DOI: 10.25140/2411-5363-2024-4(38)-189-196
УДК 004.94

Денис Вікторович Кузьменко

аспірант кафедри інформаційних та комп'ютерних систем
Національний університет «Чернігівська політехніка» (Чернігів, Україна)
E-mail: deniskuzmenko961@gmail.com. **ORCID:** https://orcid.org/0009-0009-0314-568X

МЕТОДИ ТА МОДЕЛІ ЕМУЛЯЦІЇ НЕГАТИВНИХ ВПЛИВІВ НА РЕСУРСИ ІНФОРМАЦІЙНИХ СИСТЕМ

Представлена у статті інформація має оглядовий характер. У статті розглянуто сучасні методи та моделі емуляції негативних впливів на ресурси інформаційних систем з метою підвищення їхньої стійкості та безпеки. Проаналізовано методи емуляції DoS/DDoS атак, включаючи моделі Пуассона, фрактальні та епідеміологічні моделі ботнетів. Розглянуто ін'єкцію вразливостей та хаос-інжиніринг як інструменти для тестування надійності та відмовостійкості систем. Підкреслено важливість використання математичних моделей і методів, таких як процеси Маркова та Монте-Карло симуляції, для точного відтворення реальних загроз. Зроблено висновки про необхідність інтегрованих підходів та впровадження штучного інтелекту для підвищення рівня кібербезпеки.

Ключові слова: *емуляція негативних впливів; інформаційні системи; DoS/DDoS атаки; модель Пуассона; фрактальні моделі; епідеміологічні моделі; ін'єкція вразливостей; хаос-інжиніринг; машинне навчання; штучний інтелект; кібербезпека; моделювання ботнетів; Монте-Карло симуляції; теорія ігор; відмовостійкість системи.*

Бібл.: 12.

Актуальність теми дослідження. У сучасному цифровому світі інформаційні системи стали фундаментальною основою для функціонування бізнесу, державного управління та повсякденного життя громадян. Зі зростанням обсягів даних та підвищенням складності технологічних рішень збільшується і вразливість цих систем до негативних впливів. Кібератаки, такі як DoS/DDoS, відмови апаратного та програмного забезпечення, людські помилки та природні катастрофи можуть призвести до серйозних збоїв у роботі інформаційних систем, що у свою чергу спричиняє значні фінансові втрати, компрометацію конфіденційних даних та підрив довіри клієнтів. Загрози кібербезпеки постійно еволюціонують, стаючи більш складними та витонченими. Зловмисники активно використовують нові методи та інструменти для обходу традиційних засобів захисту. У цьому контексті дослідження методів та моделей емуляції негативних впливів набуває особливої актуальності. Воно дозволяє імітувати потенційні загрози та оцінювати стійкість інформаційних систем до реальних атак і відмов, що є критично важливим для їхнього вдосконалення та розвитку ефективних стратегій захисту. Емуляція негативних впливів є ключовим інструментом для проактивного виявлення вразливостей та тестування реакції систем на різні сценарії негативних подій. Це сприяє не лише підвищенню рівня безпеки, але й забезпеченню безперервності бізнес-процесів, що є особливо важливим у сферах з високими вимогами до надійності, таких як фінансовий сектор, енергетика, охорона здоров'я та транспорт. Крім того, розвиток методів емуляції негативних впливів підтримує тенденції впровадження передових технологій, таких як штучний інтелект та машинне навчання, для покращення засобів кібербезпеки. Це відкриває нові можливості для створення адаптивних систем захисту, які можуть самостійно виявляти та нейтралізовувати загрози в режимі реального часу. Отже, тема дослідження є надзвичайно актуальною в умовах сучасних кіберзагроз та швидкого розвитку інформаційних технологій. Вона має значний науковий та практичний інтерес, сприяючи підвищенню стійкості інформаційних систем та захисту критичної інфраструктури від негативних впливів. Методи та моделі емуляції негативних впливів є критично важливими для тестування та вдосконалення інформаційних систем. Вони дозволяють дослідникам і практикам імітувати різні сценарії відмов та атак, оцінювати стійкість системи та розробляти стратегії захисту. Застосування таких методів сприяє підвищенню рівня безпеки, забезпеченню безперервності бізнес-процесів та зменшенню потенційних фінансових втрат.

