УДК 004.056.55:004.42:004.7
DOI: 10.31673/2409-7292.2025.030258

Бушков В.Г.

МОДЕЛЮВАННЯ СТІЙКОСТІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ ДО ГІБРИДНИХ КІБЕРАТАК: ПІДХОДИ ТА СЦЕНАРНИЙ АНАЛІЗ ВИТРИВАЛОСТІ ІНФРАСТРУКТУРИ

У статті досліджено підходи до моделювання стійкості електронних комунікацій до гібридних кібератак, які становлять зростаючу загрозу для критичної інформаційної інфраструктури в умовах сучасної кібергібридної війни. Основну увагу приділено застосуванню сценарного аналізу та імітаційного моделювання як засобів вивчення витривалості телекомунікаційних систем до комбінованих атак, що поєднують технічні (DDoS, routing attack, перехоплення трафіку) та інформаційно-психологічні (фішинг, маніпулятивний вплив) компоненти. Розроблено методику побудови гібридних сценаріїв та створено експериментальне середовище з використанням OMNeT++, Scapy (Python) та NetEm для тестування критичних умов експлуатації. В рамках дослідження проведено симуляцію кількох типових атак із фіксацією метрик якості обслуговування (QoS), часу відновлення (RTO) та структурної стійкості мережі. Встановлено, що поєднання інфраструктурного та когнітивного впливу може призвести до деградації функціональності до 50% та суттєвого збільшення часу відновлення, особливо у випадку відсутності резервних каналів та сегментації мережі. Результати дослідження можуть бути використані для проектування архітектур телекомунікацій з підвищеним рівнем стійкості, побудови цифрових двійників для превентивної оцінки ризиків, а також формування нормативної бази національного рівня у сфері забезпечення кіберстійкості критичної інфраструктури.

Ключові слова: гібридні загрози, електронні комунікації, сценарії атак, моделювання стійкості, кіберінфраструктура, витривалість мереж, імітація.

Вступ

У сучасних умовах геополітичної нестабільності, зокрема у Східній Європі, кіберпростір став повноцінним театром бойових дій, де цифрові загрози дедалі частіше комбінуються з традиційними військовими засобами. Зростання кількості гібридних кібератак, що поєднують технічні (інфраструктурні) та когнітивні (інформаційно-психологічні) компоненти, зумовлює потребу у фундаментально новому підході до проектування стійких систем електронних комунікацій [1]–[5]. Класичні засоби захисту – фаєрволи, IDS/IPS-системи, VPN – недостатні у ситуаціях, коли атака охоплює не лише мережеву інфраструктуру, а й людський фактор, знижуючи рівень довіри до каналів зв'язку [6], [7]. Такі гібридні впливи можуть паралізувати як фізичні вузли, так і логічні маршрути прийняття рішень у критичних інфраструктурах – від енергетики до державного управління [8], [9]. Особливої актуальності набуває моделювання витривалості систем електронних комунікацій у конфліктних регіонах, де поєднання DDoS, routing-атак, фішингу, дезінформації та інших сценаріїв вимагає симбіозу технічних, поведінкових та організаційних моделей [10-12]. Дане дослідження пропонує метод інтеграції сценарного аналізу гібридних впливів у процес моделювання витривалості інформаційно-комунікаційних систем (ІКС). Новизна полягає у поєднанні технічного і когнітивного рівнів атак у симуляційному середовищі з динамічною побудовою гібридних сценаріїв. На відміну від ізольованих моделей, тут враховується мультивекторність, часові залежності, зміна довіри та архітектурна деградація [13-15].

Дослідження в області DDoS-атак охоплюють їхню класифікацію, механізми поширення та стратегії пом'якшення (Cisco [16], ENISA [17]). Routing-атаки вивчаються у контексті BGP-маніпуляцій, перехоплення трафіку та GPS-spoofing [18], [19]. Гібридні моделі атак активно розглядаються у доповідях NATO STRATCOM [20] і дослідженнях RAND Corporation [21], де окреслюється зв'язок між кібервпливами та інформаційними операціями. У частині моделювання стійкості використовуються підходи на основі NIST SP 800-160 [22], ISO/IEC 27001 [23], а також пропозиції з resilience engineering [24-26]. Проте більшість з них не охоплює міждисциплінарну природу гібридних загроз.

Метою дослідження є побудова багатоаспектної моделі стійкості ІКС до гібридних атак, яка враховує комбіноване навантаження від технічних і соціотехнічних впливів, і дозволяє проводити симуляційні експерименти для оцінки показників витривалості.

Постановка проблеми

У сучасних реаліях розвитку телекомунікаційних систем критична інформаційна інфраструктура все частіше стає об’єктом гібридних кібератак, які поєднують технічні та когнітивні методи впливу. Традиційні підходи до забезпечення кіберстійкості, орієнтовані переважно на технічні засоби захисту, виявляються недостатніми у ситуаціях, коли надійність електронних комунікацій підривається не лише через технічні вразливості, але й за допомогою інформаційно-психологічних операцій. Дедалі більшої актуальності набувають сценарії, у яких противник синхронно використовує DDoS-атаки, routing manipulation, фішинг, дезінформацію та інші гібридні загрози для досягнення комплексного впливу на інфраструктуру та користувачів.

Відсутність цілісної методології моделювання стійкості електронних комунікацій до таких складних багатовекторних впливів ускладнює процес розробки адаптивних мережевих архітектур, здатних витримувати як потужні технічні атаки, так і маніпулятивний тиск на людський фактор. Більшість існуючих підходів не враховують міждисциплінарну природу загроз, часові залежності та динаміку деградації, що обмежує можливості превентивного аналізу ризиків та розробки ефективних стратегій захисту.

Таким чином, виникає необхідність у створенні багатоаспектної моделі стійкості інформаційно-комунікаційних систем до гібридних атак із залученням сценарного аналізу та імітаційного моделювання. Такий підхід має забезпечити не лише технічну оцінку стійкості, а й урахування психологічних, поведінкових та організаційних аспектів впливу на електронні комунікації в умовах сучасної кібергібридної війни.

