© Akhramovych V.M., Ilienko A.V., Fesenko A.O., Akhramovych V.V. Study of a linear model of interaction between traffic overflow and dos attacks in a network and server // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 74-84. © This is an open access article under the CC BY 4.0 International license.*

DOI: 10.18372/2225-5036.32.21650

ДОСЛІДЖЕННЯ ЛІНІЙНОЇ МОДЕЛІ ВЗАЄМОДІЇ МІЖ ПЕРЕПОВНЕННЯМ ТРАФІКУ ТА DOS АТАКАМИ В МЕРЕЖІ ТА СЕРВЕРІ

Володимир Ахрамович, Анна Ільєнко, Андрій Фесенко,

Вадим Ахрамович

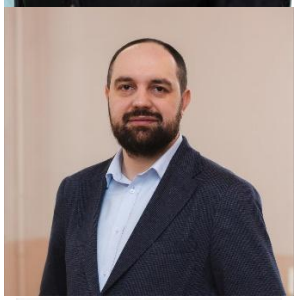
Державний університет: «Київський авіаційний інститут»
Національна академія статистики, обліку та аудиту



АХРАМОВИЧ Володимир Миколайович, д.т.н., проф.
Рік та місце народження: 1951р., с. Бовище, Поліського району, Київської обл.
Освіта: Київський політехнічний інститут 1980р.
Посада: Професор кафедри кібербезпеки Державний університет: «Київський авіаційний інститут»,
Наукові інтереси: кібербезпека, інформаційна безпека, технічний захист інформації,- захист мереж, автоматизація захисту інформації.
Публікації: більше 230 наукових праць, серед них: монографії, наукові статті , підручники та навчально -методичні посібники.
E-mail: 12z@ukr.net
Orcid ID: https://orcid.org/0000-0002-0086-9131



ІЛЬЄНКО Анна Вадимівна, к.т.н., доцент
Рік та місце народження: 1987р., м.Венспілс, Латвія
Освіта: Національний авіаційний університет, 2009
Посада: Завідувач кафедри кібербезпеки Державного університету «Київський авіаційний інститут»
Наукові інтереси: кібербезпека, інформаційна безпека, методи побудови та аналізу криптосистем, захищені інформаційні та комунікаційні системи і технології
Публікації: більше 200 наукових праць, серед них: монографії, посібник, статті у вітчизняних та міжнародних фахових виданнях, навчально-методичні комплекси дисциплін, матеріали і тези доповідей на конференціях, патенти на корисні моделі
E-mail: anna.ilienko@npp.kai.edu.ua
Orcid ID: https://orcid.org/*0000-0001-8565-1117*



ФЕСЕНКО Андрій Олексійович, к.т.н., доцент
Рік та місце народження: 1988 р., смт. Дігтярі Срібнянського району, Чернігівської обл.
Освіта: Національний авіаційний університет 2011р.
Посада: Декан факультету комп'ютерних наук та технологій Державний університет «Київський авіаційний інститут»,
Наукові інтереси: інформаційна та кібербезпека, системи захисту інформації, захист критичної інформаційної інфраструктури, криптографічні методи.
Публікації: більше 70 наукових праць, серед них: колективні монографії, наукові статті , підручники та навчально -методичні посібники, в тому числі - 34 Scopus
E-mail: andrii.fesenko@npp.kai.edu.ua
Orcid ID: 0000-0001-5154-5324



АХРАМОВИЧ Вадим Володимирович
Рік та місце народження: 1980 р., м. Київ.
Освіта:, Київський політехнічний інститут 1993р.
Посада: Завідувач ком'ютерним центром, Національної академії статистики, обліку та аудиту.
Наукові інтереси: кібербезпека, програмування, програмне та технічне забезпечення захисту інформації, мережі.
Публікації: більше 20 наукових праць, в тому числі - 4 Scopus,
E-mail: 12zstzi@ukr.net
ORCID ID: https://orcid.org/0009-0003-2787-8745

Анотація. У роботі досліджено лінійну математичну модель взаємодії між переповненням мережевого трафіку та DOS/DDoS-атаками в інформаційній системі «мережа–сервер». Запропоновано формалізований підхід до опису динаміки інформаційного потоку та рівня захищеності системи з урахуванням інтенсивності загроз, швидкості їх дії та ефективності захисних заходів. Побудовано систему диференціальних рівнянь, що описує поведінку системи поблизу стаціонарного стану, та виконано її аналіз методом малих відхилень. Показано, що лінійна модель приводить до рівняння гармонічного осцилятора з затухаючою амплітудою. Визначено основні параметри системи захисту: власну частоту коливань, період коливань і коефіцієнт демпфування. Проведено

© Akhramovych V.M., Ilienko A.V., Fesenko A.O., Akhramovych V.V. Study of a linear model of interaction between traffic overflow and dos attacks in a network and server // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 74-84. © This is an open access article under the CC BY 4.0 International license.*

імітаційне моделювання у дискретному часі, яке дозволило виявити області лінійної та нелінійної поведінки системи. Отримані результати можуть бути використані для аналізу стійкості мережевих і серверних ресурсів до DOS-атак та для обгрунтування вимог до систем захисту.

Ключові слова: DOS-атака, DDoS-атака, переповнення трафіку, інформаційна безпека, лінійна модель, гармонічний осцилятор, демпфування, мережа, сервер.

Постановка проблеми

Сучасні мережеві та серверні інформаційні системи функціонують в умовах постійного зростання обсягів мережевого трафіку та ускладнення сценаріїв DOS/DDoS-атак. Однією з ключових загроз є переповнення трафіку, яке призводить до зниження доступності ресурсів або повної відмови в обслуговуванні легітимних користувачів. Практична реалізація таких атак тісно пов'язана з динамічними процесами у мережі та на сервері, що ускладнює їх аналіз і прогнозування.

Наявні підходи до захисту здебільшого базуються на емпіричних або евристичних методах, які не завжди дозволяють формально оцінити вплив інтенсивності атак, швидкості їх реалізації та рівня захищеності системи на загальну стійкість. У зв'язку з цим актуальною є задача побудови математичної моделі, яка б дозволила дослідити взаємодію між переповненням трафіку та DOS-атаками, визначити умови стаціонарності та оцінити характер динамічної поведінки системи захисту.

Аналіз останніх досліджень і публікацій

В статті [1] розроблено математичну модель захисту корпоративної мережі та проведено її дослідження. Розглянуто залежність величини рівня захисту від потоку інформації в корпоративній мережі, а також вплив параметрів, що діють на систему захисту та функціонування системи. Визначено взаємозв'язок між захищеністю мережі, розмірами системи та загрозами безпеці. Отримано систему лінійних рівнянь, яка відображає зміну рівня захищеності від швидкості потоку інформації залежно від та впливу заходів безпеки: контролю цілісності та автентичності даних, обмеження доступу, функціонування антивірусного захисту та Firewall, резервного копіювання, аудиту, фізичних заходів захисту, боротьби з побічним електромагнітним випромінюванням, а також впливу можливих збоїв та відмов апаратного і програмного забезпечення. Досліджено вплив кількості персональних даних на їх витік, швидкість витоку та ефективність механізмів захисту.

У результаті розв'язання системи лінійних диференціальних рівнянь отримано математичні та графічні залежності рівня захищеності корпоративної мережі від різних чинників. Розглянувши три варіанти вирішення рівняння близько стаціонарного стану системи, можна прийти до висновку, що, виходячи з умов співвідношення дисипації і власної частоти коливань величини, загасання останньої до певного значення здійснюється періодично, з затухаючо. амплітудою, або експоненціально згасаючим законом. Виконано більш наочний аналіз поведінки системи, перейшовши від диференціальної форми рівнянь до дискретної і промоделювати деякий інтервал існування системи. Для більш наочного аналізу виконано перехід від диференціальної форми рівнянь до дискретної та промодельовано еволюцію системи у вибраному часовому інтервалі.

