УДК 004.738.5

МЕТОД ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ

Ахрамович Вадим Володимирович

Розроблено математичну модель та проведено дослідження моделі захисту локальної мережі. Розглянуто залежності величини потоку інформації в локальній мережі від складових захисту інформації, захищеності системи, розмірів системи загроз безпеці інформації та коефіцієнта кластеризації мережі.

Отримано систему лінійних рівнянь, яка відображає вплив швидкості зміни потоку інформації на захищеність локальної мережі і коефіцієнтів, що характеризують: вплив заходів захищеності, таких як боротьба з побічним електромагнітним випромінюванням, фізичний захист, контроль цілісності та автентичності даних, розмежування доступу до інформації, роботу firewall, антивірусне забезпечення, збої та відмови компонент програмного і апаратного забезпечення, вплив швидкості витоку персональних даних, кількості персональних даних, ідентифікацію та автентифікацію користувачів, резервне копіювання даних, аудит, вплив захищеності на витік інформації та вплив розмірів системи на захищеність.

В результаті розв'язку системи диференціальних рівнянь отримано математичні та графічні залежності показника захисту персональних даних в локальній мережі від різних складових.

Розглянувши три варіанти вирішення рівняння біля стаціонарного стану системи, зроблено висновок, що при співвідношенні дисипації та власної частоти коливань величина загасання до певного значення може здійснюватися періодично з затухаючою амплітудою або за експоненціально згасаючим законом. Виконано більш наочний аналіз поведінки системи, перейшовши від диференціальної форми рівнянь до дискретної та промоделювавши деякий інтервал існування системи.

Представлені математичні та графічні залежності частоти власних коливань системи, періоду коливань та коефіцієнта загасання.

Проведено імітаційне моделювання для значень з відхиленням від стаціонарної позиції системи. В результаті імітаційного моделювання доведено, що система захисту локальної мережі є нелінійною.

Ключові слова: *показник захисту; локальна мережа; потік; інформація; дані; витік; коефіцієнт; система; рівняння.*

Вступ

Захист інформації в комп'ютерних системах та мережах набуває дедалі більшого значення, що підтверджується зростанням кількості наукових публікацій та комерційних організацій, які спеціалізуються на розробці та впровадженні засобів інформаційної безпеки. Однією з основних загроз для інформаційних систем є умисний несанкціонований доступ (НСД) до інформації з боку сторонніх осіб, що може призвести до викрадення, спотворення, знищення або блокування даних.

Захист інформації – це комплекс організаційних, програмно-технічних і правових заходів, спрямованих на попередження витоку, втрати, модифікації, несанкціонованого копіювання або знищення інформації. Сюди також відносяться заходи, пов'язані з підвищенням надійності функціонування апаратних та програмних компонентів, які можуть вийти з ладу з технічних чи об'єктивних причин.

В контексті комп'ютерних мереж термін "захист інформації" часто використовується як синонім до поняття "комп'ютерна безпека", що охоплює всі аспекти забезпечення надійного функціонування мережевої інфраструктури.

Перехід від використання персональних комп'ютерів до інтегрованих мережевих рішень ускладнює завдання захисту інформації з низки причин:

збільшення кількості користувачів у мережі та динамічність їх складу, що ускладнює ідентифікацію та автентифікацію;

зростання фізичних розмірів мережі та кількості потенційних точок вторгнення;

наявність вразливостей в апаратному і програмному забезпеченні, які часто виявляються лише на етапі експлуатації, навіть у системах із вбудованими механізмами захисту.

Серйозну загрозу становлять також канали витоку інформації через фізичні та електромагнітні середовища. Кожен пристрій у мережі може бути джерелом електромагнітного випромінювання, що не завжди достатньо екранування. Крім того, елементи електроживлення, заземлення та кабельні системи можуть слугувати каналами перехоплення інформації, зокрема за межами контрольованих зон.

До інших потенційних каналів витоку інформації належать:

сховища інформаційних носіїв;

конструктивні елементи будівель, зокрема вікна, які створюють ефект акустичного резонансу (так званий "мікрофонний ефект");

сторонні дротові та бездротові канали, включно з телефонними лініями, радіозв'язком і мобільними мережами.

Наявність широкого спектру загроз вимагає комплексного, науково обґрунтованого підходу до побудови систем захисту інформації в

комп'ютерних корпоративних мережах, що враховує як технічні параметри системи, так і поведінкові моделі потенційних порушників.