Аналіз останніх досліджень і публікацій

Сучасні дослідження у сфері кіберстійкості критичної інфраструктури демонструють зміщення акцентів від суто технічного до міждисциплінарного підходу. У праці Алана Котта (Kott) та Крістофера Арнольда (Arnold) розглядаються когнітивні аспекти кібероборони, де наголошується на важливості врахування людських факторів у процесі моделювання захисту. Дослідження Тоні Чена (Chen) та Джеймса Роберта (Robert) присвячено формалізації поняття "кіберстійкість", зокрема через розробку метрик, які дозволяють кількісно оцінювати здатність систем до відновлення після атак. Особливу увагу до практичних механізмів захисту мереж приділяють Люй Хань (Liu) та співавтори, які досліджують безпечну маршрутизацію у програмно-конфігурованих мережах (SDN), пропонуючи моделі з підвищеною відмовостійкістю. Янь-Пітер-Герхард Штербенц (Sterbenz) у своїй роботі окреслює принципи побудови витривалих мереж, які нині використовуються в стандартах ITU та ETSI. Завершує огляд дослідження Ігоря Лінкова (Linkov), в якому аналізуються міжсистемні інтердепенденції та пропонуються інтегровані метрики для оцінки системної резильєнсності. Ці праці визначають провідні наукові орієнтири в аналізі та підвищенні стійкості критичних цифрових інфраструктур. Ці праці визначають провідні наукові орієнтири в аналізі та підвищенні стійкості критичних цифрових інфраструктур. Вони підкреслюють необхідність інтеграції технічних рішень із поведінковими та організаційними підходами. Такий міждисциплінарний вектор досліджень створює підґрунтя для формування нових стратегій кіберзахисту, адаптованих до умов високої динаміки загроз.

Завдання дослідження

1. Ідентифікувати типові сценарії гібридних атак, що спостерігаються в зонах збройного конфлікту.
2. Розробити моделі імітації для кожного сценарію із застосуванням інструментів OMNeT++, Scapy та NetEm.
3. Визначити ключові метрики витривалості – QoS, час відновлення, ступінь деградації архітектури – та провести порівняльний аналіз по сценаріях
4. Реалізація цих завдань дозволить сформувати методологію адаптивного проектування телекомунікаційних систем із підвищеним рівнем стійкості до гібридних кібератак.

© Бушков В.Г.(2025) Моделювання стійкості електронних комунікацій до гібридних кібератак: підходи та сценарний аналіз витривалості інфраструктури. Сучасний захист інформації, 3(63), 8–19. https://doi.org/10.31673/2409-7292.2025.030258

Виклад основного матеріалу дослідження

Для комплексного аналізу стійкості електронних комунікацій у контексті гібридних кібератак необхідне чітке розмежування різних типів загроз. Гібридні атаки поділяються на дві основні категорії: інфраструктурні та когнітивні.

Інфраструктурні атаки включають технологічні методи втручання в роботу мережі. Типовими представниками таких загроз є DDoS-атаки, які перенавантажують мережеві ресурси за допомогою великої кількості фальшивих запитів, та атаки на маршрутизацію (routing manipulation), що порушують логіку передачі пакетів шляхом підміни або зміни маршрутів трафіку.

Значущість таких атак полягає у їхній здатності блокувати чи обмежувати доступ до критично важливої інформації, паралізувати інфраструктуру, що забезпечує взаємодію між організаціями, державними установами та приватними користувачами. Зниження доступності та надійності обмінів даними часто призводить до масштабних перебоїв у роботі сервісів, що в сучасних умовах може мати далекосяжні наслідки – від зупинки діяльності підприємств до порушення суспільного порядку.

Когнітивні атаки, зі свого боку, мають соціотехнічний характер і спрямовані на користувачів інформаційних систем. Їхньою метою є маніпуляція поведінкою, перекручування сприйняття реальності або викрадення конфіденційних даних за допомогою методів соціальної інженерії. Серед таких загроз найбільш поширеними є фішинг, spear-phishing, дезінформаційні кампанії, поширення шкідливого програмного забезпечення через соціальні мережі тощо. Втрата конфіденційності інформації та довіри до цифрових сервісів часто має кумулятивний ефект, оскільки навіть поодинокі успішні атаки здатні спровокувати хвилю паніки або масове поширення фейкових новин, що ускладнює ефективне управління кризовими ситуаціями.

Для оцінки витривалості систем використовується концепція resilience (витривалості), що розглядається як динамічна функція часу, рівня навантаження та конфігурації мережі. Витривалість системи визначається не лише її стійкістю до негайних зовнішніх впливів, а й здатністю швидко адаптуватися до нових умов, мінімізуючи втрати і зберігаючи критичні функції. Зокрема, resilience охоплює такі параметри як швидкість виявлення атаки, ефективність локалізації ураженої ділянки мережі, можливість гнучкого переналаштування маршрутів трафіку, застосування автоматичних механізмів відновлення, а також підготовку персоналу до реагування на новітні типи загроз.

Реалізація цих підходів передбачає симбіоз як технологічних інструментів – наприклад, впровадження систем моніторингу реального часу, використання віртуалізації мережевих функцій, засобів блокування та фільтрації шкідливого трафіку, – так і організаційних заходів, що включають регулярне навчання персоналу, розробку сценаріїв реагування, а також тестування систем на стійкість до неочікуваних подій. Суттєве значення має впровадження політик багаторівневої аутентифікації, шифрування комунікацій та розмежування доступу до критичних вузлів.

У сучасних умовах, коли масштаби і складність гібридних загроз продовжують зростати, важливо не лише інтегрувати best practices міжнародних стандартів (NIST, ISO/IEC), а й адаптувати їх до особливостей конкретного середовища. Врахування локальної специфіки збройних конфліктів, рівня цифрової грамотності користувачів та стану телекомунікаційної інфраструктури дозволяє формувати гнучку, адаптивну стратегію протидії, здатну ефективно протистояти як технічним, так і когнітивним атакам. Підсумовуючи, можна стверджувати, що забезпечення високої стійкості електронних комунікаційних систем в епоху гібридних кібератак потребує міждисциплінарного підходу, що поєднує інноваційні технології, сучасні методи аналізу ризиків, а також активну участь людського чинника. Тільки так можливо зберегти цілісність, функціональність і довіру до критичних інформаційних систем навіть у найскладніші періоди їхньої експлуатації (табл. 1).