Представлено математичні та графічні залежності частоти власних коливань системи, коефіцієнта загасання та періоду коливань. Проведено імітаційне моделювання з відхиленнями від стаціонарного стану, що підтвердило нелінійність системи захисту корпоративної мережі.

В статтях [2-6] показані математичні моделі на основі нелінійних систем рівнянь для визначення впливу різних динамічних параметрів, в тому числі, від параметрів центральності мережі, відстані та взаємовпливу між користувачами, об'ємом еволюції, кількості співтовариств в соціальних мережах на систему захисту та визначення кількісного показника захисту.

В роботі [7] переведено дослідження методів захисту корпоративної мережі, збір та аналіз інформації з приводу політик безпеки. Було проведено опитування серед експертів, для виявлення найважливіших місць у технічному захисті, що можуть бути використані проти методів соціальної інженерії. Для цього результати опитування було проаналізовано та вибрано основні критерії. Далі, використовуючи матриці переваг та математичний аналіз було виявлено які критерії з обраних є найважливішими, та вказано фактори котрі можуть як позитивно так і негативно вплинути на обрані основні критерії. Це необхідно для того, щоб розуміти як саме можна захиститися від методів соціальної інженерії.

В статті [8] розглянуті основні принципи оцінки ефективності захисту інформації в розподілених корпоративних мережах. Обгрунтована необхідність створення систем комплексної оцінки захисту інформації в розподілених корпоративних мережах, в яких обробляється інформація з обмеженим доступом. Обгрунтовані основні положення проведення пентестінгу в інформаційно-телекомунікаційних системах.

В статті [9] представлена власна реалізація рішення в галузі захисту інформації корпоративних мереж, мета якої забезпечити захист від одних з найбільш поширених веб загроз, а саме SQL Injection та Cross-site scripting.

В статті [10] вказується, що аналіз текстів глобального інформаційного простору дозволяє скоротити час виявлення можливих загроз. Аналіз останніх досліджень і публікацій. Були розглянуті останні публікації щодо систем захисту від атак та використання аналізу текстів у разі виявлення загроз. Виділення недосліджених частин загальної проблеми. Вдосконалення методів опрацювання масивів даних тіла мережевих пакетів, вмісту інтернет-сторінок, інформації СМІ та соціальних мереж, що у свою чергу порушує проблему семантико-синтаксичної обробки текстів природної мови. Постановка завдання. Організація колективного захисту корпоративних мереж шляхом впровадження систем моніторингу загроз, активної

розвідувальної діяльності в глобальному інформаційному просторі з метою пошуку, збору та аналізу даних про атаки, аномальну поведінку, вміщуваний контент ресурсів мережі Інтернет.

В статті [11] проведена організація на несанкціоноване проникнення. Проведено моделювання тестування на несанкціонований доступ до вибраних інформаційних ресурсів та охарактеризовано можливі атаки після здобуття такого доступу. Наведено найбільш типові методи експлуатації можливих вразливостей укорпоративних мережах. Вибрано дистрибутив Kali Linux, оскільки він містить багато інструментів для тестування на проникнення, що дозволяє проводити як періодичні тестування мереж та вузлів, так і аудит безпеки корпоративної мережі з метою виявлення існуючих уразливостей, недоліків налаштування та закриття їх ще до можливого використання зловмисниками. У ході дослідження виявлено, що кожна система по-своєму унікальна через використання різного типу сигнатур та застосувань. Таке подання вимагає поглиблених знань про атаки та документації конкретної системи від розробника для налаштування самої системи щодо спостереження за специфічними додатками. Проведені моделювання процесу виявлення мережевих атак на основі утиліт ОС Kali Linux показали, що даний засіб є практичним вибором для адміністратора безпеки і дозволяє йому своєчасно виявити загрози інформаційній системі та проводити ефективний моніторинг операційного середовища в реальному часі.

В статті [12] з'ясовано, що реалії сучасного бізнесу – це доступ відповідних працівників компанії до її інформаційних ресурсів з будь-якої точки місця перебування, використання ними особистих мобільних пристроїв для вільного переміщення конфіденційних даних усередині корпоративної мережі та за її межами, що призводить до серйозних ризиків забезпечення безпеки господарської 314 Збірник науково-технічних праць Науковий вісник НЛТУ України. – 2013. – Вип. 23.4 діяльності компанії. Тому керівникам служб ІБ корпоративних мереж компаній до водиться враховувати багато особливостей захисту інформації, а також знати, за до помогою яких засобів може забезпечуватися реалізація тих чи інших завдань ІБ.

В статті [13] описано аналіз концепції "нульової довіри" (ZT, Zero Trust) для забезпечення кібербезпеки корпоративних мереж. Автори прагнуть виявити найбільш ефективні методи захисту, що відповідають сучасним вимогам до кібербезпеки, дослідити їх впровадження та забезпечити безперервний моніторинг й управління ризиками в умовах зростаючих кіберзагроз.

В статті [14] розглядаються основні підходи до розробки алгоритму опти мізації системи захисту інформації корпоративної мережі. Запропоновано перехід від багатокритеріальної задачі оптимізації, до однокритеріальної. При сформульованому понятті захищеності системи оптимізаційна задача полягає в забезпеченні максималь ного рівня захищеності (як функції вартості інформації, що захи щається і ймовірності злому) при обмеженнях вартості системи захисту і впливу на продуктивність системи.

В статті [15] встановлено, що права доступу користувачам до інформаційних ресурсів корпорації встановлюються згідно розробленої політики інформаційної безпеки організації для збереження конфіденційності, цілісності та доступності корпоративної інформації.З огляду на це, в роботі розглядаються правила створення облікових даних користувачів корпоративної мережі та досліджуються способи забезпечення їх безпеки на основі мережевих операційних систем Windows. Визначено базовий список правил щодо створення, призначення та використання облікових даних, а саме: встановлення максимального обмеження адміністративних привілеїв для користувачів з привілеями адміністратора, надання користувачам та групам підтримки лише тих прав, які необхідні для виконання ними повсякденних завдань, використання облікових записів адміністраторів домену організації лише для керування контролерами домену.Організовано інсталяційний файл, який містить у собі комплекс найбільш поширених утиліт для адміністрування Active Directory (AD). Основою цього комплексу є утиліти: Account Lockout Examiner, Netwrix Auditor, SolarWinds Permissions Analyzer, Active Directory Health Profiler і Semperis DS Protector. Проведене моделювання щодо діагностики AD на предмет його захищеності показує, що використання зібраних утиліт в одному інсталяційному файлі значно спрощує процес моніторингу стану захищеності AD та проведення діагностики встановлених прав доступу користувачів.Встановлено, що найвищий рівень захищеності облікових записів привілейованих користувачів та системних адміністраторів засобами Active Directory досягається починаючи з Windows Server 2012 R2, оскільки ця ОС і пізніші версії володіють функціоналом захищеної групи користувачів, що дає змогу отримати додатковий захист проти компрометації їхоблікових даних при виконанні процедури перевірки автентичності.Ключові слова:мережева операційна система, облікові дані користувачів, контролер домену, права доступу користувачів, служба каталогів, сервер, корпоративна інформація.

В статті [16] розглядаються існуючі методи захисту комп'ютерних систем (КС), а також нового підходу – адаптивного захисту.

Разом з безперервним розвитком ІТ з'являються все нові способи несанкціонованого проникнення в КС. Існуючі традиційні механізми захисту, реалізовані в міжмережевих екранах, серверах аутентифікації, системах розмежування доступу і так далі, по суті є засобами, блокуючими атаки. Для побудови захищеної мережі потрібні засоби, які не лише виявляють і блокують атаки, але і попереджують їх. На підставі вимог до захищеної комп'ютерної системи в цій роботі будуть розглянуті існуючі методи захисту КС і запропонований новий підхід до захисту - адаптивний захист.

