SECTION 2: CYBERSECURITY AND CRITICAL INFRASTRUCTURE

FEATURES OF MODELING AND INVESTIGATING INFORMATION AND CYBERSECURITY INCIDENTS

Orest Polotai, Valeriia Balatska, Artur Tkachenko

ОСОБЛИВОСТІ МОДЕЛЮВАННЯ ТА РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

Полотай О.І., Балацька В.С., Ткаченко А.М.
Львівський державний університет безпеки життєдіяльності, (Україна)

Анотація. У сучасному цифровому світі кіберзагрози стають усе більш витонченими та небезпечними. Виявлення, аналіз і реагування на інциденти кібербезпеки потребують ефективних підходів, серед яких особливе місце займає моделювання інцидентів. У доповіді розглянуто роль моделювання в розслідуванні кіберінцидентів, наведено методи побудови моделей, а також засоби ідентифікації джерел загроз.

Вступ. З розвитком інформаційних технологій питання забезпечення кібербезпеки набуває першочергового значення. Організації стикаються з дедалі більш складними загрозами – від фішингу та шкідливого програмного забезпечення до цілеспрямованих атак на критичну інфраструктуру. Розслідування інцидентів кібербезпеки [4] стає необхідною умовою мінімізації втрат, попередження повторних атак і підвищення загального рівня захисту.

Однак сам процес розслідування потребує чіткого розуміння механізмів атак, джерел загроз і вразливостей, які були використані. Тут на допомогу приходить моделювання – створення логічних або віртуальних моделей інцидентів, які дозволяють відтворити хід подій, знайти слабкі місця та розробити ефективні заходи реагування.

Актуальність досліджень. На сьогодні рівень цифровізації критичних сфер діяльності суспільства – фінансів, охорони здоров'я, енергетики – вимагає надійного кіберзахисту. Статистика свідчить про щорічне зростання кількості інцидентів, зокрема через соціальну інженерію, zero-day вразливості та складні багаторівневі атаки (APT – Advanced Persistent Threats). У 2024 році кількість кібератак на Україну зросла на 69,8%, досягнувши 4315 інцидентів, у порівнянні з 2023 роком, коли було зафіксовано 2541 кіберінцидентів [3].

Зважаючи на це, моделювання інцидентів дозволяє:

- визначити потенційні вектори атак;
- імітувати поведінку зловмисника в контрольованому середовищі;
- оцінити ефективність систем виявлення атак;
- пришвидшити процес реагування на інциденти;
- надати доказову базу для юридичного розслідування.

Таким чином, розробка і дослідження моделей кіберінцидентів є важливою складовою сучасної практики кіберзахисту.

Постановка задачі. Метою даного дослідження є вивчення ролі моделювання у процесі розслідування інцидентів кібербезпеки, аналіз існуючих підходів та інструментів, а також визначення ефективності їх застосування.

Задачами дослідження є:

1. Провести аналіз існуючих методів моделювання інцидентів.
2. Побудувати модель типового інциденту за методикою STRIDE/ATT&CK.
3. Визначити ефективність використання моделювання у виявленні джерел загроз.
4. Розробити рекомендації щодо інтеграції моделювання в системи кіберзахисту.

Результати досліджень. У рамках дослідження було проаналізовано кілька підходів до моделювання інцидентів [2], зокрема:

- Метод STRIDE – класифікація загроз за шістьма основними категоріями (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Це методологія моделювання загроз, розроблена компанією Microsoft для систематичної ідентифікації потенційних вразливостей у проєктуванні інформаційних систем. Назва STRIDE є абревіатурою з перших літер шести основних категорій загроз:

S – Spoofing (Підміна особи)
T – Tampering (Підробка або модифікація даних)
R – Repudiation (Відмова від дій)
I – Information Disclosure (Розкриття інформації)
D – Denial of Service (Відмова в обслуговуванні)
E – Elevation of Privilege (Підвищення привілеїв)

Ця модель допомагає інженерам і аналітикам безпеки структуровано аналізувати можливі загрози ще на етапі розробки систем або під час розслідування інцидентів. Більш детальна інформація про дану модель наведена в таблиці 1.