Постановка задачі

Сучасні локальні мережі характеризуються високою складністю та динамічністю, зумовленою інтеграцією новітніх інформаційних технологій, що істотно змінює вимоги до їх захисту. У таких умовах забезпечення належного рівня інформаційної безпеки потребує постійного вдосконалення методів аналізу та оцінювання ефективності систем захисту.

Аналіз науково-технічної літератури [1–15] показав, що на сьогодні відсутні комплексні, науково обґрунтовані підходи до визначення кількісних показників рівня захисту інформації залежно від параметрів впливу зовнішніх та внутрішніх факторів на систему захисту локальних мереж. Це ускладнює об'єктивну оцінку стійкості системи захисту до потенційних загроз, а отже — й побудову ефективних заходів щодо її оптимізації.

Актуальним та практично значущим завданням є розроблення методики аналізу моделей систем захисту, що дозволяє отримати оцінку впливу факторів (та їхньої сукупної дії) на ефективність функціонування системи.

Однією з основних причин недостатньої дослідженості проблеми є складність урахування взаємодії великої кількості параметрів, які можуть мати різноспрямовану та нерівномірну дію на систему захисту. Також існує потреба у встановленні характеру цієї взаємодії — лінійного чи нелінійного — що унеможливлює застосування класичних методів аналізу без належної адаптації або ускладнює їх використання взагалі.

Мета дослідження — дослідження кількісних параметрів показника захисту локальної мережі та визначення її лінійності.

1. Аналіз останніх досліджень та публікацій.

В статті [1] показані якісні показники системи захисту інформації в локальній мережі в залежності від факторів впливу, та прогнозується отримання кількісних показників на основі загальних підходів.

В статті [2] розроблена математична модель захисту інформації в ПК на основі системи диференціальних рівнянь та проведено моделювання рішень у системі MatLab. Розглянуто три варіанти вирішення рівняння біля стаціонарного стану системи (виконано більш наочний аналіз поведінки системи з переходом від диференціальної форми рівнянь до дискретної та моделювання деякого інтервалу існування системи). Зроблено висновок, що, виходячи з умов співвідношення дисипації та власної частоти коливань, величина загасання останньої до певного значення здійснюється періодично, з затухаючою амплітудою або за експоненціально загасаючим законом.

З врахуванням впливу вказаних параметрів на захист інформації та можливості визначення кількісного показника захисту, користувачі ПК зможуть самостійно оцінити вплив кожної складової загроз і прийняти адекватні рішення з захисту.

В роботі [3] досліджено динамічні моделі системи захисту даних у соціальних мережах з огляду еволюції соціальних мереж та досліджено надійність системи захисту даних.

З точки зору математики розроблено прототип системи захисту на основі нелінійних диференціальних рівнянь і проведено його трансцендентний перегляд. Трансцендентний огляд динамічних моделей системи захисту в соціальних мережах довів, що параметри факторів, які впливають на систему захисту, мають суттєвий вплив при можливих значеннях – до ста відсотків.

Перевірено параметри системи захисту на фазовій площині та доведено її стійкість.

В статті [4] досліджено лінійну модель захисту від розширення соціальної мережі була побудована система лінійних рівнянь, що описує захист інформації в соціальних мережах, залежно від типу та параметрів розширення мережі. Визначено умови для стаціонарного стану системи, вирішено рівняння методом «малих відхилень», отримано графічні залежності та проведено ітераційне моделювання коливань системи захисту. Використання методу диференціювання функції захисту дало змогу дослідити поведінку системи та отримати кількісні оцінки рівня захисту від різних факторів впливу..

В роботі [5] Описано основні концептуальні аспекти створення, функціонування, розвитку та використання національної системи конфіденційного зв'язку. Розглянуті системи захисту інформації на різних рівнях моделі взаємодії відкритих систем, основні загрози інформаційній безпеці комп'ютерних систем і мереж, а також представлені протоколи та інструменти захисту інформації, зокрема в локальних мережах і в Інтернеті.

В роботі [6] відмічається, що локальні мережі відіграють ключову роль у функціонуванні бізнес-процесів, оскільки забезпечують ефективний зв'язок між різними елементами

інфраструктури компанії. Завдяки локальним мережам співробітники отримують доступ до необхідних ресурсів, а компанії можуть підтримувати стабільну роботу, керувати даними та забезпечувати надійний захист інформації.

Оновлення програмного забезпечення, операційних систем та мережевих пристроїв є важливим заходом для підтримки безпеки та стабільності мережі. Регулярне оновлення дозволяє усунути вразливості, які зловмисники можуть використовувати для несанкціонованого доступу до мережі. Регулярні оновлення допомагають закрити вразливості, які можуть бути використані зловмисниками для доступу до мережі. Також необхідно впровадити політику регулярного резервного копіювання даних, щоб у разі збоїв або атак (наприклад, програмами-вимагачами) можна було швидко відновити роботу компанії без втрат важливої інформації.