Реалізацією інформаційних систем, учасниками якої може бути обмежене коло осіб, визначене її власником, являється корпоративна

мережа (далі КМ). Головним завданням КМ є здійснення автоматизованої обробки інформації. Метою застосування засобів захисту КМ є надання єдиного захищеного мережевого простору обмеженому рамками корпорації кругу користувачів.

При створенні КМ важливим аспектом є побудова корпоративних систем захисту інформації. Реалізація системи захисту проводиться з метою протидії несанкціонованій дії на інформацію, що обробляється автоматизованою системою. При цьому передбачається, що є "джерело інформації" і "одержувач інформації", а інформація передається по каналах зв'язку.

Суб'єкти автоматизованої системи можуть проводити операції над інформацією (створення, копіювання, поширення, перетворення, обробка, зберігання і так далі). Такі операції утворюють інформаційний процес.

В статті [17] представлено математичну модель, розроблену на основі моделі Гросса для оцінки рівня інформаційної безпеки фінансових організацій за різних умов функціонування. Особливу увагу приділено ролі моделі в оптимізації розподілу ресурсів захисту для забезпечення надійності інформаційної безпеки в режимі реального часу. Запропонований підхід дозволить досягти раціонального розподілу ресурсів захисту при побудові адаптивних систем захисту інформації, що дозволить підвищити ефективність захисту від гібридних загроз. У статті запропоновано конкретну модель оцінювання інформаційної безпеки фінансових установ, що включає важливий аспект вибору критеріїв і визначення пріоритетів. Зазначено, що ефективний розподіл ресурсів захисту є ключовим пріоритетом управління інформаційною безпекою.

В статті [18] розглядаються принципи створення математичної моделі та архітектури системи шляхом застосування методу штучного інтелекту для виявлення кібератак на інформаційно-комунікаційні системи, де використовується нейронна мережа, здатна навчатися та виявляти кібератак. Запропонований підхід, заснований на застосуванні розробленої математичної моделі та архітектури штучних нейронних мереж, як детектора мережевих атак на інформаційно-комунікаційні системи, дозволяє підвищити рівень виявлення мережевих вторгнень у комп'ютерні системи, веб- та інтернет-ресурси. Запропоновано алгоритм обробки параметрів мережевого трафіку в системах реального часу шляхом структурування нейронної мережі, що дозволяє оптимізувати надлишковість її багаторівневої структури на рівні міжелементних зв'язків.

В статті [19] додатково поєднуючи важливість ефективної реалізації захисту безпеки, заснованого на алгоритмі послідовної локалізації Монте-Карло, новий метод позиціонування може підвищити надійність якірної коробки, оптимізувати область вибірки та покращити точність позиціонування вузла під час придбання якірної коробки на етапі прогнозування за рахунок інтеграції принципу RSSI та центроїда принцип. Удосконалена модель призначена для аналізу впливу мереж зв'язку на безпеку на основі алгоритму Монте-Карло. Хоча цей алгоритм певною мірою збільшує складність позиціонування, весь процес розрахунку споживає менше енергії і ефект оптимізації очевидний. Ця модель ґрунтується на кількісному аналізі загроз безпеці мережі зв'язку, методів боротьби з мережею зв'язку, атрибутів мережевої безпеки та змагальних атрибутів мережевої безпеки. Він використовує нечітку математичну теорію та адаптивні алгоритми зважування для ефективного зв'язку у випадку ефективного захисту безпеки Вплив мережевої безпеки було кількісно проаналізовано та змодельовано. Результати моделювання на основі методу Монте-Карло доводять обґрунтованість моделі, наведеної в даній роботі. Результати моделювання показують, що в порівнянні з традиційним алгоритмом позиціонування МСВ, цей алгоритм може ефективно підвищити точність позиціонування.

В статті [20] розглянуто математичні аспекти інтелектуальної системи підтримки прийняття інформаційних рішень (СППР) у сфері інформаційної безпеки. Представлено математичну модель системи. Описано реакцію на сигнал про зниження рівня захищеності IT-активів. При досягненні критичного значення цільової функції безпеки вносяться корективи в перелік заходів захисту інформації і переглядаються поточний рівень кіберризиків. Система налаштована таким чином, щоб не спрацьовувати при першій, можливо, випадковій, зовнішній сигналізації. Також в основі математичної моделі лежать фінансові обмеження організації щодо забезпечення інформаційної безпеки і враховуються ціни на блоки захисту. У статті показано зв'язок представленої математичної моделі з класичними задачами лінійного програмування. Математичне формулювання цієї моделі еквівалентне модифікованій задачі про ранець, відомій дискретній задачі оптимізації.

В статті [21] вказується, що традиційні методи безпеки виявилися недостатніми для вирішення проблеми мінливого ландшафту загроз, що призвело до потреби в більш просунутих та ефективних механізмах захисту . Нова галузь глибокого нейронного навчання виявилася перспективною в кібербезпеці, оскільки вона може вивчати складні закономірності та поведінку в даних і забезпечувати більш точні та ефективні можливості виявлення та прогнозування . Це дослідження спрямоване на розробку надійної системи кіберзахисту під назвою NeuroCyberGuard, використовуючи математичне моделювання на основі глибокого нейронного навчання. Запропонований підхід використовує можливості глибоких нейронних мереж для аналізу великих обсягів даних мережевого трафіку, виявлення потенційних загроз та надання сповіщень та реагування в режимі реального часу для запобігання порушенням безпеки. Компонент математичного моделювання дозволяє системі оптимізувати свою продуктивність та адаптуватися до змінних мережевих умов та схем атак. Система буде оцінюватися за допомогою різноманітних наборів даних для порівняння та реальних сценаріїв для перевірки її ефективності та результативності.

Очікуваним результатом цього дослідження є створення найсучаснішої системи кіберзахисту, яка забезпечує комплексний захист від кіберзагроз та покращує безпеку організацій.

В статті [22] пояснюється, що кібератаки в різних форматах, особливо відомі, постійно вимагають безперервну оцінку захищеності інформаційних систем. Ці отримані дані необхідні для вивчення і дослідження фахівцями для їх подальшого використання. Один із перспективних методів Data mining, який є прогресивним і поглибленим можливовважати вейвлет-перетворення. Алгоритм вейвлет-перетворення слід застосовувати для аналізу дискретних даних. Це важливо коли потрібна висока швидкість обробки та аналізу інформації. Що є актуальним пунктом для вирішення завдання захисту корпоративної мережі та Інтернет.

В результаті аналізу літературних даних [1–22] виявлено, що на даний момент часу відсутнє дослідження, пов'язане дослідження лінійної моделі взаємодії між переповненням трафіку та dos атаками в мережі та сервері.

Мета та постановка завдань дослідження.

Метою роботи є розроблення та аналіз лінійної математичної моделі взаємодії між переповненням мережевого трафіку та DOS-атаками в системі «мережа–сервер» з метою оцінювання стійкості та динамічних властивостей системи захисту інформації. Для досягнення поставленої мети в роботі необхідно розв’язати такі завдання: Формалізувати процес взаємодії між інтенсивністю інформаційного потоку, переповненням трафіку та рівнем захищеності мережі і сервера від DOS-атак. Побудувати систему диференціальних рівнянь, що описує динаміку параметрів системи захисту. Визначити стаціонарні стани системи та умови їх існування. Дослідити поведінку системи поблизу стаціонарного стану методом малих відхилень. Отримати аналітичні вирази для власної частоти, періоду коливань та коефіцієнта демпфування. Провести імітаційне моделювання дискретної моделі та проаналізувати лінійність і нелінійність поведінки системи захисту.