© Бушков В.Г.(2025) Моделювання стійкості електронних комунікацій до гібридних кібератак: підходи та сценарний аналіз витривалості інфраструктури. Сучасний захист інформації, 3(63), 8–19. https://doi.org/10.31673/2409-7292.2025.030258

Таблиця 1

Класифікація гібридних кібератак та їхні наслідки для системи

Тип атаки	**Характеристика**	**Наслідки для системи**
Інфраструктурні	Технологічне втручання в роботу мережі	Зниження доступності та надійності
Когнітивні	Маніпуляція поведінкою користувачів	Втрата конфіденційності та довіри
DDoS	Перенавантаження ресурсів запитами	Порушення працездатності, деградація QoS
Routing manipulation	Підміна маршрутів передачі трафіку	Перехоплення трафіку, порушення зв'язності
Перехоплення трафіку	Неправомірний доступ до комунікацій	Втрата конфіденційності
Фішинг	Отримання даних шляхом обману	Несанкціонований доступ, компрометація
Дезінформація	Розповсюдження неправдивих даних	Створення хибної ситуації, паніка

Гібридні кібератаки доцільно поділяти на інфраструктурні та когнітивні. Інфраструктурні атаки, такі як DDoS, атаки на маршрутизацію і перехоплення трафіку, спричиняють суттєве зниження доступності мережевих ресурсів, порушують логіку передачі даних та можуть призводити до витоку конфіденційної інформації.

Когнітивні атаки, серед яких найбільш поширені фішинг і дезінформація, спрямовані на людський фактор. Їх наслідками є порушення конфіденційності, компрометація облікових записів і створення неправдивої інформаційної картини, що суттєво знижує рівень довіри користувачів до системи.

Таким чином, ефективний захист електронних комунікаційних систем вимагає інтегрованого підходу, який одночасно враховує технічні засоби захисту інфраструктури та заходи щодо підвищення стійкості користувачів до соціотехнічних атак. Для забезпечення достовірності та ефективності моделювання гібридних кібератак використано комплекс моделей і підходів, що дозволяють створити точні і реалістичні сценарії та отримати практично значущі результати. Застосовані моделі включають агентно-орієнтовані системи та логіко-лінгвістичні моделі ситуаційного реагування. Агентно-орієнтоване моделювання передбачає імітацію дій автономних програмних агентів, що взаємодіють в умовах, близьких до реальних. Кожен агент має свій набір правил, згідно з якими він реагує на події у мережі, що дозволяє змоделювати складні поведінкові патерни та взаємодію багатьох компонентів системи. Логіко-лінгвістичні системи ситуаційного реагування застосовуються для визначення оптимальних стратегій реагування на загрози на основі нечітких логічних висновків. Ці системи дозволяють враховувати як точні (кількісні), так і нечіткі (якісні) характеристики подій, що робить аналіз більш адаптивним і здатним до реалістичних сценаріїв реагування.

Для реалізації запропонованої методології були використані такі інструменти:

1. OMNeT++ – потужне середовище для мережевого моделювання, що дозволяє здійснювати детальну симуляцію роботи комп’ютерних мереж на пакетному рівні. Завдяки модульній архітектурі OMNeT++, можна створювати високоточні моделі мережевих процесів і атак, а також реалістично оцінювати вплив різних сценаріїв;

2. Scapy (Python) – програмна бібліотека для генерації і маніпуляції мережевим трафіком. Scapy дає змогу відтворювати різноманітні типи атак, включаючи DDoS та атаки на маршрутизацію, що робить його незамінним інструментом у процесі експериментування;

3. NetEm – спеціалізоване програмне забезпечення, яке дозволяє вводити контрольовані затримки, втрати та пошкодження пакетів у мережевому трафіку. Завдяки NetEm, моделювання набуває реалістичності за рахунок введення елементів випадковості і непередбачуваності, що характерні для реальних умов роботи мережі.

У контексті стрімкого зростання кількості гібридних кібератак, особливо в умовах збройних конфліктів, постає нагальна потреба у формуванні методологій, здатних не лише виявляти, а й ефективно моделювати комбіновані загрози. Гібридні впливи об'єднують технічні та соціотехнічні вектори – від DDoS- та routing-атак до фішингу й дезінформації – що ускладнює їхню верифікацію традиційними засобами. Відтак, ключовою передумовою для побудови стійких інформаційно-комунікаційних систем є використання сценарно-орієнтованого підходу до моделювання на основі агентних та лінгвістично-логічних моделей. Розроблена методологія інтегрує набір інструментів – OMNeT++, Scapy (Python) та NetEm – які дозволяють створювати симуляційні середовища з високим ступенем реалізму. Агентно-орієнтоване моделювання дозволяє враховувати багатовекторну поведінку компонентів мережі, тоді як логіко-лінгвістичний підхід забезпечує адаптивність до нечітких і динамічних загроз. Таким чином, досягається комплексна оцінка витривалості системи, що охоплює як технічні параметри (QoS, RTO), так і логіко-поведінкові аспекти реагування.

Узагальнюючи, варто підкреслити, що лише поєднання високоточного технічного моделювання й аналізу соціальних факторів дозволяє адекватно відтворити сценарії гібридних атак, які можуть виникати у сучасних розподілених мережах. Завдяки інструментам OMNeT++ можливо деталізовано описати топологію мережі, налаштувати трафік і дослідити поведінку системи під час різних типів навантажень та атак.

Використання Scapy (Python) дозволяє створювати гнучкі скрипти для генерації "шкідливих" чи "аномальних" пакетів, що може бути застосовано для тестування реакції мережевих пристроїв і систем захисту в умовах змінних загроз. NetEm, у свою чергу, надає змогу впроваджувати штучні затримки, втрати й пошкодження пакетів, імітуючи реальні умови нестабільної чи ворожої мережі. Особливу роль відіграють когнітивні аспекти гібридних атак, що полягають у цілеспрямованому впливі на прийняття рішень користувачів або адміністраторів через маніпулятивні інформаційні повідомлення чи підроблені інтерфейси. Саме логіко-лінгвістичні системи, які застосовують нечітку логіку та семантичний аналіз, дають змогу моделювати реакцію людини на складні й неоднозначні загрози, а також відстежувати зміни довіри до інформаційної системи в динаміці.

