КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.891
УДК 004.056.53

Драгунцов Роман Ігорович
аспірант, Інститут проблем моделювання
в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна
ORCID ID: 0000-0002-1781-7530
draguntsow@yahoo.com

Зубок Віталій Юрійович
доктор наук, старший дослідник, старший науковий співробітник,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
Київ, Україна
ORCID ID: 0000-0002-6315-5259
vitaly.zubok@gmail.com

ДИНАМІЧНІ ІНФРАСТРУКТУРНІ КОМПОНЕНТИ ТА ВИДИМІСТЬ СИСТЕМИ ПІД ЧАС РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ

Анотація. Стійкість інфраструктури кібербезпеки є критично важливою для захисту активів підприємства, оскільки відключення електроенергії та подібні масштабні джерела невизначеності становлять суттєву й часто недооцінену загрозу. Такі збої можуть порушити функціонування ключових механізмів моніторингу та логування, що призводить до втрати критичних даних і значного простою систем. Особливий вплив відключень позначається на динамічних компонентах систем, таких як пристрої, динамічною конфігурацією мережевого стеку, конфігурації в оперативній пам'яті, які вразливі через свою волатильну природу. Мета дослідження: У статті розглядаються різнорідні наслідки відключень електроенергії в інформаційних системах для динамічних компонентів, з акцентом на те, як ці збої впливають на ширші аспекти роботи системи безпеки, зокрема на здатність реагувати на кіберінциденти. Методи: Шляхом оцінки динамічних властивостей і формалізації низки ключових характеристик динамічних компонентів, автори прагнуть покращити маркування даних та планування реагування на інциденти, підвищуючи ефективність оцінки динамізму системи та його впливу на робочі процеси інфраструктури й здатність до кіберреагування. Результати: Запропоновано аналіз наслідків відключень електроенергії для динамічних об'єктів і окреслено підходи до підвищення стійкості систем та мінімізації ризиків у сфері кібербезпеки, пов'язаних із втратою видимості динамічних компонентів. Висновки: Динамічні компоненти інфраструктури є вразливою ланкою архітектури захисту в умовах обмеженої видимості. Розглянуті в дослідженні аналітичні моделі є корисними для виявлення потенційного впливу динамічних компонентів на видимість системи. Наразі існує потреба в розробці прикладної моделі, яка буде придатною для практичного маркування даних і планування реагування на інциденти.

Ключові слова: кібербезпека; кіберстійкість; видимість системи; реагування на кіберінциденти; динамічна інфраструктура; теорія керування;.

ВСТУП

Постановка проблеми. Сучасні складні інфраструктури стикаються зі значними ризиками, серед яких відключення електроенергії становлять критичну, але часто недооцінену загрозу. Такі збої можуть спричинити суттєву втрату видимості та спостережності, що глибоко впливає на кібербезпекову стійкість організації — особливо з огляду на об'єкти динамічного характеру.

У типових випадках відключення електроенергії порушується робота ключових механізмів моніторингу та логування, що призводить до втрати журналів подій та

операційних даних, а також викликає простій систем безпеки. Без безперервної роботи цих механізмів організації втрачають можливість виявлення, реєстрації та реагування на потенційні кіберінциденти в реальному часі [6].

Найбільший вплив спостерігається на динамічні компоненти систем, зокрема пристрої з DHCP-конфігурацією, волатильні конфігурації, налаштування в оперативній пам'яті (RAM) [6], динамічну маршрутизацію та інші компоненти з несталою природою. Ці об'єкти є вразливішими через транзитний характер інформації, яку вони обробляють. Відключення електроенергії може призвести до миттєвої втрати критичних конфігураційних даних і цілісності системи, що викликає збої в мережевій інфраструктурі, зокрема конфлікти IP-адрес, помилкові мережеві призначення та відмову динамічних механізмів маршрутизації. Окрім того, очищення оперативної пам'яті (RAM) ускладнює потенційне розслідування, обмежуючи можливості відновлення даних після інциденту [6].

Такі збої поширюють свій вплив і на ширші процеси безпеки. Наприклад, ізоляція критичних систем від засобів захисту через переривання VPN-тунелів може нівелювати захисні заходи, залишаючи критично важливі активи беззахисними [2]. Крім того, порушення роботи систем «приманок» (deception systems) через конфлікти, викликані динамічним призначенням мережевих адрес, може спричинити хибні спрацювання або дозволити реальним атакам залишитися непоміченими, що додатково ускладнює ситуацію у сфері безпеки.

Аналіз останніх досліджень і публікацій. Останні дослідження досліджуваної тематики дозволяють у реальному часі відтворювати стан електромережі та застосовувати адаптивні стратегії виявлення аномалій і пом'якшення наслідків під час відключень електропостачання [7]. Паралельно розроблені концепції мікромереж, які використовують IoT та блокчейн, сприяють децентралізованому обміну енергією та гарантують цілісність даних у разі втрати зв'язку з центральною системою [8]. В розрізі підтримки інфраструктури кіберзахисту, дослідження інтелектуальних SCADA-архітектур акцентують увагу на інтеграції циклів адаптивного керування й розглядать застосування IDS для підтримки функцій моніторингу всупереч перебоям живлення [9]. Даний підхід застосовується для промислових систем, і, як і більшість існуючих досліджень, фокусуються саме на підтримці кібербезпеки електрогенеруючих та розподільчих потужностей. В розрізі оцінки впливу відключень електропостачання, публікації з аналізу волатильної пам'яті висвітлюють труднощі збору та аналізу RAM-конфігурацій, які втрачаються внаслідок раптових відключень, що ускладнює подальші розслідування [10]. Важливим дослідженням в розрізі оцінки впливу масових відключень електропостачання на кібербезпеку окремих інфраструктур є розгляд застосування зловмисниками вимкнення електропостачання для підтримки зниженої видимості під час кібератак — таким чином, в процеси моніторингу та реагування вносяться хибні дані, що сповільнює реагування на інциденти [11]. Однак, в розглянутих дослідженнях відсутні методології для маркування динамічних компонентів з метою автоматизації та оптимізації процесів реагування на інциденти.