В статті [7] розглянуто питання захисту інформаційних ресурсів локальної та розподіленої обчислювальної мережі, наведено характеристику і механізми реалізації загроз у розподілених мережах, запропоновано модель загроз від факторів, що впливають на систему захисту та визначення методів його удосконалення

В статті [8] обговорюються питання захисту інформаційних ресурсів комунікаційних мереж у розподілених обчислювальних системах, пропонується модель багаторівневого захисту ресурсів мережі, а також розглядаються механізми, що забезпечують функціонування послуг безпеки.

В статті [9] пропонується можливість використання найбільш ефективної та перспективної архітектури DLP-системи для захисту даних від сучасних загроз в локальній мережі підприємства. Сучасні системи DLP (Data Leak Prevention) — це технології, що дозволяють запобігати витоку конфіденційної інформації з підприємства, а також можуть застосовуватися для вирішення інших завдань, таких як моніторинг діяльності персоналу. У зв'язку з цим, потреба в DLP-системах є високою і актуальною для кожного підприємства. З урахуванням вищевказаного, зрозуміло, що цим обумовлюється затребуваність і актуальність сучасних DLP-систем для будь-якого підприємства.

Проаналізовано можливість використання DLP-системи для захисту інформації у локальній мережі підприємства. Розроблено програму для виконання моніторингу системних подій у додатках, визначених політиками інформаційної безпеки.

В статті [10] розглядаються основні особливості захисту інформації в локальних обчислювальних мережах, наводиться аналіз несанкціонованого доступу та способи вирішення можливих проблем щодо захисту цілісності комп'ютерної мережі

В роботі [11] . запропоновано новий підхід до вдосконалення інформаційної безпеки (ІБ) мережі навчального закладу, заснований на системному та структурованому підході. Цей метод дозволяє оцінити захищеність не лише загальної мережі, а й окремих її підсистем і компонентів, що забезпечують ІБ. Для оцінки використано різні показники, включаючи статистичні, експертні та евристичні. Запропонована модель забезпечення ІБ університетської мережі описує відповідні процедури та включає збалансовану систему показників для оцінки ефективності захисту. У ході дослідження була розроблена модель захищеної мережі навчального закладу, де мережеві пристрої були змодельовані у віртуальній машині (ВМ) з використанням програмного забезпечення EVE-NG.

В роботі [12] вивчено питання захисту конфіденційної та комерційної інформації в бездротових локальних мережах, що використовують технологію Wi-Fi. Окремо розглянуті види загроз і атак, орієнтованих на бездротові мережі, а також запропоновані методи для їх запобігання та підвищення загального рівня безпеки.

В роботі [13] для захисту локальної мережі та інформації в локальній мережі проведено систематичний огляд літератури щоб отримати більш глибоку інформацію про методи та аспекти мережевої безпеки. Для цього використовується Cisco Packet Tracer. Поширеними методами є безпека портів, ACL, AAA та Підглядання за DHCP. Однак, з точки зору інформаційної безпеки, DMZ, ACL, VLAN, STP і DHCP Snooping є більш важливими аспектами, які треба враховувати, тому що кожен з них є вразливістю для доступу до інформації. Метод AAA відіграє ключову роль у їх захисті в локальній мережі.

В роботі [14] надано детальний огляд мережевої безпеки, зокрема реалізацій брандмауера, на Local. Мережі операційних систем Windows NT і Unix. У ньому розглядаються основи безпеки комп'ютерної мережі, її еволюція та проблеми, з якими стикаються під час захисту даних мережі, де бажано дозволити доступ кільком користувачам одночасно відмовляти іншим у такому доступі. На додаток до цього, впровадження

брандмауерів є, мабуть, найбезпечнішим способом захисту даних від вторгнення в комп'ютерні мережі. Як наслідок, цей документ дає уявлення про проблеми комп'ютерної безпеки, які викликали необхідність розробки та впровадження брандмауерів.