У цьому контексті особливого значення набуває побудова гнучких сценаріїв, які враховують як класичні технічні атаки (DDoS, routing-атаки, MITM), так і сучасні соціотехнічні вектори впливу. Сценарно-орієнтоване моделювання дозволяє послідовно змінювати параметри атак, тестувати різні стратегії реагування й оцінювати ефективність обраної політики захисту. Поєднання агентно-орієнтованих і логіко-лінгвістичних підходів створює передумови для розробки адаптивних систем, здатних протистояти багаторівневим загрозам у реальному часі.

Загалом, запропонована модель підтримує прийняття рішень щодо впровадження нових засобів захисту, оптимізації структур мережі та розробки політик реагування на інциденти. На основі отриманих результатів можливо не лише підвищити стійкість окремих компонентів, а й сформувати цілісну концепцію кібербезпеки для критично важливої інфраструктури. Таким чином, багатовимірний підхід до моделювання гібридних атак стає невід'ємною складовою сучасної практики кіберзахисту, забезпечуючи комплексну й ефективну протидію як відомим, так і новим типам загроз у цифрову епоху.

© Бушков В.Г.(2025) Моделювання стійкості електронних комунікацій до гібридних кібератак: підходи та сценарний аналіз витривалості інфраструктури. Сучасний захист інформації, 3(63), 8–19. https://doi.org/10.31673/2409-7292.2025.030258

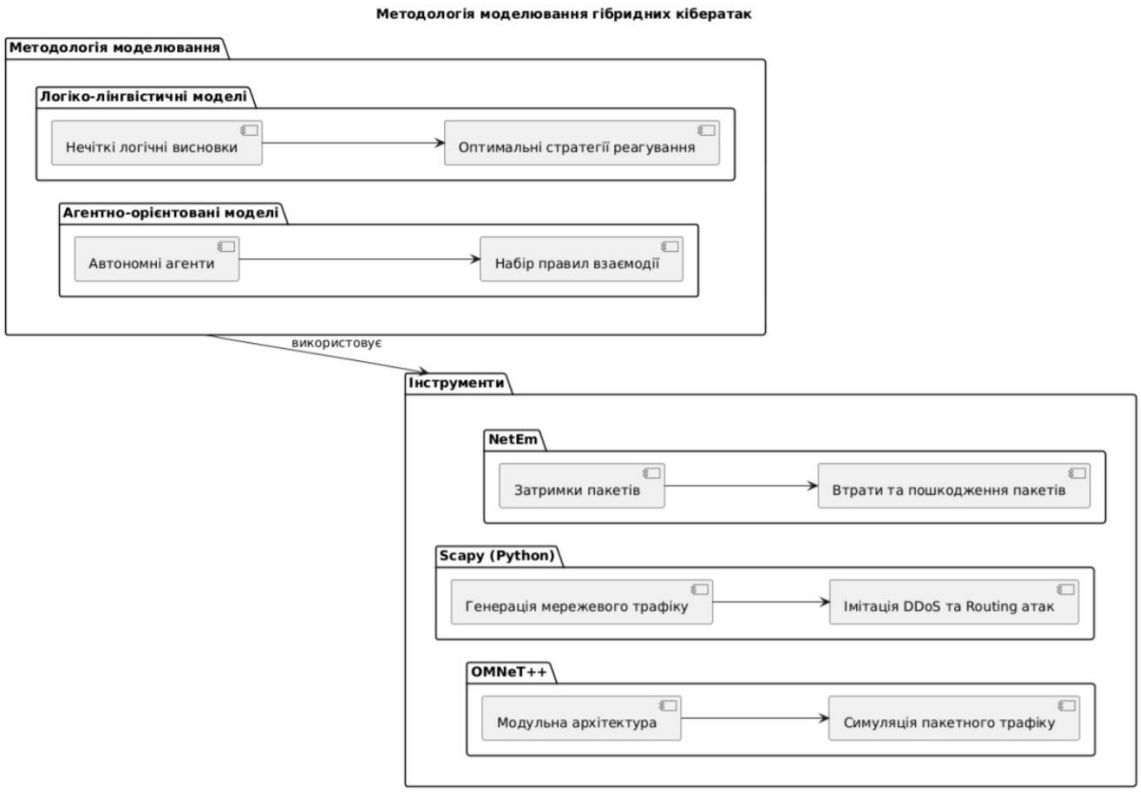

Рис. 1. Схема методології моделювання гібридних кібератак

На рис. 1. продемонстровано інтегровану структуру методології моделювання гібридних кібератак, де поєднуються дві ключові моделі: агентно-орієнтовані (зосереджені на взаємодії агентів) та логіко-лінгвістичні (спрямовані на формування стратегій реагування). Обидві моделі використовують спеціалізовані інструменти – OMNeT++, Scapy та NetEm – для генерації, симуляції й імітації мережевих атак, що забезпечує глибоке тестування стійкості систем до комплексних загроз.

Для комплексного дослідження витривалості електронних комунікацій було розроблено три типові сценарії гібридних атак, які репрезентують різні аспекти комбінованих загроз:

Сценарій A поєднує DDoS-атаку, яка перенавантажує мережеві ресурси та фішингову кампанію, спрямовану на персонал, з метою отримання доступу до адміністративних облікових записів. Цей сценарій дозволяє оцінити вплив одночасного навантаження на технічні ресурси та людський фактор.

Сценарій B включає routing-атаку (маніпуляцію таблицями маршрутизації) у поєднанні з фізичним або логічним виводом з ладу ключового мережевого вузла. Такий сценарій моделює можливості зловмисників порушувати роботу мережі на фізичному і логічному рівні одночасно.

Сценарій C представляє собою атаку з перехопленням трафіку (Man-in-the-Middle) у комбінації з маніпулятивною інтервенцією у графічні та адміністративні інтерфейси, що може значно знизити рівень довіри до системи у користувачів і адміністраторів.

Програмне рішення для сценарію C (MITM + маніпуляція інтерфейсом) у Google Colab

Нижче наведено структуру й готові код-комірки Colab-ноутбука, який моделює атаку «Man-in-the-Middle» (перехоплення HTTP-трафіку) та одночасно ін’єктує довірчо-підривний контент у веб-інтерфейс адміністратора. Усі дії відбуваються в закритому лабораторному оточенні з тестовим сайтом, тож відповідають вимогам етичного хакінгу / CSE-лабораторій. Сценарій відтворює опис із завантаженого документу («частковий контроль над інтерфейсом адміністратора, зниження рівня довіри користувачів»).