Таблиця 1 – Основні кроки методу STRIDE

Суть	Приклади	Контрзаходи
Spoofing – Підміна особи		
Атака, під час якої зловмисник видає себе за іншого користувача або систему	• Вхід до системи з використанням чужих облікових даних. • Підробка IP-адреси, MAC-адреси або DNS-даних.	• Багатофакторна аутентифікація. • Зашифровані канали передачі (наприклад, HTTPS). • Захист облікових даних та моніторинг логінів.
Tampering – Підробка або модифікація даних		
Несанкціоновані зміни даних у процесі зберігання або передавання	• Модифікація конфігураційних файлів. • Втручання в трафік через MITM (людина посередині). • Підміна вмісту оновлень або програм.	• Контроль цілісності даних (хеші, цифрові підписи). • Використання контрольованого доступу. • Захист каналів зв'язку.
Repudiation – Відмова від дій		
Користувач або система заперечує виконання певних	Користувач каже, що не здійснював транзакцію.	• Аудит і логування дій користувачів.

дій, і при цьому немає доказів протилежного	Відсутність журналів аудиту.	• Нерозривність логів (журнали, які неможливо змінити без сліду). • Цифрові підписи транзакцій.
Information Disclosure – Розкриття інформації		
Несанкціонований доступ до конфіденційної або внутрішньої інформації	• Злив паролів, особистих даних, комерційної інформації. • Витік через лог-файли або помилки в коді (наприклад, stack trace).	• Шифрування даних. • Обмеження прав доступу. • Захист середовищ розробки і тестування.
Denial of Service – Відмова в обслуговуванні		
Атака, яка призводить до недоступності сервісу для легальних користувачів	• Масові запити (DoS або DDoS-атаки). • Вичерпання ресурсів сервера (CPU, RAM, мережевий трафік).	• Балансування навантаження. • Використання фаєрволів і систем виявлення атак. • Захист на рівні додатку (наприклад, ліміти для запитів).
Elevation of Privilege – Підвищення привілеїв		
Отримання зловмисником доступу або прав, які йому не належать.	• Атака через вразливість у веб-застосунку, що дозволяє стати адміністратором. • Виконання коду з правами суперкористувача.	• Принцип найменших привілеїв (least privilege). • Регулярне оновлення ПЗ. • Сегментування доступу в системі.

Метод STRIDE – один із найефективніших інструментів моделювання загроз, який дозволяє виявити потенційні вразливості ще до того, як інцидент відбудеться. У поєднанні з іншими моделями (наприклад, MITRE ATT&CK) він дозволяє побудувати повну картину захисту, що включає як профілактику, так і аналіз після атаки.

- **MITRE ATT&CK Framework** – це всесвітньо визнана база знань про поведінку кіберзловмисників, яка використовується для моделювання загроз, аналізу інцидентів та підвищення рівня кіберзахисту організацій. Цей фреймворк був розроблений дослідницькою організацією MITRE Corporation та з моменту створення став одним із ключових інструментів для аналітиків з кібербезпеки.

MITRE ATT&CK структурується за такими елементами:

1. Tactics (Тактики): Це цілі або стратегічні наміри зловмисника на кожному етапі атаки (наприклад, отримання доступу, утримання присутності в системі, збір інформації).
2. Techniques (Техніки): Це конкретні способи досягнення цілей, визначених у тактиках. Наприклад, техніка «Phishing» використовується в тактиці Initial Access (початковий доступ).
3. Sub-techniques (Підтехніки): Дозволяють деталізувати техніки, щоб відобразити різноманітні методи їх реалізації.
4. Mitigations (Засоби захисту): Рекомендовані заходи для зменшення або запобігання ефективності атак.

MITRE ATT&CK – це не просто база даних атак, а потужний аналітичний фреймворк, який надає змогу не лише розуміти поведінку зловмисників, але й активно будувати стратегії захисту, що базуються на реальних даних. Його впровадження є важливою складовою сучасної кібербезпеки, особливо у контексті розслідування інцидентів та моделювання загроз.