Вступ. Тип атаки "Відмова від технічного обслуговування" - це спроба заподіяти шкоду, зробивши недоступну цільову систему, наприклад, веб -сайт або додаток для звичайних кінцевих користувачів. Зазвичай зловмисники генерують велику кількість пакетів або запитів, які в кінцевому рахунку перевантажують роботу цільової системи. Якщо атака виконується одночасно з великої кількості комп'ютерів, говорять про DDoS-атаку (від англ. Distributed Denial of Service, розподілена атака типу «відмова в обслуговуванні»). Принцип експлуатації DDOS атак лежить в заголовку: відмова від обслуговування. Будь -яке обладнання має обмеження на пропускну здатність та кількість оброблених запитів. А організатор атаки встановлює завдання завантаження всіх каналів на максимум, щоб реальні користувачі не могли проникнути в послугу через величезну кількість запитів.

У загальному випадку DDoS-атаки можна розділити на типи в залежності від класу (табл. 1).

Таблиця 1

Класифікація DDoS-атак відносно OSI

Клас DDoS-атак	Рівень	Додаток	Опис	Приклад вектора
7	Додаток	Дані	Мережевий процес на адресу додатку	флуд DNS-запитів, HTTP-флуд
6	Подання	Дані	Подання та шифрування даних	SSL-порушення
5	Сеанс	Дані	Сеанс між хостами	Н/Д
4	Транспортний	Сегменти	Зв’язок між кінцевими пунктами та надійність	SYN-флуд
3	Мережевий	Пакети	Визначення маршруту та логічної адресації	Атаки з відбиванням UDP-пакетів
2	Канальний	Кадри	Фізична адресація	Н/Д
1	Фізичний	Біти	Середовище передачі, сигнали та двійкові коди	Н/Д

Розглядаючи методи запобігання таким атакам, корисно розділити їх на дві групи: атаки рівня інфраструктури (рівні 3 та 4) та атаки рівня програми (рівні 6 та 7).

Атаки рівня інфраструктури. До атак рівня інфраструктури зазвичай відносять атаки на рівнях 3 та 4. Це найбільш поширений тип DDoS-атак, який включає такі вектори, як SYN-флуд, та інші атаки відображення, такі як UDP-флуд. Подібні атаки зазвичай масові і спрямовані на те, щоб перевантажити пропускну здатність мережі або сервери програм. Проте такий тип атак має певні ознаки, тому їх легше виявити.

Атаки рівня програми. До атак рівня додатків зазвичай відносять атаки рівнях 6 і 7. Ці атаки достатньо поширені, але водночас є складнішими. Як правило, вони не такі масові, як атаки рівня інфраструктури, але націлені на певні частини програми і призводять до того, що вона стає недоступною для реальних користувачів. Як приклад можна навести потік HTTP-запитів на сторінку входу в систему, API пошуку або навіть потоки XML-RPC Wordpress (також відомі як атаки Wordpress Pingback).

Прикладний рівень (L7) -atacts, спрямовані на порушення веб-додатків. Напади цього класу дуже

© Akhramovych V.M., Ilienko A.V., Fesenko A.O., Akhramovych V.V. Study of a linear model of interaction between traffic overflow and dos attacks in a network and server // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 74-84. © This is an open access article under the CC BY 4.0 International license.*

різноманітні. Відсутність серверних ресурсів. Аналіз поведінки та кореляція необхідних серверних ресурсів. Необхідно оптимально налаштувати сервер для завдань, які він вирішує. Майже неможливо повністю автоматизувати боротьбу проти цього класу нападів.

Зниження зон, доступних для нападу. Один з перших методів нейтралізації DDOS -атак - мінімум розміром зони, який може атакувати. Така техніка обмежує можливості зловмисників для нападу та забезпечує можливість створення централізованої оборони. Необхідно переконатися, що доступ до програми чи ресурсів не був відкритий для портів, протоколів чи додатків, які не передбачені для взаємодії. Таким чином, мінімізація кількості можливих входів для атаки дозволяє зосередити зусилля на їх нейтралізації. У деяких випадках цього можна досягти, розмістивши свої обчислювальні ресурси за межами мереж вмісту (CDN) та обмежуючи прямий інтернет -трафік до певних частин їх інфраструктури, таких як сервери баз даних. Важливо використовувати брандмауери або списки контролю доступу (ACL) для контролю трафіка, що входить у програми.

План масштабування. Два основні елементи нейтралізації масштабних атак DDOS-це пропускна здатність (або транзитний потенціал) та продуктивність сервера, достатня для поглинання та нейтралізації атак.

Транзитний потенціал. При проектуванні додатків необхідно переконатися, що постачальник послуг хостингу забезпечує надлишкову потужність підключення до Інтернету, що дозволяє обробляти великі обсяги трафіку. Оскільки кінцева мета атак DDOS-впливати на наявність ресурсів або додатків, необхідно розмістити їх поблизу не тільки з кінцевими користувачами, але і з великими вузлами між мережами обміну трафіком, які легко забезпечать користувачам доступ до програми навіть з великим обсягом трафіку. Робота з Інтернет -додатками забезпечує ще ширші можливості. У цьому випадку можно використовувати мережі розподілу вмісту (CDN) та послуги інтелектуальної трансформації адрес DNS, які створюють додатковий рівень мережевої інфраструктури для підтримки вмісту та вирішення запитів DNS з місць, які часто розташовані ближче до кінцевих користувачів.

Продуктивність сервера. Більшість атак DDOS є об'ємними і споживають багато ресурсів, тому важливо мати можливість швидко збільшити або зменшити обсяг їх обчислювальних ресурсів. Це може бути надано за допомогою надмірного обсягу обчислювальних ресурсів або ресурсів із спеціальними можливостями, такими як більш продуктивні мережеві інтерфейси або вдосконалена конфігурація мережі, що дозволяє підтримувати великі обсяги трафіку. Крім того, для постійного моніторингу та розподілу навантажень між ресурсами та запобігання перевантаженню будь - якого одного ресурсу часто використовуються відповідні балансири.

Інформація про типовий та нетиповий трафік

Щоразу, коли виявляється збільшення обсягу трафіку, що надходить на хост, максимально можливий обсяг трафіку, який хост може обробляти без погіршення його доступності, можна сприймати як орієнтир. Ця концепція називається обмеженням швидкості. Більш розширені методи захисту, відповідно, мають додаткові можливості і можуть лише інтелектуально приймати трафік, який дозволений, аналізуючи окремі пакети. Для використання таких інструментів необхідно визначити характеристики хорошого трафіку, який зазвичай отримує цільовий об'єкт, і мати можливість порівнювати кожен пакет із цим стандартом.

Розгортання брандмауерів для відображення складних вкладень.

Проти нападів, які намагаються використовувати вразливість у застосуванні, наприклад, проти спроб ввести SQL -код або фальсифікацію запитів між мережами, рекомендується використовувати брандмауер веб - додатків (WAF). Крім того, через унікальність цих атак треба мати можливість незалежно нейтралізувати заборонені запити, які можуть мати певні характеристики, наприклад, можуть бути визначені як відмінні від хорошого трафіку або виходити з підозрілих IP -адрес, з несподіваних географічних регіонів тощо . Щоб нейтралізувати атаки, що відбуваються, іноді може бути корисно отримати підтримку фахівців для вивчення характеристик трафіку і створення індивідуального захисту.

Виклад основного матеріалу дослідження

Дослідження основних параметрів системи захисту

У класичному підході до захисту від DOS атак розрізняють:

$$T_i = \left[D_i, D_j \right], \qquad (1)$$

де Ti – множина загроз від DOS атак, Di –позитивна взаємодія між DOS атаками та мережею і сервером, Dj – негативна взаємодія між між DOS атаками та мережею і сервером.

Втрата такої якості як взаємодія між переповненням трафіку та DOS атаками – процес, який має часовий інтервал. Нехай функція I(t) – потік інформації. Якщо зробити припущення, що потік інформаціїї відбувається неперервно протягом проміжку часу, який є циклом спостереження, то I(t) є неперервною детермінованою величиною. Тоді швидкість зміни цього потоку визначається як похідна функції I(t), тобто $\frac{dI}{dt}$.