Постановка проблеми. Інформаційні системи сьогодні піддаються різноманітним негативним впливам, включаючи кібератаки, відмови апаратного та програмного забезпечення, людські помилки та природні катастрофи, що загрожують їхній безпеці та стійкості. Виникає потреба в розробці ефективних методів та моделей для емуляції цих впливів з метою аналізу, виявлення вразливостей та розробки стратегій захисту.

Аналіз останніх досліджень і публікацій. Наразі, спостерігається значний прогрес у дослідженнях методів та моделей емуляції негативних впливів на інформаційні системи. Сучасні роботи зосереджені на кількох ключових напрямах. Використання штучного інтелекту та машинного навчання для моделювання та виявлення DoS/DDoS атак. Робота ведеться над застосуванням глибоких нейронних мереж [10] для детекції DDoS атак у реальному часі, що підвищує ефективність захисних механізмів. По-друге, розвиток хаос-інжинірингу як методології для тестування стійкості розподілених систем [11]. Також деякі роботи зосереджені на удосконалення епідеміологічних моделей для моделювання поширення шкідливого ПЗ [12].

Метою статті є короткий аналіз сучасних методів і моделей емуляції негативних впливів на інформаційні системи. Стаття спрямована на виявлення ефективних підходів для моделювання загроз та розробку стратегій підвищення безпеки й надійності систем.

Виклад основного матеріалу. Атаки відмови в обслуговуванні (*Denial of Service*, DoS) та розподілені атаки відмови в обслуговуванні (*Distributed Denial of Service*, DDoS) є одними з найбільш поширених та небезпечних загроз для інформаційних систем. Вони спрямовані на вичерпання ресурсів системи, роблячи її недоступною для користувачів. Емуляція таких атак є важливим інструментом для оцінки стійкості та безпеки системи, а також для розробки ефективних механізмів захисту. Атаки DoS/DDoS базуються на ідеї перевантаження ресурсів цільової системи, що може включати процесорний час, пам'ять, пропускну здатність мережі або інші критичні ресурси. У розподілених DDoS атаках використовується велика кількість скомпрометованих пристроїв (так званих «ботів») для одночасного надсилання запитів до цілі, що ускладнює їх виявлення та блокування. Емуляція DoS/DDoS атак полягає в моделюванні умов, що відповідають реальним атакам, з метою оцінки реакції системи та її здатності протистояти таким загрозам. Це дозволяє виявити вразливості в архітектурі системи, конфігурації мережі та налаштуваннях безпеки. Розглянемо основні методи емуляції DoS/DDoS атак:

1. Генерація трафіку високої інтенсивності: Створення великої кількості запитів до системи для перевірки її здатності обробляти навантаження. Це може бути досягнуто за допомогою спеціалізованих інструментів, що генерують трафік певного типу.

2. Симуляція різних типів атак: Емуляція специфічних протоколів або вразливостей, наприклад, атаки на рівні мережевих протоколів (SYN flood, UDP flood) або на рівні додатків (HTTP flood).

3. Використання розподілених інструментів: Моделювання DDoS-атак шляхом одночасного запуску трафіку з декількох джерел або за допомогою віртуалізації для імітації великої кількості атакуючих вузлів.

Далі опишемо основні моделі для емуляції трафіку DoS/DDoS атак. Модель Пуассона широко використовується для моделювання випадкових подій у часі, включаючи мережевий трафік. У контексті DoS/DDoS атак, процес Пуассона може моделювати кількість пакетів або запитів, що надходять до сервера за певний інтервал часу. Нехай N(t) – число подій (прибуття пакетів) до моменту часу t. Процес Пуассона з параметром λ має такі властивості:

$$P(N(t)=k)=\frac{(\lambda t)^k e^{-\lambda t}}{k!}. \quad (1)$$

Інтервали між подіями є незалежними та експоненційно розподіленими з параметром λ:

$$f_T(t)=\lambda e^{-\lambda t}. \quad (2)$$

У простих моделях DoS атак припускається, що атакуючі генерують пакети з постійною середньою інтенсивністю λ. Це дозволяє оцінити навантаження на систему та аналізувати її стійкість до атак з відомою інтенсивністю. Реальний трафік DoS/DDoS атак може бути більш непередбачуваним та самоподібним, що не повністю описується процесом Пуассона [1].

