies for effectively countering cyberattacks and ensuring information security for organizations or nations include the implementation of monitoring tools and coordination with governmental and international response teams. It is also crucial to regularly train employees and develop mechanisms for collaboration with partners to achieve efficient protection against cyber threats. These measures contribute to strengthening cybersecurity and reducing potential damages. Future research may encompass the development of new threat detection algorithms, evaluating the effectiveness of information security measures for governmental and commercial institutions, implementing automated incident response systems, as well as studying the impact of war on critical infrastructure and international cooperation in this field, exploring opportunities for international cooperation and information exchange in the realm of information security during conflicts for the collective defense of national interests.

Keywords: cybersecurity; security incident; information protection; quality assurance; bug bounty; security forensics; troubleshooting; fraud.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Dohtieva, I., & Shyian, A. (2023). Analysis of the Effectiveness of the Security Incident Response Team Under Intensity Cyber-Attack Increasing. In *Mathematical Modeling and Simulation of Systems*, *Lecture Notes in Networks and Systems, 667*, 183–197. https://doi.org/10.1007/978-3-031-30251-0_15
2. Embroker. (2023). *2023 Must-Know Cyber Attack Statistics and Trends*. https://www.embroker.com/blog/cyber-attack-statistics/
3. Globe Newswire. (2022). *Cybercrime to Cost the World $10.5 Trillion Annually by 2025.* https://www.globenewswire.com/news-release
4. Tsyrkaniuk, D., et al. (2021). Method of marketplace legitimate user and attacker profiling. *Cybersecurity: Education, Science, Technique, 2(14),* 50–67. https://doi.org/10.28925/2663-4023.2021.14.5067
5. Sokolov, V., & Kurbanmuradov, D. (2018). The Method of Combating Social Engineering at the Objects of Information Activity. *Cybersecurity: Education, Science, Technique*, *1*, 6–16. https://doi.org/10.28925/2663-4023.2018.1.616

6. CrowdStrike. (2023). *10 most common types of cyber attacks.* https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/
7. DNSstuff. (2023). *Types of Cyber Security Attacks.* https://www.dnsstuff.com/types-of-cyber-security-attacks
8. TechTarget. (2023). *10 types of security incidents and how to handle them*. https://www.techtarget.com/searchsecurity/feature/10-types-of-security-incidents-and-how-to-handle-them
9. Hulak, H., et al. (2020). Cryptovirology: Security Threats to Guaranteed Information Systems and Measures to Combat Encryption Viruses. *Cybersecurity: Education, Science, Technique, 2(10)*, 6–28. https://doi.org/10.28925/2663-4023.2020.10.628
10. Zhao, Y. (2021). Application of Machine Learning in Network Security Situational Awareness. In *Proceedings of the 2021 World Conference on Computing and Communication Technologies (WCCCT)*. https://doi.org/10.1109/WCCCT52091.2021.00015
11. Sriram, G. S. (2022). Security Challenges of Big Data Computing. *International Research Journal of Modernization in Engineering Technology and Science, 4(1)*, 1164–1171. https://doi.org/10.0202/DATA.2022708702
12. Xu, W., et al. (2022). Research on Network Security Situational Awareness based on Crawler Algorithm. *Security and Communication Networks II, 3188(2)*, 1–9. https://doi.org/10.1155/2022/3639174
13. Roy, Y. V., Mazur, N. P., & Skladannyi, P. M. (2018). Audit of Information Security is the Basis of Effective Protection of the Enterprise. *Cybersecurity: Education, Science, Technique, 1(1)*, 86–93. https://doi.org/10.28925/2663-4023.2018.1.8693
14. Kyrychok, R., et al. (2021). Rules for the Implementation of Exploits during an Active Analysis of the Corporate Networks' Security based on a Fuzzy Assessment of the Quality of the Vulnerability Validation Mechanism. *Cybersecurity: Education, Science, Technique, 2(14)*, 148–157. https://doi.org/10.28925/2663-4023.2021.14.148157
15. Politico. (2023). *Russia's cyberattacks aim to 'terrorize' Ukrainians.* https://www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561
16. *Information technology — Security techniques — Information security risk management.* (2022). (ISO/IEC 27005:2022)
17. State Special Communications and Information Protection Service of Ukraine. (2023). *War in Ukraine pulse of cyber defense.*
18. State Service for Special Communications and Information Protection of Ukraine. (2023) *The number of information security events in the "Malicious software code".* https://cip.gov.ua/ua/news/kilkist-podii-informaciinoyi-bezpeki-u-kategoryi-shkidlivii-programnii-kod-zrosla-u-95-8-raza-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz
19. Security Investigation. (2023). *Incident Response for Common Attack Types.* https://www.socinvestigation.com/incident-response-for-common-attack-types
20. Buriachok, V., Sokolov, P., & Skladannyi P. (2019). Security Rating Metrics for Distributed Wireless Systems. In: *8th International Conference on "Mathematics. Information Technologies. Education" (MoMLeT&DS), vol. 2386*, 222–233.
21. Kipchuk, F., et al. (2021). Assessing Approaches of IT Infrastructure Audit. In: *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PICST)*, 213–217. https://doi.org/10.1109/picst54195.2021.9772181
22. State Special Communications and Information Protection Service of Ukraine. (2022). *Cyber Attack on Ukrtelecom on March 28.* https://cip.gov.ua/ua/news/kiberataka-na-ukrtelekom-28-bereznya-detali
23. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.