В роботі [15] вказується, що дротова локальна мережа є нервовою системою інформаційних систем організації, необхідно приділити велику увагу її належному захисту. Робота починається з розгляду наслідків для безпеки дротової локальної мережевої інфраструктури. Далі розглянута сегментація локальної мережі та ізоляція трафіку. Використовуючи сегментацію та ізоляцію, збільшуються можливості для меж безпеки. Ще одним поняттям, про яке піде мова, є безпека обладнання локальної мережі. Локальна мережа функціонує лише в тому випадку, якщо основне обладнання працює, тому захист обладнання є важливою частиною будь-якої стратегії безпеки. На завершення досліджено обмеження доступу до локальної мережі та обговорено організаційний підхід. Оскільки все більше і більше користувачів потребують доступу до ресурсів локальної мережі, повинен існувати спосіб ідентифікації та обмеження того, кому дозволено перебувати в мережі та який доступ їм надається. У безпеці дротової локальної мережевої інфраструктури організації повинні пам'ятати, що вони захищені лише настільки, наскільки їх слабке місце. Ретельно розглядаючи різні аспекти безпеки локальної мережі під час проектування, можна зменшити ці слабкі місця та підвищити загальну безпеку мережі. Хоча неможливо бути на 100% безпечним і при цьому бути функціональним, використовуючи деякі загальні рекомендації для захисту дротової локальної мережі, можна зменшити багато загроз для мережі, якщо не усунути.

2. Основна частина

Втрата такої характеристики, як показник захисту інформації Z, у локальній мережі є процесом, що має часову динаміку. Це означає, що рівень захисту змінюється впродовж часу під впливом різних зовнішніх і внутрішніх чинників.

Позначимо загальний обсяг інформації в системі через I

I. Потік інформації, що виходить за межі локальної мережі, можна описати як I локальної мережі через dI–, швидкість зміни цього потоку – $\frac{dI}{dt}$. Якщо обсяг інформації, що залишає систему, не змінюється (тобто потік дорівнює нулю), і цей стан залишається стабільним у часі (тобто швидкість зміни потоку також нульова), то можна стверджувати, що витоку інформації не відбувається.

$$dI = 0; \frac{dI}{dt} = 0 \quad (1)$$

Витік інформації може бути зумовлений рівнем вразливості системи до зовнішніх або внутрішніх загроз. Насамперед це залежить від того, наскільки ефективно реалізовані заходи захисту — тобто наскільки система здатна протидіяти спробам несанкціонованого доступу чи втручання. Інакше кажучи, ступінь витоку інформації прямо пов'язаний із рівнем її захищеності, який позначимо як Z.

Таким чином, можна стверджувати: чим вищий показник захищеності Z, тим менша ймовірність або інтенсивність витоку інформації.

Складемо відповідне рівняння, яке описує цю залежність:

$$\frac{dI}{dt} = Z(Z_p + \mathrm{Q}_c + \mathrm{R}_c + \mathrm{W}_c + \mathrm{F}_c + \mathrm{Ad}_c + \mathrm{V}_c + \\ + \mathrm{A}_{rc} + \mathrm{C}_c + \mathrm{M}_c)(\mathrm{Z_{pc}Z_k}) + (C_v + C_k)I \quad (2)$$

де Z_p – коефіцієнт, який відбиває дію побічних заходів стосовно безпеки інформації (наприклад, битва з додатковим електромагнітним випромінюванням, речову безпеку і т.п.); (0…1); Qc– коефіцієнт, який відбиває контролювання цілісності та автентичності інформації (0…1); Rc– коефіцієнт, який відбиває створення копій інформації (0…1); Wc– коефіцієнт, який відбиває права доступу до даних (0…1); Fc– коефіцієнт, який відбиває діяльність брандмауера (0…1); A_{dc} – коефіцієнт, який відбиває аудит (0…1);. Vc– коефіцієнт, який відбиває роботу антивіруса (0…1) Z_{pc} - коефіцієнт, який відбиває роботу компонент ПЗ, які контролюють діяльність мережі (0,1); Z_k – коефіцієнт, який відбиває роботу складових тезнічного захисту, які контролюють діяльність мережі (0,1); A_{rc} - коефіцієнт, який відбиває систему створення копій (0…1); C_c - коефіцієнт, який відбиває систему кодування (0…1); M_c - коефіцієнт, який відбиває роботу міжмережевого фільтру (0…1); Cv – коефіцієнт, який відбиває діяння бистроти витоку інформації (0…1); C_k –

коефіцієнт, який відбиває дію кількості інформації на її стік(0…1).

Рівняння можна інтерпретувати наступним чином: витік інформації залежить від таких факторів:

- Розмір інформаційної системи, що в свою чергу пов'язано з кількістю даних, які вона обробляє.
- Швидкість витоку даних.
- Захищеність системи, що обмежує витік інформації через заходи нейтралізації загроз безпеки інформації.