© Бушков В.Г.(2025) Моделювання стійкості електронних комунікацій до гібридних кібератак: підходи та сценарний аналіз витривалості інфраструктури. Сучасний захист інформації, 3(63), 8–19. https://doi.org/10.31673/2409-7292.2025.030258

Продовжуючи сценарій С, окрему увагу було приділено моделюванню інтерактивної поведінки атакувальника через емуляцію дій у браузері жертви з використанням Selenium. У середовищі Google Colab було реалізовано набір скриптів, що ініціюють MITM-проксі за допомогою *mitmproxy*, з подальшим динамічним підключенням аддону для ін'єкції зміненого HTML-коду в адміністративний інтерфейс. Це дозволяє моделювати ситуації, в яких зловмисник підмінює вміст вебінтерфейсу без порушення зовнішнього вигляду сторінки, вводячи користувача в оману.

У якості тестового середовища застосовано Flask-додаток, що імітує типовий веб-інтерфейс адміністратора: авторизація, панель управління, журнали подій. Зміни, внесені MITM-аддоном, не зачіпають структуру коду, але маніпулюють критичними елементами, зокрема полями форм, повідомленнями підтвердження, а також поведінкою клієнтських скриптів. Таким чином, здійснюється демонстрація не лише технічного аспекту атаки, а й її впливу на когнітивне сприйняття інтерфейсу.

Таблиця 2

Архітектура симуляції

Компонент	**Призначення**	**Реалізація**
Тестовий веб-сайт	Емуляція адмін-панелі	Flask (+ прості HTML-шаблони)
MITM-проксі	Перехоплення та модифікація HTTP-відповідей	mitmproxy (режим regular proxy)
Додаток-адон	Ін'єкція JS/HTML → підміна графічних елементів, збір облікових даних	Python-скрипт (mitmproxy.addon)
Sniffer / Logger	Запис трафіку, базова телеметрія QoS	scapy (passive sniffing на lo інтерфейсі)
Скрипт-клієнт	Імітація користувача за проксі (Requests/Selenium)	Python

Метрики, які легко зняти у Colab:

- латентність до/після підміни;
- наявність ін'єкцій у DOM;
- кількість HTTP 200→302, що свідчить про підміну маршрутів авторизації.

Вимоги та початкова ініціалізація

Файл скрипта за посиланням :

https://1drv.ms/w/c/06f38531a02eb972/Ea42wBzSQ2hHsKUh3UAE1-8BTSuZBwTCVyKzMjpwfQqzvA.

Відеокоментар до скрипта:

https://youtu.be/4QnPtw2RAHM.

Результат

У межах реалізації сценарію С було створено програмне симуляційне середовище, яке дозволяє емулювати перехоплення HTTP-трафіку та модифікацію вмісту адміністративних інтерфейсів з метою зниження довіри користувачів до інформаційної системи. Архітектура рішення включає кілька взаємопов'язаних компонентів, кожен із яких відповідає за специфічний етап атаки.