- **Kill Chain Model** – це концептуальна модель, розроблена аналітиками компанії Lockheed Martin, що описує послідовні етапи кібератаки з точки зору зловмисника. Вона вперше була представлена у 2011 році в контексті військових стратегій, але була адаптована до кібербезпеки для розуміння, перехоплення та блокування дій противника на різних етапах атаки.

Модель складається з 7 основних етапів, що представляють типову послідовність кібератаки (табл. 2).

Таблиця 2 – Основні кроки моделі Kill Chain Model

№	Назва	Опис	Мета
1	Reconnaissance (Розвідка)	Зловмисник збирає інформацію про цільову організацію (наприклад, через відкриті джерела, соціальні мережі, сканування мережі).	Виявити вразливі точки або цілі для атаки.
2	Weaponization (Створення зброї)	Комбінування шкідливого ПЗ з експлойтом, наприклад, створення зараженого PDF або Word-файлу.	Підготувати засіб для проникнення.
3	Delivery (Доставка)	Надсилання шкідливого компонента до цілі, наприклад, через фішинговий email, USB-носій або вебсайт.	Донести "зброю" до системи жертви.
4	Exploitation (Експлуатація)	Використання вразливості в системі або у взаємодії користувача (наприклад, відкриття зараженого файлу) для запуску шкідливого коду.	Отримати контроль над системою.
5	Installation (Інсталяція)	Встановлення бекдору або іншого зловмисного ПЗ для забезпечення стійкої присутності у системі	Закріпитися на машині.
6	Command and Control (C2)	Встановлення зв’язку з сервером зловмисника для віддаленого керування зараженою системою.	Отримати контроль та можливість керувати діями
7	Actions on Objectives (Дії для досягнення мети)	Здійснення основної мети атаки: викрадення даних, знищення інформації, саботаж тощо	Досягти цільових результатів (наприклад, шпигунство, фінансова шкода, шифрування даних тощо).

Kill Chain Model – це корисний стратегічний інструмент, який дозволяє виявляти та блокувати кібератаки на різних етапах їх розвитку. У поєднанні з MITRE ATT&CK та

іншими фреймворками вона надає повну картину поведінки зловмисника та дозволяє ефективно будувати системи виявлення, реагування і профілактики атак.

Для практичного дослідження було змодельовано інцидент фішингової атаки з подальшим зараженням системи шкідливим програмного забезпечення. На основі логів та спостережень відтворено сценарій проникнення, ідентифіковано вектори атаки та визначено критичні точки. В табл. 3 показана класифікація загроз в контексті досліджуваного інциденту методом STRIDE.

Таблиця 3 – Класифікація загроз методом STRIDE

Компонент STRIDE	Загроза	Як проявляється в інциденті
Spoofing	Підміна особи	Атакуючий видає себе за легітимного співробітника компанії у фішинговому листі
Tampering	Зміна даних	Модифікація PowerShell-скрипту для приховання слідів
Repudiation	Відмова від дій	Атакуючий використовує викрадені облікові дані без можливості визначення особи
Information Disclosure	Розголошення даних	Облікові дані передаються через Command-and-Control (C2) сервер
Denial of Service	Відмова в обслуговуванні	Не критично в даному сценарії, але можливе в рамках знищення журналів логів
Elevation of Privilege	Підвищення привілеїв	Атакуючий використовує викрадені облікові дані для ескалації прав у мережі

Фреймворк MITRE ATT&CK дозволяє описати кожну фазу інциденту за техніками та тактиками атак у вигляді моделі, яка представлена в таблиці 4.

Таблиця 4 – Модель MITRE ATT&CK з врахуванням тактик та технік

Етап атаки	**Тактика (Tactic)**	**Техніка (Technique)**	**Код ATT&CK**	**Опис дій атакуючого**
Initial Access	Phishing	Spearphishing Link	T1566.002	Користувачу надсилають електронний лист з шкідливим посиланням.
Execution	Command Execution	PowerShell	T1059.001	Сценарій виконується через PowerShell після кліку.
Persistence	Registry Run Keys	Registry Run Keys / Startup Folder	T1547.001	Backdoor додається в автозавантаження.
Privilege Escalation	Exploitation	Exploitation for Privilege Escalation	T1068	Якщо потрібно – експлуатація вразливостей для підвищення прав.
Credential Access	Credential Dumping	LSASS Memory	T1003.001	Збір облікових даних з пам’яті.
Defense Evasion	Obfuscated Files	Obfuscated PowerShell Script	T1027.002	Використання шифрування або маскування команд.