Провівши обчислення та порівнявши реальний мережевий трафік (з датасету CIC-IDS2017) та, згенерований за пуассонівською моделлю з тим самим середнім λ Дисперсія в реальних даних набагато більша (≈400) проти 24.2 у класичного пуассонівського розподілу. Пуассонівська модель не відображає кореляцій реального трафіку, бо реальна дисперсія та автокореляція значно вищі. Це свідчить про необхідність складніших моделей.

Фрактальні та самоподібні моделі трафіку.

Фрактальні моделі враховують довгострокову залежність та самоподібність мережевого трафіку. Інтернет-трафік часто має властивість самоподібності, що характеризується важкими хвостами в розподілах та довгостроковою залежністю. Фрактальні моделі можна представити за допомогою автокореляційної функції з повільним спаданням:

$$R(k) \sim k^{-\beta},\ 0<\beta<1 \tag{3}$$

Херстовий показник (Hurst parameter) H:

$$H=1-\frac{\beta}{2}, \tag{4}$$

де H∈(0,5,1) для самоподібних процесів.

Самоподібні моделі дозволяють більш точно описати характер трафіку під час DDoS атак, враховуючи його нерівномірність.[2]

Дисперсія фрактальної моделі (≈ 320) вища, ніж у Пуассона, і ближча до реальних даних CIC-IDS2017 (≈ 400), отже краще відображає непостійність трафіку. Автокореляційна функція у фрактальному трафіку повільно спадає (0,42 → 0,30 → 0,25 при lag = 1,5,10), що більше схоже на реальні дані (0,37 → 0,19 → 0,10), тоді як у чистому Пуассоні кореляція майже нульова.

Моделі ботнетів на основі епідеміологічних моделей.

Епідеміологічні моделі, такі як SIR (Susceptible-Infectious-Recovered), використовуються для моделювання поширення ботнетів у мережі. Модель дозволяє оцінити розмір ботнету I(t) у часі, що визначає потенційну потужність DDoS атаки.

$$\frac{dS(t)}{Dt} = -\beta S(t)I(t); \tag{5}$$

$$\frac{dI(t)}{dt} = \beta S(t)I(t) - \gamma I(t); \tag{6}$$

$$\frac{dR(t)}{dt} = \gamma I(t), \tag{7}$$

де S(t) – кількість вразливих вузлів у момент часу t, I(t) – кількість інфікованих вузлів (ботів), R(t) – кількість відновлених або захищених вузлів, β – швидкість інфікування, γ – швидкість відновлення [3].

У контексті ботнетів важливо розглянути методи симуляція вірусів та шкідливого ПЗ оскільки це є важливим аспектом дослідження кібербезпеки, що дозволяє вивчати поведінку зловмисного програмного забезпечення без ризику заподіяння реальної шкоди. Метою симуляції є розуміння механізмів поширення, інфікування та впливу шкідливого ПЗ на інформаційні системи, а також розробка ефективних методів виявлення та захисту.

Вищеописана епідеміологічна модель, як SIR (Susceptible-Infectious-Recovered) та її варіації, широко використовуються для моделювання поширення вірусів та шкідливого ПЗ у комп'ютерних мережах. Ці моделі описують динаміку інфікування вузлів мережі та

їх відновлення [8]. Також необхідно згадати про методи машинного навчання та штучного інтелекту які можуть застосовуватися для моделювання поведінки шкідливого ПЗ та розробки систем його виявлення на основі аналізу великих обсягів даних. Здебільшого методи машинного навчання застосовуються для автоматичного виявлення шкідливого ПЗ на основі поведінкових та статичних ознак, моделювання еволюції шкідливого ПЗ, що адаптується до засобів захисту та розробка активних систем безпеки, які можуть передбачати нові загрози [9; 10].

Також варто згадати застосування теорія ігор для моделювання взаємодії між атакуючим та захисником як стратегічної гри, де обидві сторони прагнуть оптимізувати свої дії. Визначення оптимальних стратегій для обох сторін, де жоден з гравців не може покращити свій виграш, змінюючи стратегію односторонньо. Модель дозволяє аналізувати оптимальні стратегії захисту та атаки, враховуючи можливі дії супротивника, та допомагає ухвалювати рішення щодо інвестицій у безпеку [4].

Та моделювання атак на рівні додатків за допомогою теорії керованих автомата. Такий підхід використовує теорію керованих автоматів для моделювання поведінки системи під час атак на рівні додатків, таких як HTTP-флуд атаки. Дозволяє аналізувати, як послідовність зловмисних запитів може перевести систему в перевантажений або відмовний стан [5].