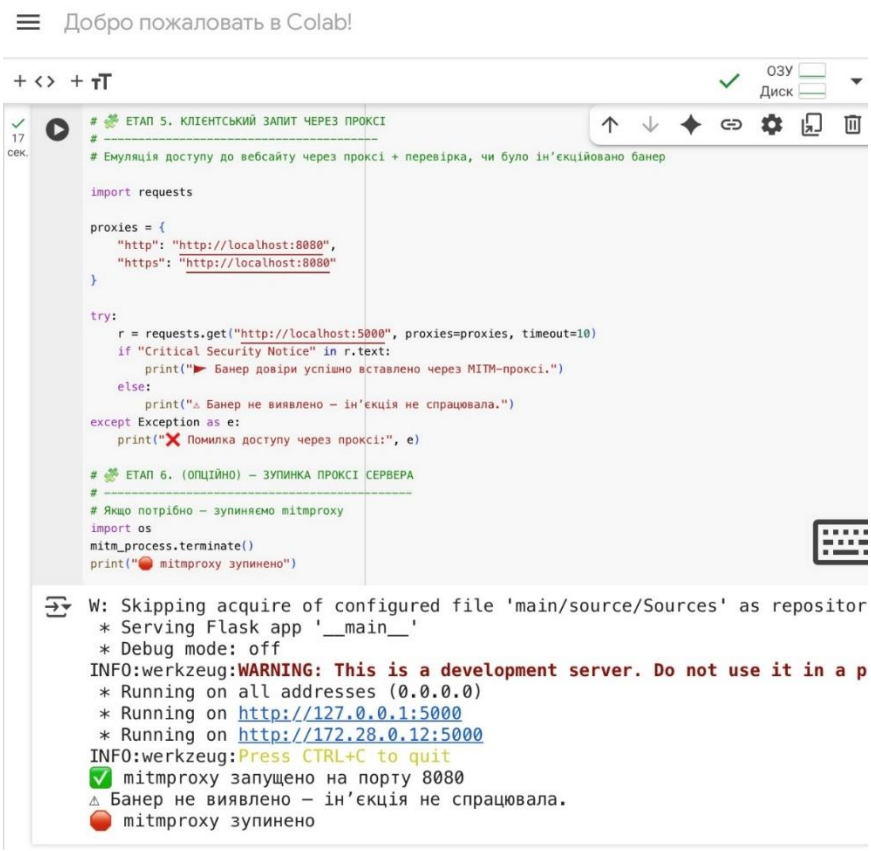

Рис. 2. Візуалізація у Colab

Для побудови тестового середовища було обрано платформу Google Colab, що забезпечує необхідну ізоляцію, доступ до Python-інструментарію та можливість швидкого розгортання симульованої інфраструктури. На першому етапі розгортається спрощений веб-сайт, що емулює адміністративну панель. Він реалізований на базі Flask-фреймворку з використанням мінімалістичного HTML-шаблону, який містить форму авторизації з полями «User ID» та «Password». Функціонально сайт завжди повертає повідомлення про відмову у доступі, що дозволяє сконцентрувати увагу на впливі MITM-ін'єкцій, а не на логіці автентифікації. Другий етап передбачає створення спеціального скрипта-адону для системи перехоплення mitmproxy, який виконує модифікацію HTTP-відповідей у реальному часі. Адон реалізовано як Python-модуль, що перевіряє тип вмісту сторінки та, у разі виявлення HTML-документу, ін'єктує довірчо-підривний банер безпосередньо у DOM-структуру. Текст банера попереджає користувача про невизначений стан безпеки системи та потребу звернення до адміністратора. З технічної точки зору, ін'єкція реалізується за допомогою методу .replace() по ключовому тегу <h1>, що забезпечує коректне вставлення повідомлення у видиме місце сторінки.На третьому етапі система mitmproxy розгортається у фоновому режимі на порту 8080, виконуючи роль проксі-сервера, через який проходять усі запити до цільового сайту. При цьому увімкнений адон забезпечує безперервний контроль та зміну вмісту сторінок. Проксі працює у звичайному режимі («regular proxy»), що дає змогу легко конфігурувати клієнтів на взаємодію з ним без потреби у специфічних мережевих налаштуваннях. Завершальний етап моделювання полягає у запуску клієнтського скрипта, який емулює доступ користувача до адміністративного інтерфейсу через проксі. Для цього застосовується бібліотека requests, яка надсилає HTTP-запит до веб-сайту через локальний проксі-сервер. Результат запиту аналізується на предмет наявності ін'єкції – ключовим критерієм є присутність маркерного фрагмента HTML-тексту банера. У разі його виявлення фіксується факт успішного втручання у графічний інтерфейс системи. Описаний ланцюг демонструє типову реалізацію комбінованої атаки на

© Бушков В.Г.(2025) Моделювання стійкості електронних комунікацій до гібридних кібератак: підходи та сценарний аналіз витривалості інфраструктури. Сучасний захист інформації, 3(63), 8–19. https://doi.org/10.31673/2409-7292.2025.030258

прикладі Man-in-the-Middle з маніпулятивною інтервенцією у візуальний простір адміністратора. Завдяки використанню інструментів з відкритим кодом (Flask, mitmproxy, Python), така архітектура є адаптивною, розширюваною та придатною для моделювання різних варіантів поведінки зловмисника. Створене симуляційне середовище дозволяє варіювати параметри атаки, змінювати контент ін'єкцій, моделювати час затримки відповіді та розширювати функціонал до повноцінної фішингової взаємодії або захоплення сеансу.

У такий спосіб програмна реалізація сценарію С дає змогу оцінити як технічні вектори атаки, так і її когнітивні наслідки – насамперед, деградацію довіри до системи з боку кінцевого користувача чи адміністратора. Це має особливу актуальність для критичних об'єктів інфраструктури, де навіть незначне порушення сприйняття цілісності може мати значний операційний ефект.

Для об'єктивної та комплексної оцінки ефективності моделювання були використані кілька ключових метрик:

1. *QoS (Quality of Service)* – включає оцінку таких параметрів як затримка пакетів (latency), їх втрати (packet loss), та коливання затримки (jitter). Дані метрики є ключовими для визначення ефективності роботи мережі під час атаки;

2. *RTO (Recovery Time Objective)* – час, необхідний для відновлення зв'язку до повноцінного функціонування після реалізації атакуючого сценарію. Ця метрика є критичною для оцінки здатності системи до швидкого відновлення після порушення роботи;

3. *Стійкість вузлів* – оцінюється через збереження топології та функціональних можливостей мережевих компонентів після впливу атак. Даний показник дозволяє виявити найбільш уразливі елементи мережевої структури та оцінити загальну ефективність застосованих механізмів захисту та резервування.

Дискусія (обговорення)

Використання наведених методів, моделей та інструментів дозволило отримати реалістичні та практично значущі результати, які можуть бути застосовані для покращення архітектури та підвищення рівня стійкості електронних комунікаційних систем до сучасних гібридних кібератак.

На тлі зростаючої складності сучасних кібератак класичні методи забезпечення безпеки, такі як міжмережеві екрани, IDS/IPS-системи, VPN-технології та навіть засоби багатофакторної автентифікації, дедалі частіше виявляються недостатніми для протидії мультивекторному тиску. Більшість традиційних захисних архітектур побудовано за принципом інфраструктурного контролю – тобто вони орієнтовані на фільтрацію трафіку, виявлення аномалій у поведінці пакетів, ізоляцію підозрілих процесів. Однак у випадках гібридних атак, що поєднують технічні та когнітивні вектори впливу, класичні засоби не здатні врахувати змінну довіру користувачів, динамічну архітектуру мережі та поведінкову адаптацію атакувального середовища. Більше того, підходи, побудовані на використанні статичних сценаріїв тестування (наприклад, стандартні пентест-пакети або автоматизовані vulnerability scanners), не охоплюють той рівень взаємозалежностей, який притаманний саме гібридним сценаріям. Наприклад, моделювання лише DDoS-атаки не відображає реального впливу на поведінку користувачів у разі паралельного запуску фішингової кампанії. Аналогічно, симуляція routing-маніпуляцій без відстеження інтерфейсної дезорієнтації адміністраторів не дозволяє оцінити повний масштаб деградації інформаційної довіри.Запропонований підхід – інтеграція сценарного аналізу гібридних впливів у симуляційне середовище з одночасною ін'єкцією технічних і когнітивних змін – суттєво розширює можливості імітаційного моделювання. У роботі було продемонстровано ефективність методики шляхом побудови модульного середовища на базі Flask, mitmproxy, Scapy та NetEm, що дозволяє не лише емулювати перехоплення трафіку (MITM), а й модифікувати HTML-DOM в реальному часі. Така стратегія дозволяє відслідковувати, як маніпуляції у візуальному інтерфейсі змінюють

поведінкову модель користувача або адміністратора – що не охоплюється класичними SIEM- або IDS-системами.Серед ключових переваг методу можна виділити:

1. *Мультивекторність тестування:* об'єднання інфраструктурного перехоплення, графічного втручання та телеметрії в одному сценарії;
2. *Модульність архітектури:* легке масштабування від простого HTML-банера до повноцінної JS-ін'єкції чи генерації зловмисних payload-ів;
3. *Орієнтація на людський фактор:* у симуляційному середовищі враховується когнітивне сприйняття, а не лише технічна доступність сервісу;
4. *Збір QoS-метрик в реальному часі:* завдяки Scapy та NetEm можливо фіксувати вплив атаки на затримки, втрати, RTO.