Логічно, що якщо потік і швидкість зміни потоку дорівнюють нулю, то наступив процес переповнення трафіку мережі, або сервера:

$$dI = 0; \ \frac{dI}{dt} = 0. \qquad (2)$$

Спроможність здійснити заходи переповненням трафіку за допомогою DOS атак безпосередньо можливий при недостатньому рівні системи захисту мережі та сервера, яка здійснює нейтралізацію загроз безпеки від переповнення трафіку від DOS атак. Нехай Z – показник захищеності інформаційної системи. Тоді

$$\frac{dI}{dt} = Z_p Z + (\sum_{i=1}^{n} C_v + \sum_{i=1}^{n} C_k) I, \qquad (3)$$

де Zp – коефіцієнт, що відображає вплив заходів які здійснюють нейтралізацію загроз безпеки від переповнення трафіку від DOS атак; $\sum_{i=1}^{n} C_v$ – коефіцієнт, що відображає вплив швидкості дії загроз безпеки на мережі та сервери від переповнення трафіку мереж та серверів DOS атаками; $\sum_{i=1}^{n} C_k$ – коефіцієнт, що відображає вплив кількості загроз безпеки від переповнення трафіку DOS атаками.

Зміст рівняння (3) полягає в наступному нейтралізація загроз безпеки від переповнення трафіку DOS атаками залежить:

– від розміру інформаційної системи (отже, в якійсь мірі і від кількості DOS атак);

– від швидкості дії загроз безпеки від переповнення трафіку DOS атаками;

– загрози безпеки від переповнення трафіку DOS атаками купірується захищенністю системи (заходами щодо нейтралізації загроз безпеки від переповнення трафіку DOS атаками).

Далі розглянуто, від чого залежить захищеність системи – Z. Визначено захищеність системи як здатність системи протистояти переповнення трафіку DOS атаками. Отже, захищеність системи буде залежати:

– від розмірів системи (як і від кількості DOS атак);

– загроз безпеки інформації від переповнення трафіку DOS атаками.

Складено рівняння:

$$\frac{dZ}{dt} = \sum_{i=1}^{n} D_m + \sum_{i=1}^{n} D_s - I\left(\sum_{i=1}^{n} C_{d2} + \sum_{i=1}^{n} C_{d1}\right), \qquad (4)$$

де прийнято: Dm – коефіцієнт, що відображає вплив загроз безпеки від переповнення трафіку DOS атаками мереж на захищеність інформаційної системи, параметр Ds коефіцієнт, що відображає вплив загроз безпеки від переповнення трафіку DOS атаками серверів на захищеність інформаційної системи, $\sum_{i=1}^{n} C_{d1}$ – коефіцієнт, що відображає вплив захищеності від переповнення трафіку DOS атаками мереж та серверів, $\sum_{i=1}^{n} C_{d2}$ – коефіцієнт, що відображає вплив кількості DOS атак на захищеність.

Рівняння (3) і (4) об'єднано в систему.

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (\sum_{i=1}^{n} C_v + \sum_{i=1}^{n} C_k) I, \\ \frac{dZ}{dt} = \sum_{i=1}^{n} D_m + \sum_{i=1}^{n} D_s - I\left(\sum_{i=1}^{n} C_{d2} + \sum_{i=1}^{n} C_{d1}\right). \end{cases} \qquad (5)$$

Знайдено стаціонарну позицію системи, що описується системою рівнянь (5). Умови стаціонарності

$$dI = 0; \ \frac{dI}{dt} = 0.$$

Отже:

$$\begin{cases} Z_p \bar{Z} \lim_{x\to\infty} + (\sum_{i=1}^{n} C_v + \sum_{i=1}^{n} C_k) \bar{I} = 0, \\ \sum_{i=1}^{n} D_m + \sum_{i=1}^{n} D_s - I\left(\sum_{i=1}^{n} C_{d2} + \sum_{i=1}^{n} C_{d1}\right) = 0. \end{cases} \qquad (6)$$

Графічна залежність представлена на рис. 1

З другого рівняння системи отримано:

$$\bar{I} = \frac{\sum_{i=1}^{n} D_m + \sum_{i=1}^{n} D_s}{\left(\sum_{i=1}^{n} C_{d2} + \sum_{i=1}^{n} C_{d1}\right)}. \qquad (7)$$

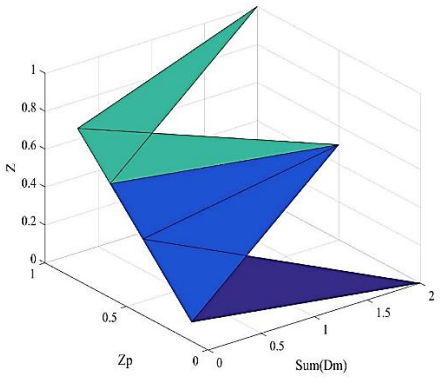
З першого рівняння системи рівнянь (6) знайдено $\bar{Z}$.

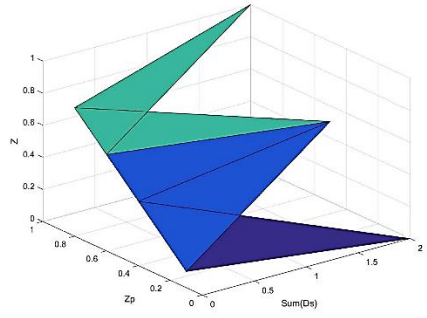
$$Z_p \bar{Z} - \frac{(\sum_{i=1}^{n} C_v + \sum_{i=1}^{n} C_k)}{\left(\sum_{i=1}^{n} C_{d2} + \sum_{i=1}^{n} C_{d1}\right)} \frac{(\sum_{i=1}^{n} D_m + \sum_{i=1}^{n} D_s)}{} = 0. \qquad (8)$$

$$\bar{Z} = \frac{(\sum_{i=1}^{n} C_v + \sum_{i=1}^{n} C_k)}{\left(\sum_{i=1}^{n} C_{d2} + \sum_{i=1}^{n} C_{d1}\right)} \frac{(\sum_{i=1}^{n} D_m + \sum_{i=1}^{n} D_s)}{Z_p}. \qquad (9)$$

Отже, умови позиції стаціонарності системи:

$$\begin{cases} \bar{I} = \frac{\sum_{i=1}^{n} D_m + \sum_{i=1}^{n} D_s}{\left(\sum_{i=1}^{n} C_{d2} + \sum_{i=1}^{n} C_{d1}\right)}, \\ \bar{Z} = \frac{(\sum_{i=1}^{n} C_v + \sum_{i=1}^{n} C_k)}{\left(\sum_{i=1}^{n} C_{d2} + \sum_{i=1}^{n} C_{d1}\right)} \frac{(\sum_{i=1}^{n} D_m + \sum_{i=1}^{n} D_s)}{Z_p}.. \end{cases} \qquad (10)$$





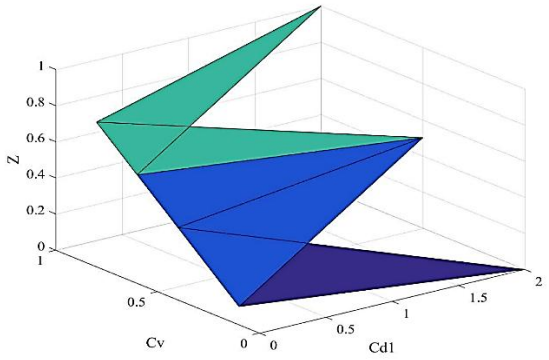


Рис. 1. Показник захисту системи мережа, сервер за (10)