Command and Control	C2 Communication	Web Protocols	T1071.001	З'єднання з сервером управління через HTTP(S).
Exfiltration	Data Exfiltration	Exfiltration Over Web Service	T1567.002	Витік даних через веб-запит до зовнішнього ресурсу.

На рис. 1 показано діаграму взаємозв'язку, яка ілюструє послідовні дії зловмисника – від фішингової атаки до витоку даних – через взаємодію між користувачем, системними компонентами (email-сервер, PowerShell, AD), і зовнішнім C2-сервером.

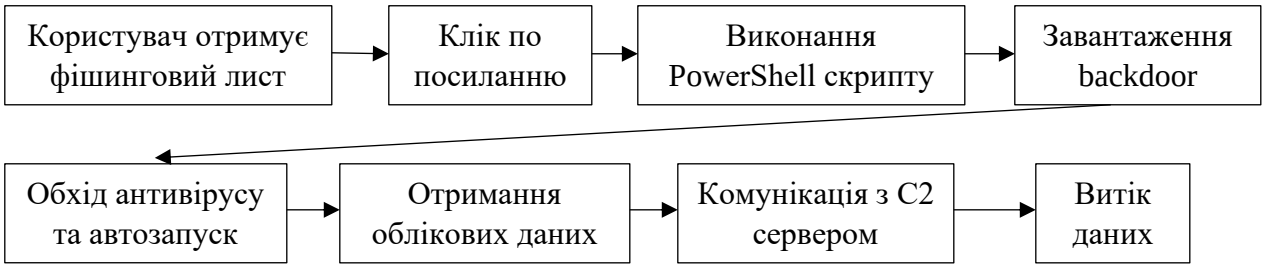

Рисунок 1 – Діаграму взаємозв'язку

Діаграми взаємозв'язку – це потужний інструмент аналізу та візуалізації кіберінцидентів, який дозволяє краще зрозуміти, що сталося, як, і які наслідки має атака. Вони особливо корисні при використанні в комбінації з моделями STRIDE, ATT&CK чи Kill Chain.

У результаті дослідження було доведено, що попереднє моделювання інцидентів дозволяє скоротити час виявлення до 40%, а також зменшити навантаження на аналітиків за рахунок автоматизації частини аналізу.

Висновки. Моделювання інцидентів кібербезпеки є надзвичайно ефективним інструментом у процесі розслідування та реагування. Воно дозволяє не лише зрозуміти механізм атаки, а й запобігти її повторенню.

На основі проведених досліджень можна зробити такі висновки:

- Використання фреймворків типу ATT&CK дозволяє стандартизувати підходи до розслідувань.
- Моделювання інцидентів значно покращує швидкість та точність аналізу.

У майбутньому слід розвивати напрямок симуляційного тестування систем безпеки, поєднуючи моделі з штучним інтелектом для передбачення складних атак.

ЛІТЕРАТУРА

1. Threatmodeler. Getting Started with Threat Modeling: How to Identify Your Mitigation Strategy. URL: https://threatmodeler.com/getting-started-with-threat-modeling-how-to-identify-your-mitigation-strategy/
2. Гапон А. О. Підходи до побудови моделі загроз для аналізу безпеки відкритого програмного кода / А. О. Гапон, В. М. Федорченко, А. О. Поляков // Системи обробки інформації. 2020. Вип. 1. С. 128-135.
3. Державна служба спеціального зв'язку та захисту інформації України: URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
4. Полотай О.І. Використання комп'ютерної криміналістики для забезпечення ефективного розслідування інцидентів інформаційної та кібербезпеки. Вісник ЛДУБЖД : зб. наук. праць. Львів : ЛДУБЖД, 2023. № 28. С. 73–80.