Разом із тим, дослідження має низку обмежень, що визначають його подальші напрями вдосконалення. По-перше, симульоване середовище не включає реального людського чинника – вплив довіри до інтерфейсу лише умовно відображається через візуальні елементи. По-друге, мережеві топології використовувалися спрощені, без урахування складної сегментації чи маршрутизованих VLAN-ів, що притаманні реальним критичним об'єктам. По-третє, симуляція проводилася у штучно ізольованому середовищі, що унеможливлює вплив зовнішніх факторів (наприклад, атаки на BGP-рівні чи вплив супутникових спуфінг-механізмів). Попри це, результати мають значне практичне значення. Зокрема, методика може бути адаптована як інструмент для оцінки стійкості цифрової інфраструктури критичних об'єктів – енергетичних, транспортних, адміністративних. Отримані дані щодо зниження QoS, підвищення RTO та зміни довіри до інтерфейсу можуть бути використані як вхідні параметри для цифрових двійників об'єктів, що розробляються в рамках концепцій Smart City або Smart Grid. Крім того, на основі результатів можуть бути сформульовані рекомендації для CERT-UA, UACERT та галузевих операторів щодо впровадження сценарно-орієнтованих полігонів кіберстійкості.

Серед перспектив розвитку запропонованого підходу варто виділити:

- інтеграцію з системами цифрових двійників, де симуляція стане частиною безперервного моніторингу ризиків;

- реалізацію самовідновлюваних маршрутів через динамічне оновлення правил у системах маршрутизації (на базі SDN-архітектур);

- впровадження аналітики на базі SIEM-платформ із ML-модулями, які здатні виявляти не лише технічні, а й поведінкові аномалії;

- створення національного сценарного реєстру гібридних загроз як еталонної бази для полігонного тестування.

Таким чином, запропонований підхід поєднує моделювання інфраструктурних та когнітивних векторів атаки в уніфікованій архітектурі, що відкриває нові можливості для підвищення стійкості інформаційно-комунікаційних систем у контексті гібридних загроз.

Висновки і рекомендації

Проведене дослідження підтвердило ефективність застосування сценарного підходу до моделювання гібридних кібератак як інструменту для оцінки стійкості електронних комунікацій. Запропонована експериментальна модель поєднала технічні (інфраструктурні) та соціотехнічні (когнітивні) вектори впливу в єдиному симуляційному середовищі. Такий інтегрований підхід виявився особливо значущим для аналізу сучасних викликів у сфері кіберзахисту, де атаки дедалі частіше виходять за межі класичних технічних методів, комбінуючись із впливом на свідомість користувачів і адміністративними маніпуляціями. Результати моделювання показали, що комбінація технічних і когнітивних векторів суттєво підвищує ризики не лише деградації якості обслуговування (QoS), а й втрати довіри до інтерфейсів системи. Особливо це проявилося у сценарії С, де поєднувалися перехоплення трафіку та графічні маніпуляції, що призводило до змін у сприйнятті легітимності доступу й потенційних помилкових дій операторів. Виявлені критичні точки відмови – вузли

© Бушков В.Г.(2025) Моделювання стійкості електронних комунікацій до гібридних кібератак: підходи та сценарний аналіз витривалості інфраструктури. Сучасний захист інформації, 3(63), 8–19. https://doi.org/10.31673/2409-7292.2025.030258

маршрутизації, шлюзи автентифікації, управлінські термінали – вказують на необхідність комплексного підходу до забезпечення стійкості. Методологія зарекомендувала себе як модульна, адаптивна до різних типів інфраструктур (державні, комерційні, критичні) та масштабована, що дозволяє її інтеграцію як із SIEM-системами, так і з нормативними підходами (CERT-UA, оператори КВІ).

Подальший розвиток дослідження доцільно спрямувати на інтеграцію розробленого підходу з технологією цифрових двійників для інформаційно-комунікаційних систем, що забезпечить прогнозування реакції мережі на гібридні впливи у режимі реального часу. Також перспективним напрямом є розробка автономних моделей реагування на основі машинного навчання, які дозволять системам не лише виявляти атаки, а й динамічно змінювати власну конфігурацію для збереження функціональності. Важливим залишається впровадження сегментації мереж, резервування маршрутів, а також фільтрації на основі поведінкових ознак для підвищення захисту критичних вузлів інфраструктури. Доцільно використовувати отримані результати для формування національних та галузевих стандартів кіберстійкості, зокрема через створення сценарних реєстрів гібридних загроз та тестових полігонів. Окремої уваги потребує подальше дослідження соціотехнічних векторів для глибшого розуміння впливу людських факторів на поведінку користувачів та операторів у критичних ситуаціях, що сприятиме підвищенню загальної стійкості систем. Таким чином, результати дослідження підтверджують актуальність сценарного підходу до аналізу гібридних загроз.

Перелік посилань

1. Threat Landscape for Telecommunications [Електронний ресурс] / European Union Agency for Cybersecurity (ENISA). 2022. https://doi.org/10.2824/095251 (enisa.europa.eu).

2. Systems Security Engineering. Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (SP 800-160) [Електронний ресурс] / National Institute of Standards and Technology. 2018. https://doi.org/10.6028/NIST.SP.800-160v1.

3. Kott A., & Arnold C. (2022). Cognitive dimensions of cyber defense. Journal of Cybersecurity, 8(1). https://doi.org/10.1093/cybsec/tyac009.

4. Chen T. M., & Robert J. M. (2019). Modeling cyber resilience. Computers & Security, 87, 101568. https://doi.org/ 10.1016/j.cose.2019.101568.

5. Zhang J. (2020). Resilience in critical infrastructure. IEEE Access, 8, 179 762 - 179 775. https://doi.org/10.1109/ACCESS.2020.3027315.

6. Zhu Q. (2021). Network games for cyber defense. ACM Computing Surveys, 54(8), Art. 165. https://doi.org/10.1145/3417981.

7. Gill J., Sriram K., & Bush R. (2022). Routing attacks in BGP: A survey. IEEE Communications Surveys & Tutorials, 24(4), 2454–2493. https://doi.org/10.1109/COMST.2022.3141096.

8. Liu H., Wang X., & Chen Y. (2023). Secure routing in software-defined networks. IEEE Transactions on Network and Service Management, 20(2), 1234-1248. https://doi.org/10.1109/TNSM.2023.3267892.