Метою цієї статті є глибше дослідження проблематики впливу відключень електроенергії на безпеку динамічних об'єктів, запропонувавши аналіз наслідків таких збоїв в описаних умовах. Наступні розділи міститимуть аналіз змодельованих сценаріїв втрати видимості динамічних компонентів, її впливу на реагування на кіберінциденти, а також можливих підходів до оцінки властивостей динамічності об'єктів.

АСПЕКТИ ВИДИМОСТІ ДИНАМІЧНИХ СТРУКТУР

У цій статті широко використовується термін “динамічна структура” або волатильний об’єкт для позначення певного типу об’єктів, які залежать від енергетичного стану системи та можуть змінюватися або знищуватися в разі зміни цього стану. Нижче наведено табл. 1, у якій описано різні об’єкти динамічної інфраструктури з акцентом на їхню роль у забезпеченні кібербезпеки та потенційні наслідки відключень електроенергії для цих систем.

Таблиця 1

Динамічні об’єкти інфраструктури та їхній вплив на кібербезпеку

Тип об’єкта	**Опис об’єкта**	**Приклад використання в контексті безпеки**	**Можливий розширений вплив на безпеку об’єкта та пов’язаної інфраструктури в разі відключення живлення**
Об’єкти з конфігурацією DHCP	Пристрої та програмне забезпечення, які отримують IP-конфігурацію від DHCP-сервера.	Автоматичне призначення IP-адрес пристроям у мережі.	Втрата IP-конфігурації під час відключення живлення може призвести до мережевих збоїв, IP-конфліктів і потенційного несанкціонованого доступу до невірно призначених адрес або конфігурацій за замовчуванням. Зміни в адресному розподілі у системах Deception можуть спричинити хибні спрацювання. Кешовані дані DNS і IP-інформація SIEM можуть ускладнити аналіз під час інциденту.
Кеш в оперативній пам’яті	Тимчасові області зберігання в RAM, що використовуються для прискорення процесів отримання даних.	Кешування даних аутентифікації користувача для пришвидшення процесу авторизації.	Втрата кешованих даних може зробити агенти аутентифікації недоступними через завершення терміну дії облікових даних, що потребуватиме взаємодії з користувачем і може вплинути на загальну доступність системи. Форензика значною мірою залежить від аналізу кешованих даних, що зумовлює вплив на можливості відновлення після інциденту.
Волатильні конфігурації в оперативній пам’яті	Налаштування і стани, що зберігаються в RAM та не записуються у постійну пам’ять.	Зміни конфігурації під час роботи в мережевих пристроях.	Відключення живлення може призводити до втрати конфігурацій, викликаючи повернення до застарілих або стандартних налаштувань під час перезапуску. Це створює операційні невідповідності, порушення в безпекових протоколах і подовжує простої системи.

Динамічні маршрути	Маршрути, що змінюються в режимі реального часу відповідно до змін у мережі.	Адаптивна маршрутизація на основі трафіку та умов у мережі.	Порушення динамічної маршрутизації під час збоїв живлення може призвести до втрати або неправильної маршрутизації пакетів даних. Це шкодить цілісності мережі, призводить до відмови в обслуговуванні, особливо в реальному часі.
VPN-тунелі	Захищені з'єднання, встановлені через Інтернет, що з'єднують дві мережі.	Захищений віддалений доступ до корпоративної мережі.	Відключення живлення спричиняє обрив VPN-тунелів, що потребує повторної аутентифікації та встановлення з'єднання, що значно затримує безпечну комунікацію. Також можливе зниження стабільності мережі.
Дані в оперативній пам'яті (RAM)	Дані, що тимчасово зберігаються в RAM під час активних сесій.	Зберігання ключів дешифрування під час сесії.	Будь-яке відключення живлення призводить до повного стирання даних у RAM, що унеможливлює відновлення сесійно-залежних даних, таких як ключі шифрування, сеансові токени або відкриті з'єднання. Це значно ускладнює процес розслідування іцниденту.

Очевидно, що в IT-інфраструктурі може існувати більше прикладів волатильних об'єктів, однак згадані вище мають вимірюваний і зрозумілий вплив у процесі реагування на кіберінциденти в умовах втрати видимості.

ЗМІНИ ДИНАМІЧНИХ КОМПОНЕНТІВ У КОНТЕКСТІ ТЕОРІЇ КЕРУВАННЯ

Як зазначалося раніше, ми виходимо з припущення, що ефективність реагування на кіберінциденти значною мірою залежить від можливостей видимості та спостережуваності досліджуваної інфраструктури. У теорії керування поширеним способом представлення динаміки системи є використання моделей у просторі станів, які забезпечують математичну основу для моделювання та аналізу систем, що описуються системами диференціальних рівнянь першого порядку:

$$\begin{aligned} x(t) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t) + Du(t) \end{aligned} \quad (1)$$

де $x(t)$ — вектор стану, що представляє атрибути системи в момент часу t; $u(t)$ — вектор вхідних впливів (керування); $y(t)$ — вектор вихідних спостережуваних величин. Матриці A, B, C, D визначають динаміку системи та зв'язки між її входами, станами й виходами. Спостережуваність — це характеристика, що відображає здатність визначити внутрішні стани системи на основі знань про її зовнішні виходи. Математичною умовою спостережуваності лінійної системи є вимога, щоб матриця спостережуваності:

$$O = \begin{bmatrix} C \\ C\,A \\ C\,A^2 \\ . \\ . \\ . \\ CA^{n-1} \end{bmatrix} \quad (2)$$

мала повний ранг. Тут n — кількість станів системи. Якщо ця матриця має повний ранг, початковий стан системи може бути точно визначений на основі вихідних даних, зібраних за скінчений проміжок часу.