Ін'єкція вразливості (Fault Injection).

Ін'єкція вразливості є методологією тестування та верифікації, що полягає в навмисному введенні помилок або відмов у систему з метою оцінки її надійності, стійкості та здатності до відновлення. Цей підхід дозволяє імітувати негативні впливи на ресурси інформаційних систем і є критичним для виявлення вразливостей та забезпечення безперебійної роботи системи в умовах реальних відмов. Ін'єкція вразливості базується на принципах теорії надійності та відмовостійкості систем. Відповідно до моделі відмов система може піддаватися різним видам помилок: апаратним, програмним або викликаним зовнішніми факторами. Метод ін'єкції вразливості дозволяє дослідити реакцію системи на такі помилки та оцінити її здатність до коректного функціонування або відновлення після відмов. Виділяють такі типи методів:

1. Апаратна ін'єкція вразливості: використовує фізичні засоби для створення відмов апаратних компонентів, наприклад, введення електричних перешкод, радіаційного випромінювання або зміни параметрів живлення.

2. Програмна ін'єкція вразливості: введення помилок на рівні програмного забезпечення шляхом модифікації коду, змінних, виклику помилкових функцій або використання спеціалізованих інструментів для ін'єкції помилок у процес виконання програми.

3. Ін'єкція вразливості на рівні даних: маніпуляція даними, що передаються між компонентами системи, з метою перевірки стійкості до корупції даних, неочікуваних або некоректних значень.

4. Мережева ін'єкція вразливості: емуляція мережевих відмов, таких як затримки, втрата пакетів, порушення з'єднань, для оцінки стійкості системи до нестабільності мережі.

Застосування ін'єкції вразливості.

1. Верифікація систем безпеки: оцінка здатності системи протистояти атакам або несправностям, що можуть бути викликані зловмисниками або непередбаченими подіями.

2. Тестування розподілених систем: перевірка стійкості кластерних, хмарних сервісів та мікросервісних архітектур до відмов окремих компонентів або вузлів.

3. Розробка відмовостійких систем: виявлення слабких місць та вдосконалення механізмів відновлення, резервування та масштабування.

Для моделювання надійності систем із відмовами та відновленням також використовують Марковські процеси. Марковські моделі описують різні стани системи та ймовірності переходів між ними, що виникають через введення помилок і процеси відновлення,

дозволяючи оцінити вплив помилок на ймовірність безвідмовної роботи системи та визначити оптимальні параметри відновлення для мінімізації часу простою. І аналогічно до попереднього процес Пуассона застосовується для моделювання випадкових подій у часі, таких як введення помилок або відмов компонентів, з певною середньою інтенсивністю. Це дозволяє планувати експерименти фолт інжекції, визначати частоту та кількість помилок, а також аналізувати вплив інтенсивності введення помилок на загальну надійність системи [6].

Хаос-інжиніринг (Chaos Engineering).

Хаос-інжиніринг є сучасною методологією випробування розподілених комп'ютерних систем, що полягає у навмисному введенні несправностей та відмов з метою оцінки їхньої стійкості та надійності в умовах непередбачуваних подій. Цей підхід дозволяє моделювати негативні впливи на ресурси інформаційних систем, сприяючи виявленню прихованих вразливостей та підвищенню здатності системи витримувати збої. Теоретичні основи хаос-інжинірингу базуються на принципах теорії складних систем та стохастичних процесів. Сучасні розподілені системи характеризуються високою складністю та динамічністю, що призводить до виникнення непередбачуваних взаємодій між компонентами. Це може спричинити відмови, які важко передбачити та запобігти традиційними методами тестування. Хаос-інжиніринг дозволяє досліджувати поведінку таких систем, моделюючи реальні умови експлуатації та потенційні несправності. Основний принцип хаос-інжинірингу полягає у проведенні експериментів, що навмисно вводять зміни або відмови в систему, для перевірки її здатності підтримувати нормальну роботу. Процес починається з визначення нормального стану системи шляхом встановлення базових метрик стабільності та продуктивності. Після цього формулюються гіпотези щодо очікуваної поведінки системи при введенні несправностей. Проведення експериментів дозволяє перевірити ці гіпотези, а аналіз результатів дає змогу порівняти фактичну поведінку з очікуваною та виявити можливі розбіжності.