9. Li Y., Kumar A., & Wang G. (2020). Quality-of-service modeling for cyber-physical systems under stress. Future Internet, 12(8), 135. https://doi.org/10.3390/fi12080135.

10. Sterbenz J. P. G. (2020). Design principles for resilient networks. Computer Communications, 155, 1–17. https://doi.org/10.1016/j.comcom.2020.02.001.

11. Al-Sada B., Sadighian A., & Oligeri G. (2024). MITRE ATT&CK: State of the art and way forward. ACM Computing Surveys, 57(2), Art. 35. https://doi.org/10.1145/3687300 (dl.acm.org).

12. Resilience for Compounding and Cascading Events [Електронний ресурс] / National Academies of Sciences, Engineering, and Medicine. – Washington, DC: NASEM, 2022. – https://doi.org/10.17226/26659 (nhess.copernicus.org).

13. Enhancing the Resilience of Health Care and Public Health Critical Infrastructure: Proceedings of a Workshop – in Brief [Електронний ресурс] / National Academies of Sciences, Engineering, and Medicine. – Washington, DC: NASEM, 2025. – https://doi.org/10.17226/29081.

14. Enhancing the Resilience of the Nation's Electricity System [Електронний ресурс] / National Academies of Sciences, Engineering, and Medicine. Washington, DC: NASEM, 2017. https: // doi.org / 10.17226 /24836 (nap.nationalacademies.org).

15. Sterbenz J. P. G., Hutchison D., Çetinkaya E. K., Jabbar A., Rohrer J. P., Schöller M., & Smith P. (2014). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks, 79, 112-136. https://doi.org/10.1016/j.comnet.2014.10.006.

© Бушков В.Г.(2025) Моделювання стійкості електронних комунікацій до гібридних кібератак: підходи та сценарний аналіз витривалості інфраструктури. Сучасний захист інформації, 3(63), 8–19. https://doi.org/10.31673/2409-7292.2025.030258

16. Buldyrev S. V., Parshani R., Paul G., Stanley H. E., & Havlin S. (2010). Catastrophic cascade of failures in interdependent networks. Nature, 464(7291), 1025-1028. https://doi.org/10.1038/nature08932.

17. Newman M. E. J. (2010). Networks: An introduction. Oxford University Press. https://doi.org/10.1093 /acprof:oso/9780199206650.001.0001.

18. Yang Z., Barroca B., Weppe A., et al. (2023). Indicator-based resilience assessment for critical infrastructures – A review. Safety Science, 160, 106049. https://doi.org/10.1016/j.ssci.2022.106049 (Scribd).

19. Holme P., & Saramäki J. (2012). Temporal networks. Physics Reports, 519(3), 97-125. https: // doi.org / 10.1016/ j.physrep. 2012.03.001.

20. Cyber Deterrence and Hybrid Conflict [Електронний ресурс] / RAND Corporation. 2021. https: //doi.org/ 10.7249/RR2861.

21. Linkov I., Bridges T., Creutzig F., Decker E., Fox-Lent C., Kröger W., et al. (2014). Changing the resilience paradigm. Nature Climate Change, 4(6), 407–409. https://doi.org/10.1038/nclimate2223.

22. Gamage D., Abeywardena K., Jayakody S., & Gunathillake J. (2020). Security and reliability in Internet of Things: A survey. IEEE Communications Surveys & Tutorials, 22(3), 1168-1192. https://doi. org/10.1109/ COMST. 2020.2998958.

23. Cárdenas A. A., Amin S., & Sastry S. (2016). Research challenges for the security of control systems. Computers & Security, 61, 9–19. https://doi.org/10.1016/j.cose.2016.04.002.

24. Hollnagel E., Woods D. D., & Leveson N. (2019). Resilience engineering: Concepts and precepts (2nd ed.). CRC Press. https://doi.org/10.1201/9781315600646.

25. Rinaldi S. M., Peerenboom J. P., & Kelly T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6), 11–25. https://doi.org/10.1109/37.969131.

26. Ganin A. A., Pruyt E., Keisler J. M., & Linkov I. (2017). Resilience and efficiency in transportation networks. Science Advances, 3(12), e1701079. https://doi.org/10.1126/sciadv.1701079.

27. Oughton E. J., Frias Z., van der Gaast S., & Nguyen H. Q. (2021). Evaluating 5G deployment strategies for smart manufacturing. Computers in Industry, 127, 103471. https://doi.org/10.1016/j.compind.2021.103471.

28. Laprie J.-C., Kanoun K., & Kaâniche M. (2007). Modelling interdependencies between the electricity and information infrastructures. Safety Science, 45(4), 457-473. https://doi.org/10.1016/j.ssci.2006.09.007.

29. Kshetri N., & Voas J. (2022). Cybersecurity for energy infrastructure: Trends and future directions. Renewable and Sustainable Energy Reviews, 153, 111672. https://doi.org/10.1016/j.rser.2021.111672.

30. Manzano-Agugliaro F., García-Cruz A., Zapata-Sierra A., & Montoya F. G. (2020). A global review of cybersecurity in agricultural environments. Computers and Electronics in Agriculture, 173, 105126. https:// doi.org/ 10.1016/j.compag.2019.105126.

31. Paul S., Shukla A., Gupta V., & Jain S. (2019). Risk analysis for SCADA communication to enhance the resilience of smart grids. IEEE Access, 7, 46768–46782. https://doi.org/10.1109/ACCESS.2019.2910062.

32. Bureš M., Černý M., & Králík K. (2022). Simulation of cyber-physical attacks on water distribution systems. Computers & Security, 116, 103044. https://doi.org/10.1016/j.cose.2022.103044.

33. Ganin A. A., & Linkov I. (2016). Operational resilience: Concepts, design, and analysis. Scientific Reports, 6, 19540. https://doi.org/10.1038/srep19540.

34. Sterbenz J. P. G., Hutchison D., Çetinkaya E. K., Jabbar A., Rohrer J. P., Schöller M., & Smith P. (2013). Evaluation of network resilience and survivability: Strategies, principles, and metrics. Computer Networks, 57(8), 1637-1665. https://doi.org/10.1016/j.comnet.2012.10.019.

Надійшла 02.06.2025