Для динамічного відстеження стану системи в часі використовується фільтр Кальмана — оптимальна метрика, що дозволяє визначити внутрішні змінні стану процесу навіть за умов вимірювань з похибками.

Проблема, яка виникає при комбінації динамічних об'єктів, відключення електроенергії та втрати видимості, полягає в тому, що певний об'єкт може змінити свій стан та набути атрибути, які раніше належали іншому об'єкту. Позначимо стан системи в момент часу t as x^t де x^t — це вектор, що включає всі відстежувані атрибути системи. Припустімо, що існує інший об'єкт (або той самий об'єкт у попередній момент часу), стан якого було зафіксовано як $x(s)$ у момент часу s (де $s < t$ Для вимірювання близькості між x^t і $x(s)$ до того, як вони стануть ідентичними, можна використовувати метрики відстані, наприклад евклідову відстань. Якщо дані доступні у вигляді часових рядів, можуть застосовуватись методи, такі як крос-кореляція, для виявлення часової затримки t−s при якій стани максимально подібні, що вказує на точку потенційного злиття атрибутів.

Однак такі методи є складними у впровадженні та рідко застосовуються в реальних інфраструктурних умовах.

Незважаючи на те, що математична модель динамізму системи у термінах теорії керування може бути достатньо точною для побудови надійної методологічної основи зменшення невизначеності в нестабільних системах, наразі ми не маємо достатньої кількості прикладних досліджень у цьому напрямі. Планується розробка такого фреймворку, підкріпленого ґрунтовною теоретичною базою, однак на даний момент у роботі переважають спостережувальні методи та обробка аналітичних моделей з метою оцінки впливу динамічних об'єктів на стійкість системи під час втрати живлення.

ВІДКЛЮЧЕННЯ ЕЛЕКТРОЕНЕРГІЇ ТА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Для оцінки фактичного впливу, якого зазнає процес реагування на кіберінциденти через втрату видимості динамічних компонентів, ми аналізуємо та моделюємо сценарії впливу відключення електроенергії на різні типи динамічних об'єктів.

Об'єкти з конфігурацією dhcp

У мережевому середовищі, налаштованому з використанням протоколу DHCP (Dynamic Host Configuration Protocol), стійкість і стабільність мережі можуть бути серйозно порушені внаслідок відключення електроенергії, особливо якщо таке відключення зачіпає DHCP-сервери або керовані ними пристрої. За нормальних умов DHCP-сервер призначає IP-адреси та інші параметри мережевої конфігурації пристроям у мережі, забезпечуючи унікальність адрес та ефективну комунікацію. Однак у разі відключення електроенергії можуть виникнути численні точки відмови, що призводять

до конфліктів IP-адрес — ситуації, коли кілька пристроїв отримують одну й ту ж IP-адресу, що спричиняє значні збої в мережевій взаємодії [4].

Коли стається відключення електроенергії, пристрої, яким раніше були присвоєні IP-адреси DHCP-сервером, можуть вимикатися, а після повторного ввімкнення — втрачати свою попередню конфігурацію. Одночасно, якщо сам DHCP-сервер перезапускається або тимчасово виходить з ладу через перебої в живленні, його база даних активних оренд (lease), яка відстежує, які IP-адреси використовуються, а які — вільні, може повернутися до застарілого стану або бути повністю втраченою у випадку відсутності належного резервного копіювання. Після повторного ввімкнення пристрої надсилають запити на призначення IP-адрес, і DHCP-сервер, працюючи з потенційно пошкодженою або застарілою інформацією, може повторно видати вже зайняту IP-адресу іншому пристрою.

Ця проблема ускладнюється в масштабних мережах або в середовищах, де IP-конфігурації критично важливі для функціонування пристроїв, як-от у дата-центрах чи великих корпоративних мережах. Наслідки конфліктів адрес можуть варіюватися від незначних порушень з'єднання до серйозних порушень безпеки, оскільки дані, призначені для одного пристрою, можуть помилково надходити до іншого.

Технічно проблема виглядає наступним чином: коли пристрій (наприклад, мережевий принтер або робоча станція), який використовує DHCP, повертається до роботи після відключення живлення, він ініціює запит на конфігурацію за допомогою DHCP Discover. Якщо DHCP-сервер не встиг належним чином синхронізувати свою базу оренд через збій, він може надіслати DHCP Offer із IP-адресою, яка вже використовується іншим пристроєм. Як тільки обидва пристрої починають працювати в мережі, виникає конфлікт, оскільки мережевий трафік, адресований одному IP, може потрапити до неправильного пристрою, що призводить до втрати даних або перерви в обслуговуванні.

Виникнення невідповідностей IP-адрес унаслідок відключення електроенергії створює серйозні труднощі для форензичного аналізу логів, особливо при спробах відстежити активність, пов'язану з конкретними пристроями в мережі. В описаній вище ситуації в журналах може фігурувати один і той самий фізичний пристрій під різними IP-адресами в різний час. Такий стан речей ускладнює точну ідентифікацію та кореляцію мережевої активності із конкретними пристроями — критично важливий процес у розслідуванні інцидентів безпеки та аномалій у мережі.