Систему рівнянь (5) розв'язано методом «малих відхилень» $I = \bar{I} + I$; $Z = \bar{Z} + Z$, отже, система рівнянь прийняла вигляд:

$$\begin{cases} \frac{dI}{dt} = Z_p\left(\bar{Z} + Z\right) + \left(\sum_{i=1}^{n} C_v + \sum_{i=1}^{n} C_k\right)\left(\bar{I} + I\right), \\ \frac{dZ}{dt} = \left(\sum_{i=1}^{n} D_m + \sum_{i=1}^{n} D_s\right)\left(\sum_{i=1}^{n} C_v + \sum_{i=1}^{n} C_k\right) - \left(\bar{I} + I\right)\left(\sum_{i=1}^{n} C_{d2} + \sum_{i=1}^{n} C_{d1}\right). \end{cases} \quad (11)$$

$$\begin{cases} \frac{dI}{dt} = \left(\sum_{i=1}^{n} C_{d2} + \sum_{i=1}^{n} C_{d1}\right)Z - \left(\sum_{i=1}^{n} C_v + \sum_{i=1}^{n} C_k\right)I, \\ \frac{dZ}{dt} = -I\left(\sum_{i=1}^{n} C_{d2} + \sum_{i=1}^{n} C_{d1}\right) + \left(\sum_{i=1}^{n} D_m + \sum_{i=1}^{n} D_s\right)\left(\sum_{i=1}^{n} C_v + \sum_{i=1}^{n} C_k\right). \end{cases} \quad (12)$$

Диференціюючи перше рівняння системи (12) отримали:

$$\frac{d^2I}{dt^2} = -I(C_{d1} + C_{d2})(Z_p + \frac{dI}{dt}((\sum_{i=1}^{n} D_m) + \frac{dI}{dt}(\sum_{i=1}^{n} D_s) - \frac{dI}{dt}(\sum_{i=1}^{n} C_v) - \frac{dI}{dt}(\sum_{i=1}^{n} C_k)\sum_{i=1}^{n} C_{d2}) + \frac{dI}{dt}(\sum_{i=1}^{n} C_{d1})). \quad (13)$$

$$\frac{d^2I}{dt^2} + (\frac{dI}{dt}((\sum_{i=1}^{n} C_{d2}) + (\sum_{i=1}^{n} C_{d1}))((\sum_{i=1}^{n} D_m) + (\sum_{i=1}^{n} D_s))((\sum_{i=1}^{n} C_v) + (\sum_{i=1}^{n} C_k))) + IZp = 0, \quad (14)$$

Рівняння (14) є рівнянням гармонічного осцилятора з затухаючою амплітудою, де:

$$\omega_0 = \sqrt{Zp}. \quad (15)$$

Графік представлений на рис. 2

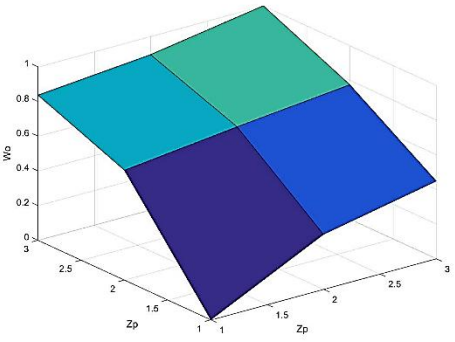


Рис. 2. Особиста частота системи мережа - сервер

$$\omega = \sqrt{Zp - \frac{(\sum_{i=1}^{n} C_{d2}) + (\sum_{i=1}^{n} C_{d1}))((\sum_{i=1}^{n} D_m) + (\sum_{i=1}^{n} D_s))^2}{4}}. \quad (16)$$

Графік представлений на рис. 3

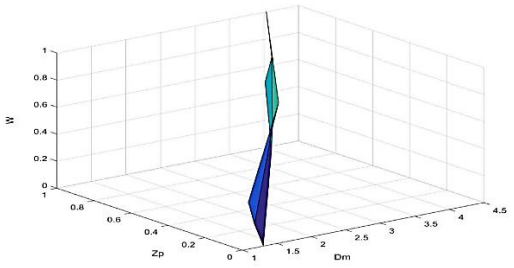


Рис. 3. Частота системи мережа-сервер

$$T = \frac{2\pi}{Z},$$

$$Z = \sqrt{Zp - \frac{(\sum_{i=1}^{n} C_{d2}) + (\sum_{i=1}^{n} C_{d1}))\left(\left(\sum_{i=1}^{n} D_m\right) + \left(\sum_{i=1}^{n} D_s\right)\right)\left(\left(\sum_{i=1}^{n} C_v\right) + \left(\sum_{i=1}^{n} C_k\right)\right)^2}{4} - \frac{((\sum_{i=1}^{n} C_v) + (\sum_{i=1}^{n} C_k))^2}{4}} \quad (17)$$

Графік представлений на рис. 4

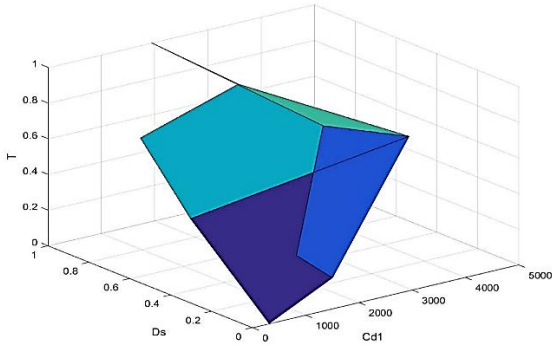


Рис. 4. Період коливань системи мережа-сервер

$$\beta = \frac{\left(\sum_{i=1}^{n} C_v\right) + \left(\sum_{i=1}^{n} C_k\right)}{2}. \quad (18)$$

Графік представлений на рис. 5

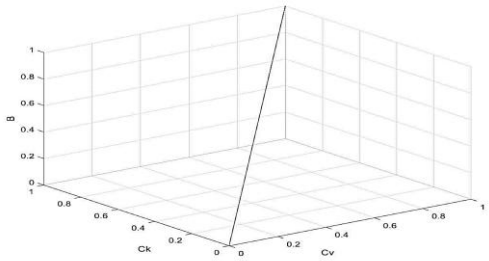


Рис. 5. Коефіцієнт демпфування системи мережа-сервер

Розв'язання рівняння гармонічного осцилятора розпалося на три випадки.

1.

$$\beta \prec \omega_0 : I = = A_0 \exp\left(\begin{array}{l} -\frac{\left(\sum_{i=1}^{n} C_v\right) + \left(\sum_{i=1}^{n} C_k\right)}{2} \times \\ \times \cos\left(\sqrt{((\sum_{i=1}^{n} C_{d2}) + (\sum_{i=1}^{n} C_{d1}))((\sum_{i=1}^{n} D_m) + (\sum_{i=1}^{n} D_s))(-\frac{\left(\sum_{i=1}^{n} C_v\right) + \left(\sum_{i=1}^{n} C_k\right)^2}{4}} t\right) + \varphi_0 \end{array}\right). \quad (19)$$

2. $\beta = \omega_0 : I = A_0 + B_0 t \exp\left(-\frac{(\sum_{i=1}^{n} C_v) + (\sum_{i=1}^{n} C_k)}{2}\right) t.$ (20)

© Akhramovych V.M., Ilienko A.V., Fesenko A.O., Akhramovych V.V. Study of a linear model of interaction between traffic overflow and dos attacks in a network and server // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 74-84. © This is an open access article under the CC BY 4.0 International license.*

$$3.\ \beta \succ \omega_0 : I = A_0\exp(-y_1 t) + B_0\exp(-y_2 t), \quad (21)$$

де:

$$y_{1,2} = \beta \mp \sqrt{\frac{\left(\sum_{i=1}^{n} C_v\right)+\left(\sum_{i=1}^{n} C_k\right)^2}{4} \mp ((\sum_{i=1}^{n} C_{d2}) + (\sum_{i=1}^{n} C_{d1}))((\sum_{i=1}^{n} D_m) + (\sum_{i=1}^{n} D_s)}} \quad (22)$$

Отже проведено дослідження лінійної моделі взаємодії між користувачами в соціальній мережі та її впливу на систему захисту. Отримано залежності гармонічного осцилятора з затухаючою амплітудою. Визначено основні параметри системи захисту: частота коливань (15), (16), період коливань (17), коефіцієнт демпфування (18). Розв'язання рівняння гармонічного осцилятора в залежності від значення параметра β, має одне з трьох представлень: (19)–(21).