Методологія хаос-інжинірингу передбачає використання різних підходів для моделювання несправностей. Це може включати відключення окремих сервісів або вузлів для оцінки здатності системи продовжувати роботу без них; введення мережевих несправностей, таких як затримки, втрата пакетів чи розриви з'єднань, для перевірки стійкості мережевих взаємодій; зміну ресурсів системи, наприклад, зменшення доступної пам'яті чи процесорної потужності, для оцінки поведінки в умовах обмежень; а також моделювання атак на рівні безпеки з метою перевірки ефективності захисних механізмів.

Застосування хаос-інжинірингу є особливо актуальним у великих розподілених системах, таких як хмарні платформи, мікросервісні архітектури та системи контейнеризації. Цей підхід дозволяє підвищити надійність та доступність системи, виявити та усунути слабкі місця, що можуть призвести до відмов, покращити реакцію на інциденти шляхом розробки та відпрацювання процедур реагування на збої, а також оптимізувати архітектуру системи для підвищення її стійкості до несприятливих умов.

Використання Монте-Карло симуляцій для хаос-інжинірингу.

Використання методу Монте-Карло в хаос-інжинірингу дозволяє моделювати складні системи та процеси шляхом багаторазового випадкового вибору значень змінних і аналізу отриманих результатів. Цей чисельний підхід є особливо корисним для моделювання та аналізу систем, які мають випадкову або стохастичну природу, що характерно для хаотичних експериментів у інформаційних системах. У контексті хаос-інжинірингу метод Монте-Карло допомагає моделювати вплив випадкових несправностей та відмов на інформаційні системи, що дозволяє оцінити стійкість системи, ймовірність відмов та інші статистичні характеристики в умовах хаотичних експериментів. Математично цей метод включає визначення випадкових змінних та їх розподілів, таких як час до відмови

компонентів або час відновлення після відмови. Для кожної симуляції генеруються випадкові значення цих змінних відповідно до заданих розподілів, використовуючи генератори випадкових чисел та статистичні методи для забезпечення достовірності моделювання. Поведінка системи з введеними несправностями моделюється шляхом симуляції подій відмов та відновлення, відстежуючи стан кожного компонента у часі, враховуючи взаємозв'язок між компонентами та можливі каскадні відмови. Стан системи оновлюється відповідно до подій і після відновлення компонента система може повертатися до нормального функціонування або залишатися в деградованому стані залежно від структури системи. Процес симуляції повторюється багаторазово для отримання статистично значущих результатів, збираючи дані про часи відмов, відновлення, тривалість простою системи та інші показники для подальшого аналізу. Застосування методу Монте-Карло в хаос-інжинірингу дозволяє оцінити ймовірності відмов та інші статистичні характеристики системи під час хаотичних експериментів, моделюючи складні сценарії, які важко описати аналітичними моделями [7].

Висновки. У статті було розглянуто основні методи та моделі для емуляції негативних впливів на ресурси інформаційних систем. Зокрема, акцентовано увагу на емуляції DoS/DDoS атак, ін'єкції вразливостей та хаос-інжинірингу. Використання математичних моделей, таких як процеси Пуассона, фрактальні моделі, епідеміологічні моделі та методи Монте-Карло, дозволяє формалізувати та точно відтворити умови, що відповідають реальним загрозам. Емуляція DoS/DDoS атак за допомогою моделей трафіку та ботнетів сприяє виявленню вразливостей у мережевій інфраструктурі та розробці ефективних механізмів захисту. Ін'єкція вразливостей дозволяє протестувати стійкість систем до внутрішніх відмов, забезпечуючи підвищення надійності та безвідмовності. Хаос-інжиніринг, застосовуючи методи стохастичного моделювання та симуляцій, допомагає виявити приховані проблеми в розподілених системах та підготувати їх до непередбачуваних подій. Застосування цих методів має велике практичне значення. Воно дозволяє не лише підвищити стійкість та безпеку інформаційних систем, але й забезпечити безперервність бізнес-процесів, мінімізувати фінансові втрати та зберегти репутацію організацій. Крім того, такі підходи сприяють вдосконаленню процесів розробки та експлуатації систем, роблячи їх більш адаптивними до сучасних викликів кібербезпеки. У майбутніх дослідженнях варто приділити увагу розвитку інтегрованих підходів, що поєднують різні методи емуляції та моделювання для більш комплексного аналізу систем. Також перспективним є використання технологій штучного інтелекту та машинного навчання для автоматизації процесів виявлення вразливостей та адаптивної реакції на загрози. Таким чином, методи та моделі емуляції негативних впливів є невід'ємною складовою сучасної практики забезпечення безпеки та надійності інформаційних систем. Вони надають можливість проактивно реагувати на потенційні загрози, підвищуючи стійкість систем та захищаючи критичні ресурси в умовах постійно розвитку кіберзагроз.