З технічної точки зору, лог-записи, які зазвичай дозволяють відстежити дії пристрою в мережі, стають фрагментованими. Наприклад, мережевий принтер може бути зафіксований у логах безпеки як такий, що звертається до певних ресурсів під однією IP-адресою, а після відключення електроенергії той самий принтер може знову з'явитися, але вже під іншою адресою, виконуючи подібні дії. Такі розбіжності можуть ввести в оману аналітиків, які сприйматимуть ці записи як активність декількох різних пристроїв, тоді як насправді йдеться про один пристрій, що змінив адресу внаслідок повторного призначення DHCP.

Кеш в пам'яті

Кеш в оперативній пам'яті (in-memory cache) зазвичай зберігає дані у вигляді волатильних, тимчасових сутностей у RAM системи. Така архітектура забезпечує швидкий доступ до даних і можливість їх оперативної обробки, що є ідеальним для високопродуктивних застосунків, які потребують мінімальної затримки у відповіді. Однак через волатильну природу оперативної пам'яті всі дані в кеші втрачаються при

вимкненні живлення пристрою. Наслідки цього можуть бути масштабними, особливо для систем, які покладаються на кеш для забезпечення як продуктивності, так і цілісності даних.

У якості модельного прикладу розглянемо вебзастосунок, що використовує Redis — широко розповсюджену систему зберігання структур даних в оперативній пам'яті, яка виконує функції бази даних, кеша та брокера повідомлень. Redis підвищує продуктивність застосунку шляхом кешування часто використовуваних даних, таких як інформація про сесії користувачів, фрагменти вебсторінок або дані аналітики в реальному часі. За нормальних умов така архітектура значно скорочує час відповіді та зменшує навантаження на основну базу даних.

Проте в разі відключення електроенергії всі дані, збережені в Redis, будуть втрачені, якщо система не налаштована на періодичне збереження даних на диск. Якщо останні зміни не були збережені перед збоєм, усі зміни, які існували лише в кеші, буде втрачено. Така втрата може призвести до порушення функціональності застосунку, несумісностей між кешем і базою даних після відновлення живлення, а також до погіршення досвіду користувачів.

Крім того, після перезапуску системи внаслідок вимкнення живлення зазвичай відбувається так зване «прогрівання кешу» (cache warm-up) — період, протягом якого кеш поступово наповнюється необхідними даними. У цей період може спостерігатися зростання навантаження на бекенд-бази даних і зниження продуктивності застосунку до моменту, коли кеш досягне оптимального стану.

Кеш в оперативній пам'яті нерідко містить критичні дані безпеки — такі як журнали в реальному часі, інформація про сесії та статус активних транзакцій — які є важливими для оперативного виявлення загроз та їх аналізу. Втрата таких даних може створити значну «сліпу зону» в можливостях моніторингу. Постінцидентна форензика значною мірою спирається на наявність детальних логів та інших артефактів, які можуть тимчасово зберігатися в оперативній пам'яті для швидкого доступу. Якщо відключення електроенергії призводить до втрати цієї інформації, це суттєво ускладнює роботу аналітиків: їм буде важко відстежити дії зловмисників, визначити точки проникнення й оцінити масштаб шкоди. Брак детальних форензичних даних також негативно впливає на загальні можливості організації з підтримання видимості [12].

Волатильна конфігурація в пам'яті

Використання динамічних конфігурацій в оперативній пам'яті (RAM) створює значні експлуатаційні вразливості через волатильний характер цієї пам'яті. Застосування волатильних конфігурацій є широко поширеним з метою оптимізації продуктивності системи та динамічного налаштування робочих параметрів. Проте дані, що зберігаються в оперативній пам'яті, за своєю природою несталі — вони не зберігаються у разі втрати живлення або неочікуваного завершення роботи системи [12].

Ця волатильність створює фундаментальну проблему: зникнення критично важливих конфігураційних даних у разі вимкнення живлення, що вимагає реалізації складних механізмів відновлення для повернення системи до її стану, який передував аварійному відключенню [1].

Щоб абстрагувати зазначену проблему у вигляді гіпотетичного сценарію, розглянемо систему, у якій конфігураційні параметри $C(t)$ змінюються в реальному часі на основі операційного зворотного зв'язку та зберігаються виключно в волатильній пам'яті. Операційний стан системи в будь-який момент часу t критично залежить від цих параметрів і позначається як $S(t)$, причому $S(t) = g(C(t))$, де g це операційні процеси

системи. Якщо відключення живлення відбувається в момент часу t_1, що призводить до втрати $C(t_1)$, система в момент часу t_2 (після відновлення живлення) стикається з критичною проблемою. Функція відновлення f, має реконструюватиC(t_2) імовірно, з використанням альтернативних джерел даних або типових налаштувань, що безпосередньо впливає на поточний операційний стан $S(t_2)$.

У контексті мережевої безпеки конфігурації міжмережевих екранів є наочним прикладом того, як динамічні конфігурації в оперативній пам'яті є водночас критичними та вразливими до відключення електроенергії. Правила iptables, що використовуються для налаштування, підтримки та перегляду таблиць фільтрації IP-пакетів у ядрі Linux, зазвичай зберігаються в волатильній пам'яті. Така архітектура дозволяє оперативно змінювати правила міжмережевого екрану відповідно до актуальних потреб безпеки мережі, але водночас означає, що ці правила не зберігаються автоматично після перезавантаження системи або зникнення живлення. Наприклад, iptables може бути налаштований для обмеження доступу до певних портів або керування трафіком між окремими сегментами мережі. Такі правила завантажуються безпосередньо в оперативну пам'ять, де використовуються мережею ядра системи.