Перевірка на лінійність системи захисту інформації

Розглянуто три варіанти розв'язання рівняння близько стаціонарного стану системи, зроблено наступний висновок. Виходячи з умов співвідношення диссипації і власної частоти коливань величини, загасання останньої до певного значення здійснюється періодично. Амплітуда коливань є затухаючою за експоненціально загасаючим законом. Зробимо більш наочний аналіз поведінки системи, шляхом переходу від диференціальної форми рівнянь (5), (6) до дискретної і промоделювавши деякий інтервал існування системи. А саме:

$$\begin{cases} \dfrac{I_{n+1}-I_n}{\Delta t} = ((\sum_{i=1}^{n} C_{d2}) + (\sum_{i=1}^{n} C_{d1}))Z_n - ((\sum_{i=1}^{n} C_v) + (\sum_{i=1}^{n} C_k))I_n, \\ \dfrac{Z_{n+1}-Z_n}{\Delta t} = Z_p - ((\sum_{i=1}^{n} C_{d2}) + (\sum_{i=1}^{n} C_{d1}))I_n - \\ -\left(Z_p + (\sum_{i=1}^{n} D_m) + (\sum_{i=1}^{n} D_s)\right)((\sum_{i=1}^{n} C_v) + (\sum_{i=1}^{n} C_k))I_n. \end{cases} \quad (23)$$

$$\begin{cases} I_{n+1} = I_n + \left(((\sum_{i=1}^{n} C_{d2}) + (\sum_{i=1}^{n} C_{d1}))Z_n - \left(C_v + C_K\right)I_n\right)\Delta t, \\ Z_{n+1} = Z_n + \left(\begin{array}{l} Z_n - I_n\left(\begin{array}{l}((\sum_{i=1}^{n} C_{d2}) + (\sum_{i=1}^{n} C_{d1})) + Z_p + \\ +(\sum_{i=1}^{n} D_m) + (\sum_{i=1}^{n} D_s)\end{array}\right)\times \\ \times((\sum_{i=1}^{n} C_v) + (\sum_{i=1}^{n} C_k)) \end{array}\right)\Delta t. \end{cases} \quad (24)$$

Створимо табл. 1 параметрів моделювання. Слідуючи з умови стаціонарної позиції системи, для I і Z прийняті зачення будуть рівні 0.5 і 0.5. Крок моделювання прийнято за 0.1 для всіх ітерацій моделювання, тому в таблиці його не відображено. Величини I_{sp}, Z_{sp} відображають стаціонарні значення параметрів, якщо такі були досягнуті за кінцеве число ітерацій. Далі проведено імітаційне моделювання для значень $\beta \prec \omega_0$, $\beta = \omega_0$, $\beta \succ \omega_0$ з відхиленням від стаціонарної позиції системи. Дані представлені в табл. 2.

Таблиця 2

Параметри моделювання

№ з/п	Z_p	I	Z	$\sum_{i=1}^{n} C_v$	$\sum_{i=1}^{n} C_{d1}$	$\sum_{i=1}^{n} C_{d2}$	$\sum_{i=1}^{n} C_k$	$\sum_{i=1}^{n} D_m$	$\sum_{i=1}^{n} D_s$	Параметри
1	1	0,5	0,5	1	1	1	0,5	1	1	β<ω0
2	1	0,5	0,5	2	1	1	2	1	1	β=ω0
3	1	0,5	0,5	4	1	1	4	1	1	β>ω0

Візуалізація результатів представимо (рис. 6–8).

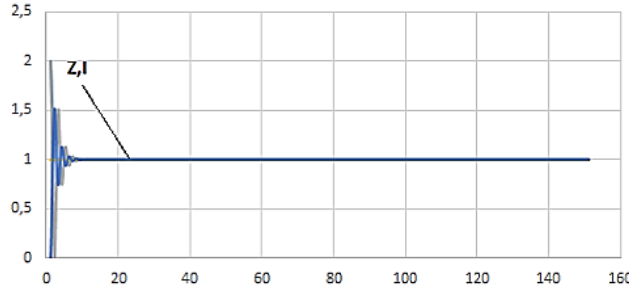


Рис. 6. Залежність інтенсивності та захисту даних від кількості ітерацій (140). Дані складових взяті з табл. 1. β<ω0

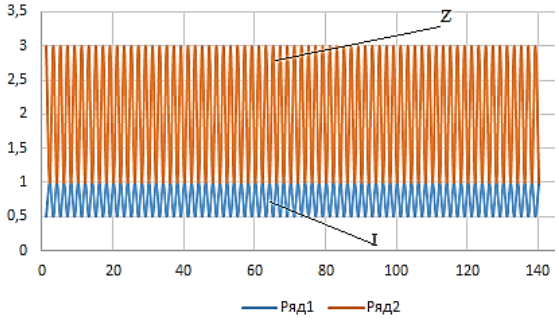


Рис. 7. Залежність інтенсивності та захисту даних від кількості ітерацій (140). $\beta = \omega_0$, Di=0,5

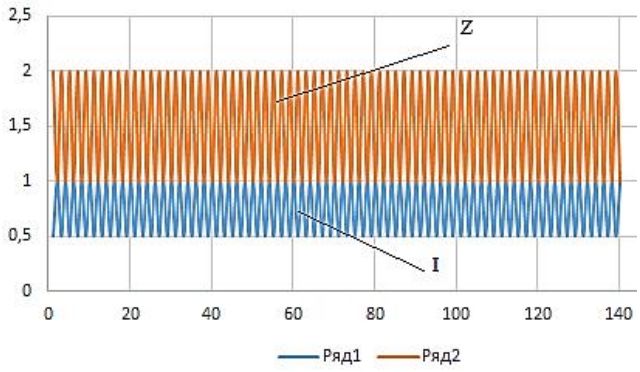


Рис. 8. Залежність інтенсивності та захисту даних від кількості ітерацій (140). $\beta \succ \omega_0$, Di=0,1

Аналіз даних на рис. 8 вказує на нелінійність системи захисту інформації.

Висновки

У роботі проведено дослідження лінійної моделі взаємодії між переповненням трафіку та DOS-атаками в системі «мережа–сервер». Побудовано систему диференціальних рівнянь, яка описує динаміку інформаційного потоку та рівня захищеності інформаційної системи. Визначено стаціонарну позицію системи та отримано умови її існування.

Показано, що поблизу стаціонарного стану поведінка системи описується рівнянням гармонічного осцилятора з затухаючою амплітудою. Аналітично визначено основні параметри системи захисту: власну частоту коливань, період коливань і коефіцієнт демпфування. Встановлено, що характер розв'язку залежить від співвідношення між коефіцієнтом демпфування та власною частотою системи і може відповідати трьом режимам: недемпфованому, критично демпфованому та передемпфованому.

Результати імітаційного моделювання у дискретному часі підтвердили аналітичні висновки та показали, що за певних параметрів система демонструє нелінійну поведінку, що вказує на обмеженість лінійної моделі при значних відхиленнях від стаціонарного стану. Отримані результати можуть бути використані для подальшого розвитку нелінійних моделей та вдосконалення методів захисту мережевих і серверних ресурсів від DOS/DDoS-атак.

Список літератури

[1]. Ахрамович Вадим. Спосіб дослідження кількісних показників системи захисту корпоративної мережі. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка, №2(14), с.36-49.

[2]. Akhramovych V , Shuklin G , Pepa Y , Lehominova S , Muzhanova T , Dzyuba T , Yakymenko Y. Methodology for Calculating the Index of Protection of a Social Media from its Centrality. International Journal of Emerging Technology and Advanced Engineering. Volume 13, Issue 04, April 2023.- pp. 17-26. DOI: 10.46338/ijetae0423_03. **Scopus**.