Список використаних джерел

1. Dovrolis, C. What do packet dispersion techniques measure? [Electronic resource] / C. Dovrolis, P. Ramanathan, D. Moore. – Accessed mode: https://www.researchgate.net/publication/3893862.

2. On the self-similar nature of Ethernet traffic [Electronic resource] / W. Leland, M. Taqqu, W. Willinger, D. Wilson. – Access mode: https://dl.acm.org/doi/10.1109/90.282603.

3. Zou, C. C. Worm propagation modeling and analysis under dynamic quarantine defense [Electronic resource] / C. C. Zou, W. Gong, D. Towsley. – Accessed mode: https://dl.acm.org/doi/10.1145/948187.948197.

4. Alpcan, T. A game theoretic approach to decision and analysis in network intrusion detection [Electronic resource] / T. Alpcan, T. Başar. – Accessed mode: https://ieeexplore.ieee.org/document/1273013.

5. Bhuyan, M. H. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection [Electronic resource] / M. H. Bhuyan, D. K. Bhattacharyya, J. K. Kalita. – Accessed mode: https://www.researchgate.net/publication/264810679.

6. Lala, J. H. Architectural principles for safety-critical real-time applications [Electronic resource] / J. H. Lala, R. E. Harper. – Accessed mode: https://ieeexplore.ieee.org/document/259424.

7. Rubinstein, R. Y. Simulation and the Monte Carlo Method [Electronic resource] / R. Y. Rubinstein, D. P. Kroese. – Accessed mode: https://onlinelibrary.wiley.com/doi/book/10.1002/9781118631980.

8. The monitoring and early detection of Internet worms [Electronic resource] / C. C. Zou, D. Towsley, W. Gong, L. Gao. – Accessed mode: https://ieeexplore.ieee.org/document/1528487.

9. Saxe, J. Deep neural network based malware detection using two dimensional binary program features [Electronic resource] / J. Saxe, K. Berlin. – Accessed mode: https://arxiv.org/abs/1508.03096.

10. Hamarshe, A. Detection of DDoS Attacks in Software Defined Networking Using Machine Learning Models [Electronic resource] / A. Hamarshe, H. I. Ashqar, M. N. Hamarsheh. – Accessed mode: https://ieeexplore.ieee.org/document/8985747.

11. Yadav, R. Harnessing Chaos: The Role of Chaos Engineering in Cloud Applications and Impacts on Site Reliability Engineering [Electronic resource] / R. Yadav. – Accessed mode: https://www.researchgate.net/publication/381479001

12. Modeling Self-Propagating Malware with Epidemiological Models [Electronic resource] / A.Chernikova, N. Gozzi, S. Boboila, N. Perra, T. Eliassi-Rad, A. Oprea. – Accessed mode: https://arxiv.org/abs/2208.03276.

References

1. Dovrolis, C., Ramanathan, P., Moore, D. (2001). What do packet dispersion techniques measure? *Proceedings of IEEE INFOCOM* (vol. 2, pp. 905-914). https://www.researchgate.net/publication/3893862.

2. Leland, W., Taqqu, M., Willinger, W., Wilson, D. (1994). On the self-similar nature of Ethernet traffic. *IEEE/ACM Transactions on Networking* (TON), 2(1), 1-15. https://dl.acm.org/doi/10.1109/90.282603.

3. Zou, C. C., Gong, W., Towsley, D. (2023). Worm propagation modeling and analysis under dynamic quarantine defense. *WORM '03: Proceedings of the 2003 ACM workshop on Rapid malcode* (pp. 51-60). https://dl.acm.org/doi/10.1145/948187.948197.

4. Alpcan, T., Başar, T. (2004). A game theoretic approach to decision and analysis in network intrusion detection. 42nd IEEE International Conference on Decision and Control (IEEE Cat. No.03CH37475). https://ieeexplore.ieee.org/document/1273013.