У разі відключення електроенергії поточний стан правил iptables може бути втрачено, якщо їх не було збережено на енергонезалежному носії до настання збою. Після перезавантаження система може застосувати набір iptables за замовчуванням, який суттєво відрізняється від попередньо активних правил. Така невідповідність може призвести до тимчасової відсутності захисту або до непередбачуваної поведінки системи, відкриваючи можливості для порушення безпеки або порушень у роботі.

Цю ситуацію доцільно розглядати крізь призму стійкості системи, цільових показників часу відновлення (RTO) та цілісності заходів безпеки під час фази відновлення. Динамічні конфігурації відіграють важливу роль у формуванні правил міжмережевого екрану, які захищають систему від несанкціонованого доступу та атак. У разі відключення живлення втрата цих конфігурацій може суттєво послабити захисні механізми, що робить систему вразливою до атак у критичний момент, коли інші компоненти системи також можуть перебувати у стані відновлення.

З позиції реагування на кіберінциденти, це підвищує рівень операційного ризику: системастикається не лише з наслідками перебою живлення, а й з потенційними загрозами безпеці за умов ослаблених механізмів захисту.

У науковому контексті цілісність заходів безпеки у фазі відновлення має вирішальне значення. Зазвичай динамічні конфігурації міжмережевих екранів є частиною адаптивної кібербезпеки, що підлаштовується до поточних загроз. Якщо ці правила не буде відновлено до стану, що передував відключенню, або не буде здійснено оперативного налаштування у відповідь на поточні інциденти, ефективність реагування на кіберінциденти може суттєво знизитися.

Підсумовуючи наведений аналіз: втрата динамічної конфігурації системи має менший вплив на видимість, але може суттєво знизити ефективність реагування на кіберінциденти.

Динамічні маршрути

Як окремий випадок волатильних конфігурацій в оперативній пам'яті, динамічна маршрутизація відіграє критично важливу роль в ефективному управлінні трафіком шляхом автоматичного коригування маршрутів відповідно до змін у топології мережі. Проте така динамічність створює суттєві вразливості у разі відключення електроенергії. Зокрема, втрата конфігурацій динамічних маршрутів може спричинити порушення

роботи мережі та зниження рівня видимості, що серйозно впливає на процес реагування на кіберінциденти.

Протоколи динамічної маршрутизації, такі як OSPF (Open Shortest Path First) або BGP (Border Gateway Protocol), зберігають інформацію про маршрути в оперативній пам'яті. У разі відключення живлення маршрутизатори можуть втратити цей важливий стан. Після відновлення живлення повторна ініціалізація маршрутів залежить від специфікацій відповідного протоколу та поточного стану інших вузлів мережі. Цей процес може бути тривалим і схильним до помилок, особливо якщо конфігурації не були збережені або зберігалися лише періодично.

Розглядаючи змодельований сценарій, наближений до реальних умов, передбачається наступна ситуація: одразу після відключення електроенергії, під час перезавантаження маршрутизаторів, відсутність попередньої динамічної інформації про маршрутизацію призводить до неправильного або неоптимального маршрутизаційного рішення. Це може спричинити появу так званих «мережевих чорних дір», у яких пакети даних втрачаються або спрямовуються хибно, знижуючи оперативну видимість у мережі. Порушення даних динамічної маршрутизації також може викривити загальний обмін трафіком, що ускладнює виявлення зловмисної активності або спроб несанкціонованого доступу.

Ефективність реагування на кіберінциденти значною мірою залежить від здатності швидко ізолювати уражені системи та перенаправити трафік до безпечних сегментів мережі. За умов порушеної маршрутизації процес реагування може бути сповільнений, оскільки мережа не здатна коректно застосувати політики або перенаправити трафік згідно з очікуванням. Крім того, непослідовність у маршрутизаторській інформації може призводити до розривів у сегментації мережі та покритті засобами моніторингу.

VPN-тунелі

VPN-з'єднання, зокрема ті, що залежать від безперервного живлення та стабільності мережі, є вразливими до збоїв, спричинених відключеннями електроенергії. У разі такого відключення встановлені VPN-тунелі можуть припинити своє функціонування [3], що запускає каскад безпекових та операційних проблем, які суттєво підривають цілісність системи та здатність організації ефективно реагувати на кіберінциденти.

VPN-технології відіграють ключову роль у забезпеченні безпечних каналів зв'язку між різними частинами мережі, часто інкапсулюючи трафік з численних кінцевих точок до центральних систем, що обробляють конфіденційні дані. У випадку обриву VPN-тунелів розриваються зашифровані канали, які захищають ці дані, що потенційно відкриває можливості для перехоплення або модифікації конфіденційних транзакцій. Такий розрив цілісності системи створює умови для атак, що використовують відсутність шифрування для проведення витоків даних або атак типу «людина посередині» (man-in-the-middle).

VPN часто реалізують політики мережевої безпеки, включаючи контроль доступу та маршрутизовані заходи захисту. Раптове припинення роботи VPN-тунелів може призвести до втрати цих функцій, залишаючи раніше захищені активи доступними без необхідної перевірки безпеки. Наприклад, системи, що покладаються на специфічну маршрутизацію IP-трафіку через VPN для застосування правил міжмережевих екранів або систем виявлення вторгнень, можуть втратити зв'язок із сегментами мережі, які потребують захисту.