[3]. Volodymyr Akhramovych, Yuriy Pepa, Anton Zahynei1, Vadym Akhramovych, Taras Dzyuba, Ihor Danylov. Method for calculating the information security indicator in social media with considerationof the path durationbetween clients. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska" – IAPGOS. Volume № 14, Number 1 (2024), pp. 71–77. DOI:

[4]. R. Khrashchevskyi, V. Klobukov, V. Kozlovskyi, V. Akhramovych, S. Lazarenko. Method of calculating information protection from mutual influence of users in social networks / // International Journal of Computer Network and Information Security (IJCNIS), Volume № 15, Number 5 (2023), pp. 27–40. DOI: https://doi.org/10.5815/ijcnis.2023.05.03. Scopus, квартіль Q1.

[5]. Akhramovych Volodymyr, Lehominova Svitlana, Stefurak Oleh, Akhramovych Vadym, Chuprun Sergii, "Methodology for Searching for the Dependence Between Data Defensiveness and Volume of Social Network Evolution", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.6, pp.1-19, 2024. DOI:10.5815/ijcnis.2024.06.01.

[6]. Akhramovych V., Akhramovych V., Ilyenko A., Halata L., Yakovenko O., Halych Y. The methodology for researching the cybersecurity of social platforms in relation to the number of communities // CSDP'2025: Cyber Security and Data Protection (Lviv, Ukraine, July 31, 2025). – Vol. 4042. – 2025. – P. 153–166.

[7]. Ткач Ю.М., Яковлєв О.О., Лисиця Т.А. Informatics and Mathematical Methods in Simulation Vol. 11 (2021), No. 4, pp. 358-364.

[8]. Бурячок В.Л., Козачок В.А., Бурячок Л.В., Складанний П.М. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах. Сучасний захист інформації No3, 2015. -с. 4-12.

[9]. Галата Л. П., Корнієнко Б. Я. дослідження системи захисту інформації корпоративної мережі на основі GNS3. Наукоємні технології № 2(46), 2020.-с. 172-179.

[10]. Vitalii Lytvynov, Nikolai Stoianov, Ihor Skiter, Helen Trunova, Alla Hrebennyk. Corporate networks protection against attacks using content-analysis of global information space. Technical sciences and technologies. No 1 (11), 2018. с. 115-130.

[11]. Тишик Іван. Тестування корпоративної мережі організації на несанкціонований доступ. Кібербезпека: освіта, науке, техніка. No 2(18), 2022.- с. 39-48.

[12]. Мілян К.В., Грицюк Ю.І. Особливості організації інформаційної безпеки корпоративної мережі промислової компанії. Науковий вісник НЛТУ України. – 2013. – Вип. 23.4. -с. 314-328.

[13]. Коробейнікова Т. І., Журавель І. М., Бодак А. О., Бороденко Д. В. Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах. Bulletin of Lviv State University of Life Safety, №30, 2024. с. 67-77.

[14]. Корнієнко Б. Я. , Галата Л. П. Оптимізація системи захисту інформації корпоративної мережі. Математичне та комп'ютерне моделювання. Серія:Технічні науки. Випуск19. 2019.- с. 56-62.

[15]. Тишик Іван. Забезпечення безпеки облікових записів корпоративних користувачів. Кібербезпека: освіта, науке, техніка. No 2(22), 2023.-с. 214-225.

[16]. Єлізаров А.Б., Симониченко Я.А., Рябінко О.М. Адаптивний захист корпоративної мережі.

[17]. Карпенко Оксана, Рабчун Андрій. Математичне моделювання управління ресурсами захисту в системах інформаційної безпеки фінансових організацій в умовах гібридних загроз. Січень 2023. Бізнес Інформ 11(550): pp. 180-187

[18]. Lubov Zahoruiko1,2, Tetiana Martianova3, Mohammad Al-Hiari4, Lyudmyla Polovenko1, Maiia Kovalchuk1, Svitlana Merinova5, Volodymyr Shakhov, Bakhyt Yeraliyeva. Mathematical model and structure of a neural network for detection of cyber attacks on information and communication systems. IAPGOŚ 3/2024. pp. 49-55.

[19]. Chong Tian a , Siqiu Hu. Математичне моделювання аналізу впливу на безпеку мережі зв'язку на

© Akhramovych V.M., Ilienko A.V., Fesenko A.O., Akhramovych V.V. Study of a linear model of interaction between traffic overflow and dos attacks in a network and server // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 74-84. © This is an open access article under the CC BY 4.0 International license.*

основі алгоритму Монте-Карло. Комп'ютерні комунікації. Том 157, 1 травня 2020, pp. 20—27

[20]. Валерій Хранилов, Павло Бураго та Альберт Єгамов. Математична модель ДДС для управління інформаційною безпекою організації. E3S Web of Conferences SDEA-2024 09 , 090 (2024). pp. 1-8.

[21]. Ghazi Ghader Mohammed, Zeedon Zaheer. NeuroCyberGuard: Developing a Robust Cybersecurity Defense System through Deep Neural Learning-Based Mathematical Modeling. Journal of Smart Internet of Things (JSIoT) VOL 2023, No.02 2023/ pp. 133-145.

[22]. ПЕТРИК Б. В., ДУБРОВІН В. І. Виявлення атак типу dos в мережевому трафіку за допомогою вейвлет-перетворення. Прикладні питання математичного моделювання т. 4, No 1, 2021. -с. 45-56.

УДК 004.738.5

Akhramovych V.M., Ilienko A.V., Fesenko A.O., Akhramovych** V.V. **Study of a linear model of interaction between traffic overflow and dos attacks in a network and server

Abstract.*This paper investigates a linear mathematical model of interaction between network traffic overflow and DOS/DDoS attacks in a "network–server" information system. A formalized approach is proposed to describe the dynamics of the information flow and the level of system security, taking into account the intensity of threats, the speed of their impact, and the effectiveness of protective measures. A system of differential equations describing the system behavior near a stationary state is constructed and analyzed using the small perturbation method. It is shown that the linear model leads to the equation of a harmonic oscillator with a damped amplitude. The main parameters of the protection system are determined, including the natural frequency of oscillations, the oscillation period, and the damping coefficient. Discrete-time simulation modeling is performed, which makes it possible to identify regions of linear and nonlinear behavior of the system. The obtained results can be used to analyze the resilience of network and server resources to DOS attacks and to substantiate requirements for information security systems.*

Keywords: *DOS attack, DDoS attack, traffic overflow, information security, linear model, harmonic oscillator, damping, network, server.*

Ахрамович Володимир Миколайович, д.т.н., професор, професор кафедри кібербезпеки Національного університету «Київський авіаційний інститут»
Akhramovych Volodymyr, Doctor of Technical Sciences, Professor, Professor of the Department of Cybersecurity, National University «Kyiv Aviation Institute»

Ільєнко Анна Вадимівна, к.т.н., доцент, завідувач кафедри кібербезпеки Національного університету «Київський авіаційний інститут»
Ilienko Anna, Ph.D., Associate Professor, Head of the Department of Cybersecurity, National University «Kyiv Aviation Institute»

Фесенко Андрій Олексійович, к.т.н., доцент, декан факультету комп'ютерних наук та технологій Національного університету «Київський авіаційний інститут»
Fesenko Andrii, Ph.D., Associate Professor, Dean of the Faculty of Computer Science and Technologies, National University «Kyiv Aviation Institute».

Ахрамович Вадим Володимирович, завідувач комп'ютерного центру Національної академії статистики, обліку та аудиту.
Akhramovych Vadym, Head of the Computer Center, National Academy of Statistics, Accounting and Audit.

Дата надходження:	Дата прийняття:	Дата публікації:
08.01.2026	30.01.2026	22.04.2026