5. Bhuyan, M. H., Bhattacharyya, D. K., Kalita, J. K. (2014). An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. *Pattern Recognition Letters.* https://www.researchgate.net/publication/264810679.

6. Lala, J. H., Harper, R. E. Architectural principles for safety-critical real-time applications. *Proceedings of IEEE INFOCOM* (Vol. 82(1)). (pp. 25-40). https://ieeexplore.ieee.org/document/259424.

7. Rubinstein, R. Y., Kroese, D. P. (2016). Simulation and the Monte Carlo Method. Book Series: Wiley Series in Probability and Statistics. John Wiley & Sons. https://onlinelibrary.wiley.com/doi/book/10.1002/9781118631980.

8. Zou, C. C., Towsley, D., Gong, W., Gao, L. (2005). The monitoring and early detection of Internet worms. *IEEE/ACM Transactions on Networking* (Vol. 13(5)). https://ieeexplore.ieee.org/document/1528487.

9. Saxe, J., Berlin, K. (2015). Deep neural network based malware detection using two dimensional binary program features. *Cornell University.* https://arxiv.org/abs/1508.03096

10. Hamarshe, A., Ashqar, H. I., Hamarsheh, M. N. (2023). Detection of DDoS Attacks in Software Defined Networking Using Machine Learning Models. *ResearchGate.* https://www.researchgate.net/publication/369198910_Detection_of_DDoS_Attacks_in_Software_Defined_Networking_Using_Machine_Learning_Models.

11. Yadav, R. Harnessing Chaos: The Role of Chaos Engineering in Cloud Applications and Impacts on Site Reliability Engineering. *International Journal of Computer Trends and Technology, 72*(6), 25-30. https://www.researchgate.net/publication/381479001.

12. Chernikova, A., Gozzi, N., Boboila, S., Perra, N., Eliassi-Rad, T., Oprea, A. (2022). Modeling Self-Propagating Malware with Epidemiological Models. *Cornell University.* https://arxiv.org/abs/2208.03276.

Отримано 20.11.2024

TECHNICAL SCIENCES AND TECHNOLOGIES

UDC 004.94

Denis Kuzmenko

PhD Student of Department of Information and Computer Systems
Chernihiv Polytechnic National University (Chernihiv, Ukraine)
E-mail: deniskuzmenko961@gmail.com. **ORCID** https://orcid.org/0009-0009-0314-568X

METHODS AND MODELS FOR EMULATING NEGATIVE IMPACTS ON INFORMATION SYSTEM RESOURCES

Modern information systems and existing protection methods often cannot keep up with the rapid evolution of threats, and traditional approaches to security testing do not always allow for the identification of all potential vulnerabilities. Methods of emulating negative impacts on information system resources are in a stage of active development and are used in various fields, but they require further improvement and systematization. The aim of the article is to uncover and analyze modern methods and models of emulating negative impacts in a broader context, as well as to determine their advantages, limitations, and areas of application. The study examines the emulation of DoS/DDoS attacks using traffic models, such as the Poisson model and fractal models, as well as modeling botnets based on epidemiological models. Methods of fault injection and chaos engineering, along with machine learning and artificial intelligence techniques, have been investigated as tools for testing system reliability and fault tolerance. The conclusion of this study is that the application of mathematical models such as Poisson processes, fractal models, epidemiological models, and Monte Carlo methods allows for more accurate modeling of negative impacts and assessment of system resilience to various types of attacks and failures. A comprehensive approach to emulating negative impacts, which combines different methods and models, is necessary for enhancing cybersecurity levels. This approach allows not only for the detection of existing vulnerabilities, but also for proactive responses to potential threats. The detection and neutralization of these attacks is a complex task that requires a comprehensive approach integrating various modeling, analysis, and counteraction methods.

Keywords: *emulation of negative impacts; information systems; DoS/DDoS attacks; Poisson model; fractal models; epidemiological models; fault injection; chaos engineering; machine learning; artificial intelligence; cybersecurity; botnet modeling; Monte Carlo simulations; game theory; system fault tolerance.*

References: 12.

Кузьменко Д. В. Методи та моделі емуляції негативних впливів на ресурси інформаційних систем. *Технічні науки та технології.* 2024. № 4(38). С. 189-196.