Ефективність реагування на кіберінциденти також може знижуватися через часткову ізоляцію мережі, спричинену деградацією тунелів. Це може призводити до затримки у виявленні та стримуванні загроз, підвищуючи загальний рівень ризику в критичні періоди.

RAM data

На відміну від пристроїв постійного зберігання, таких як SSD або жорсткі диски, дані, що зберігаються в оперативній пам'яті (RAM), зникають після вимкнення пристрою або втрати живлення. Ця особливість RAM може суттєво ускладнити форензичний аналіз, особливо в контексті розслідування вторгнень та кібератак. В оперативній пам'яті зазвичай зберігається критично важлива інформація про системні процеси, мережеві з'єднання та дії користувачів — все це має високу цінність для аналізу інцидентів [6].

Під час реагування на кіберінциденти експерти з цифрової криміналістики значною мірою покладаються на ці волатильні дані, щоб отримати уявлення про стан системи в момент інциденту. Вони допомагають встановити, які дії були здійснені зловмисниками на скомпрометованій системі. У випадку відключення живлення вміст RAM миттєво стирається, що призводить до втрати цієї короткочасної, але критично важливої інформації. Така втрата суттєво обмежує можливості фахівців у встановленні дій зловмисників або точному визначенні масштабу порушення.

Відсутність даних з оперативної пам'яті створює значні прогалини у хронології подій, що ускладнює відновлення послідовності дій до, під час та після інциденту безпеки [12].

У таких випадках розслідування змушене спиратися винятково на менш волатильні джерела, такі як жорсткі диски або журнали з мережевих пристроїв, які можуть не фіксувати всі релевантні дії або найостанніші зміни в системі. Наприклад, зловмисне програмне забезпечення, що повністю функціонує в оперативній пам'яті та не залишає суттєвих слідів на диску, є особливо складним для аналізу після зникнення живлення. Аналогічно, інформація про відкриті мережеві з'єднання або активні сесії користувачів, яка могла б надати важливий контекст інциденту, втрачається, що унеможливлює повне розуміння масштабу й природи порушення.

ДИНАМІЧНІ КОМПОНЕНТИ ПІД ЧАС РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В УМОВАХ НЕСТАБІЛЬНОГО ЕНЕРГОЗАБЕЗПЕЧЕННЯ — ПІДСУМКОВИЙ ОГЛЯД АСПЕКТІВ

Динамічні компоненти за своєю природою створюють труднощі для повноцінного ведення обліку в рамках інформаційно-безпекових платформ, що істотно впливає на подальшу ефективність реагування на кіберінциденти. На основі детального аналізу поведінки динамічних елементів інфраструктури під час відключень електроенергії очевидним є те, що необхідно враховувати певні критично важливі відмінності між цими компонентами. Відповідні атрибути наведено в табл. 2.

Таблиця 2

Атрибути динамічних об'єктів, які визначають їхній вплив на видимість інфраструктури

Повнота динамічної природи	Властивість класу компонентів, що визначає, чи змінює об'єкт усі свої атрибути під час зміни стану енергоживлення системи, чи лише окремі, які не є критичними для інвентаризації або ідентифікації об'єкта, має вирішальне значення. Об'єкти можуть класифікуватися за ступенем динамічності: – Повністю динамічні — стан об'єкта до і після відключення живлення не має взаємозв'язку; – Частково динамічні — певні атрибути залишаються незмінними до та після відключення живлення, що дозволяє пов'язувати стани об'єкта. Ця класифікація є ключовою для розуміння та управління впливом енергетичних збоїв на компоненти системи.
Здатність до стабілізації	Властивість класу компонентів або конкретного об'єкта, що визначає здатність змінити свій динамічний статус на стабільний, тобто гарантує незмінність загального стану та важливих атрибутів до та після відключення живлення.
Повнота знищення об'єкта	Властивість класу компонентів, яка визначає поведінку об'єкта під час відключення живлення — чи буде об'єкт повністю знищено, чи є можливість його часткового або повного відновлення.
Можливість фіксації знищення компонента	Властивість класу компонентів, яка визначає здатність підтвердити факт знищення конкретного об'єкта після відключення живлення, є критично важливою для оцінки стійкості системи. Ця властивість гарантує, що існування об'єкта після інциденту не може бути підтверджене без наявності відповідного механізму. Якщо компонент не має цієї властивості, перевірити наявність або працездатність об'єкта після збоїв у живленні неможливо, що підкреслює необхідність урахування цієї характеристики під час проєктування критичних архітектур систем для збереження цілісності та безперервності їх функціонування.
Можливість фіксації знищення компонента	Властивість класу компонентів, яка визначає здатність підтвердити факт знищення конкретного об'єкта після відключення живлення, є критично важливою для оцінки стійкості системи. Ця властивість гарантує, що існування об'єкта після інциденту не може бути підтверджене без наявності відповідного механізму. Якщо компонент не має цієї властивості, перевірити наявність або працездатність об'єкта після збоїв у живленні неможливо, що підкреслює необхідність урахування цієї характеристики під час проєктування критичних архітектур систем для збереження цілісності та безперервності їх функціонування.

Зазначені висновки були сформульовані на основі обробки аналітичних моделей, що ґрунтуються на сценаріях із реального середовища. Наведені вище властивості можуть бути використані для опису будь-якого інфраструктурного об'єкта, проте, якщо вони визначені для компонентів динамічної системи, це дозволяє сформувати цілісну модель, яка дає змогу вимірювати потенційний вплив на видимість і стійкість системи під час відключення електроенергії, особливо в умовах активного реагування на кіберінцидент. Ці властивості повністю охоплюють такі аспекти:

- Масштаб динамічних об'єктів в інфраструктурі — оцінка співвідношення повністю динамічних, статичних і частково динамічних об'єктів дозволяє прогнозувати потенційні втрати у видимості, що можуть негативно вплинути на реагування під час відключення електроенергії. Така оцінка допомагає краще зрозуміти ступінь вразливості системи в контексті динамічних компонентів.
- Стратегії пом'якшення ризиків — можливі дії для зменшення ризику повної втрати видимості через відключення живлення, включаючи визначення

атрибутів для ідентифікації та відстеження змінених об’єктів, застосування контрзаходів та зміни в інфраструктурі для зменшення кількості повністю динамічних об’єктів.

- Стратегії реагування — розуміння того, які об’єкти будуть повністю знищені при зникненні живлення і які судово-аналітичні дії стануть неефективними, дозволяє підвищити ефективність реагування.

Розуміння потенційних сценаріїв інцидентів — інтеграція аналітичних моделей для оцінки впливу відключень живлення на різні динамічні компоненти у поєднанні з класифікацією цих компонентів суттєво покращує процес планування реагування на інциденти та збагачує плани відновлення. Такий підхід дозволяє проактивно враховувати потенційні сценарії та оптимізувати процеси відновлення, забезпечуючи швидке відновлення сервісів і зниження ризиків

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У ході проведеного дослідження було розроблено формалізовані метрики для кількісної оцінки втрати видимості системи. Зокрема, розширено класичну матрицю спостережуваності лінійної системи, додавши змінні, що описують волатильність тих чи інших компонентів системи в розрізі впливу на їх спостережність відключень електропостачання. Розроблено математичну модель визначення динамізму системи та її окремих комонентів, яка може застосовуватись для розробки та впровадження стратегії реагування на інциденти кібербезпеки, оцінювати рівень довіри до отримуваних даних та оперативно приймати рішення щодо балансування зусиль в пост-інцидентному аналізі. На основі визначених метрик динамізму можлива розробка планів відновлення після інциденту — розподіл ресурсів для виконання відновлення компонентів, пріоритетного відновлення спостережності та контролів кібербезпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Динамічні компоненти інфраструктури є вразливою ланкою будь-якої архітектури захисту в умовах відключення електроенергії. Оцінити той вплив, який ці компоненти можуть мати на загальну складність реагування та втрату видимості під час кіберінциденту, є складним завданням як для типових, так і для специфічних сценаріїв, спричинених перебоями в живленні. Розглянуті в цій роботі аналітичні моделі сприяють ідентифікації таких загроз, а оцінка динамічних властивостей допомагає виявляти конкретні вразливості, пов’язані з втратою видимості через відключення живлення.

На даний момент нами розробляється практичний фреймворк, який буде придатний для реального маркування даних та планування реагування на інциденти. Цей фреймворк допоможе оцінити динамічний характер системи та його вплив на функціонування інфраструктури і процеси кіберреагування в умовах інциденту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Paar, K., & Harper, S. (2024, January 2). *Challenges and mitigations for data remanence in FPGA based systems*. Paper presented at the NDIA Michigan Chapter Ground Vehicle Systems Engineering and Technology Symposium, Michigan, USA.

2. Krause, T., Ernst R., Klaer B., Hacker I., Henze M.. (2021). Cybersecurity in power grids: Challenges and opportunities. *Sensors, 21*(18), 6225. https://doi.org/10.3390/s21186225
3. CheckPoint CheckMates. (n.d.). *Lost site-to-site VPN connection after power outage*. Retrieved September 30, 2024, from https://community.checkpoint.com/t5/SMB-Gateways-Spark/Lost-Site-to-Site-VPN-Connection-after-power-outage/td-p/215653
4. Siles, S. (n.d.). *Real world ARP spoofing*. GIAC. Retrieved September 30, 2024, from https://www.giac.org/paper/gcih/487/real-world-arp-spoofing/105411
5. Padmanabhan, R., Dhamdhere A., Aben Emile, Claffy K., Spring N. (2016). Reasons dynamic addresses change. In *Proceedings of IMC 2016: Internet Measurement Conference*, Santa Monica, CA, USA. https://doi.org/10.1145/2987443.2987461
6. Buquerin, K. K. G., Corbett, C., & Hof, H.-J. (2021, September 28). *Structured methodology and survey to evaluate data completeness in automotive digital forensics*. Paper presented at the 19th escar Europe – The World's Leading Automotive Cyber Security Conference, Ruhr region, Germany.
7. Salvi, A., Spagnoletti, P., & Noori, N. S. (2022). Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security*, *112*, 102507. https://doi.org/10.1016/j.cose.2021.102507
8. Sai Shibu, N. B., Devidas, A. R., Balamurugan, S., Ponnekanti, S., & Ramesh, M. V. (2024). Optimising Microgrid Resilience: Integrating IoT, Blockchain, and Smart Contracts for Power Outage Management. *IEEE Access*, 1. https://doi.org/10.1109/access.2024.3360696
9. Pricop, A.-I., GavrilaŞ, M., SĂlceanu, A., & Neagu, B.-C. (2023). Power systems resilience against cyber-attacks. A systematic analysis. У *2023 10th International Conference on Modern Power Systems (MPS)*. IEEE. https://doi.org/10.1109/mps58874.2023.10187420
10. Nyholm, H., Monteith, K., Lyles, S., Gallegos, M., DeSantis, M., Donaldson, J., & Taylor, C. (2022). The Evolution of Volatile Memory Forensics. *Journal of Cybersecurity and Privacy*, *2*(3), 556–572. https://doi.org/10.3390/jcp2030028
11. Yang, S., Lao, K.-W., Hui, H., & Chen, Y. (2024). Secure Distributed Control for Demand Response in Power Systems Against Deception Cyber-Attacks With Arbitrary Patterns. *IEEE Transactions on Power Systems*, 1–12. https://doi.org/10.1109/tpwrs.2024.3381231
12. Kapade, P., Pandey, A. K. (2018). Technical issues and challenges in memory forensics. *International Journal of Creative Research Thoughts (IJCRT)*, *6*(2).

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Roman Drahuntsov
PhD Student, G.E. Pukhov Institute for Modelling in
Energy Engineering of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0002-1781-7530
draguntsow@yahoo.com

Vitaliy Zubok
Dr.Sci., G.E. Pukhov Institute for Modelling in Energy
Engineering of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0002-6315-5259
vitaly.zubok@gmail.com

DYNAMIC INFRASTRUCTURE COMPONENTS AND SYSTEM VISIBILITY DURING CYBERSECURITY INCIDENT RESPONSE

Abstract. The resilience of cybersecurity infrastructure is critically important for protecting enterprise assets, as power outages and other large-scale sources of uncertainty represent a significant and often underestimated threat. Such disruptions can impair the functioning of key monitoring and logging mechanisms, resulting in the loss of critical data and substantial system downtime. Power outages have a particularly pronounced impact on dynamic system components, such as devices with dynamic network stack configurations and in-memory settings, which are vulnerable due to their volatile nature. Aim: This study examines the diverse consequences of power outages in information systems, with a focus on dynamic components and their effect on broader security system operations, particularly the capacity for cyber incident response. Methods: By evaluating the dynamic properties and formalizing several key characteristics of these components, the authors aim to improve data labeling and incident response planning, thereby enhancing the effectiveness of dynamism assessment and its impact on infrastructure workflows and cyber response capability. Results: The article presents an analysis of the consequences of power outages for dynamic objects and outlines approaches to increasing system resilience and minimizing cybersecurity risks associated with the loss of visibility of dynamic components. Conclusions: Dynamic components of infrastructure constitute a vulnerable link in the protection architecture under conditions of limited visibility. The analytical models discussed in this study are useful for identifying the potential impact of dynamic components on system visibility. There remains a need for the development of an applied model suitable for practical data labeling and incident response planning.

Keywords: cybersecurity; cyber resilience; system visibility; cyber incident response; dynamic infrastructure; control theory.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Paar, K., & Harper, S. (2024, January 2). *Challenges and mitigations for data remanence in FPGA based systems*. Paper presented at the NDIA Michigan Chapter Ground Vehicle Systems Engineering and Technology Symposium, Michigan, USA.
2. Krause, T., Ernst R., Klaer B., Hacker I., Henze M.. (2021). Cybersecurity in power grids: Challenges and opportunities. *Sensors, 21*(18), 6225. https://doi.org/10.3390/s21186225
3. CheckPoint CheckMates. (n.d.). *Lost site-to-site VPN connection after power outage*. Retrieved September 30, 2024, from https://community.checkpoint.com/t5/SMB-Gateways-Spark/Lost-Site-to-Site-VPN-Connection-after-power-outage/td-p/215653
4. Siles, S. (n.d.). *Real world ARP spoofing*. GIAC. Retrieved September 30, 2024, from https://www.giac.org/paper/gcih/487/real-world-arp-spoofing/105411
5. Padmanabhan, R., Dhamdhere A., Aben Emile, Claffy K., Spring N. (2016). Reasons dynamic addresses change. In *Proceedings of IMC 2016: Internet Measurement Conference*, Santa Monica, CA, USA. https://doi.org/10.1145/2987443.2987461

6. Buquerin, K. K. G., Corbett, C., & Hof, H.-J. (2021, September 28). *Structured methodology and survey to evaluate data completeness in automotive digital forensics*. Paper presented at the 19th escar Europe – The World's Leading Automotive Cyber Security Conference, Ruhr region, Germany.
7. Salvi, A., Spagnoletti, P., & Noori, N. S. (2022). Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security*, *112*, 102507. https://doi.org/10.1016/j.cose.2021.102507
8. Sai Shibu, N. B., Devidas, A. R., Balamurugan, S., Ponnekanti, S., & Ramesh, M. V. (2024). Optimising Microgrid Resilience: Integrating IoT, Blockchain, and Smart Contracts for Power Outage Management. *IEEE Access*, 1. https://doi.org/10.1109/access.2024.3360696
9. Pricop, A.-I., GavrilaŞ, M., SĂlceanu, A., & Neagu, B.-C. (2023). Power systems resilience against cyber-attacks. A systematic analysis. У *2023 10th International Conference on Modern Power Systems (MPS)*. IEEE. https://doi.org/10.1109/mps58874.2023.10187420
10. Nyholm, H., Monteith, K., Lyles, S., Gallegos, M., DeSantis, M., Donaldson, J., & Taylor, C. (2022). The Evolution of Volatile Memory Forensics. *Journal of Cybersecurity and Privacy*, *2*(3), 556–572. https://doi.org/10.3390/jcp2030028
11. Yang, S., Lao, K.-W., Hui, H., & Chen, Y. (2024). Secure Distributed Control for Demand Response in Power Systems Against Deception Cyber-Attacks With Arbitrary Patterns. *IEEE Transactions on Power Systems*, 1–12. https://doi.org/10.1109/tpwrs.2024.3381231
12. Kapade, P., Pandey, A. K. (2018). Technical issues and challenges in memory forensics. *International Journal of Creative Research Thoughts (IJCRT)*, *6*(2).