Далі розглянемо, від чого залежить захищеність системи (Z). Захищеність можна визначити як здатність системи протистояти несанкціонованому доступу до даних. Отже, захищеність системи залежить від таких факторів:

- Розмір системи, що також включає кількість даних, які в ній зберігаються.
- Загрози безпеки інформації, що виникають через взаємодію між користувачами.

На основі цих залежностей можемо сформулювати відповідне рівняння.

$$\frac{dZ}{dt} = I_d A(D_c + M_c + N_c + S_c) - (C_{d2} + C_{d1})I \quad (3)$$

де: I_d –коефіцієнт, який відбиває ідентифікацію акторів (0 або 1); Ac – коефіцієнт, який відбиває автентифікацію акторів (0 або 1); D_c - коефіцієнт, який відбиває посередницькі сервери (0…1); M_c - коефіцієнт, який відбиває екран безпеки (0…1); N_c - коефіцієнт, який відбиває VPN (0…1); S_c - коефіцієнт, який відбиває засоби виявлення аномалій; (0…1); C_{d1} – коефіцієнт, який відбиває рівень захисту даних (0…1); C_{d2} – коефіцієнт, який відбиває масштабованість безпеки: (0…1).

На основі наданих рівнянь (2) і (3), можемо сформулювати систему диференціальних рівнянь, яка описує динаміку витоку інформації та зміну рівня захищеності інформаційної системи:

$$\begin{cases} \dfrac{dI}{dt} = Z(Z_p + \mathrm{Q}_c + \mathrm{R}_c + \mathrm{W}_c + \mathrm{F}_c + \mathrm{Ad}_c + \mathrm{V}_c + \mathrm{A}_{rc} + \\ + \mathrm{C}_c + \mathrm{M}_c)(\mathrm{Z}_{\mathrm{pc}}\mathrm{Z}_{\mathrm{k}}) + (C_v + C_k)I \\ \dfrac{dZ}{dt} = I_d A(D_c + M_c + N_c + S_c) - (C_{d2} + C_{d1})I \end{cases} \quad (4)$$

Щоб знайти стаціонарну позицію системи, потрібно застосувати умови стаціонарності, тобто прирівняти похідні до нуля:

$dI = 0; \dfrac{dI}{dt} = 0$. Тоді:

$$\begin{cases} Z(Z_p + \mathrm{Q}_c + \mathrm{R}_c + \mathrm{W}_c + \mathrm{F}_c + \mathrm{Ad}_c + \mathrm{V}_c + \mathrm{A}_{rc} + \\ + \mathrm{C}_c + \mathrm{M}_c)(\mathrm{Z}_{\mathrm{pc}}\mathrm{Z}_{\mathrm{k}}) + (C_v + C_k)I = 0 \\ I_d A(D_c + M_c + N_c + S_c) - (C_{d2} + C_{d1})I = 0 \end{cases} \quad (5)$$

Аналіз другого рівняння системи показує:

$$\bar{I} = \frac{I_d A(D_c + M_c + N_c + S_c)}{(C_{d2} + C_{d1})} \quad (6)$$

Аналіз першого рівняння системи рівнянь (5) показує: $\bar{Z}$.

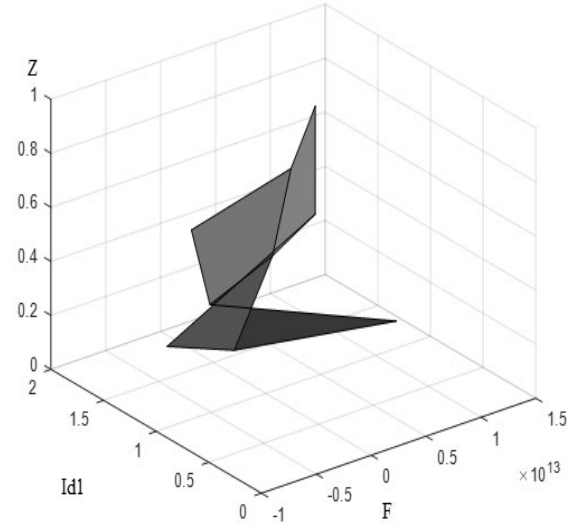
$$\bar{Z} = \frac{I_d A(D_c + M_c + N_c + S_c) - (C_v + C_k)}{(Z_p + \mathrm{Q}_c + \mathrm{R}_c + \mathrm{W}_c + \mathrm{F}_c + \mathrm{Ad}_c + \mathrm{V}_c + \mathrm{A}_{rc} + \\ + \mathrm{C}_c + \mathrm{M}_c)(\mathrm{Z}_{\mathrm{pc}}\mathrm{Z}_{\mathrm{k}})(C_{d2} + C_{d1})} \quad (7)$$

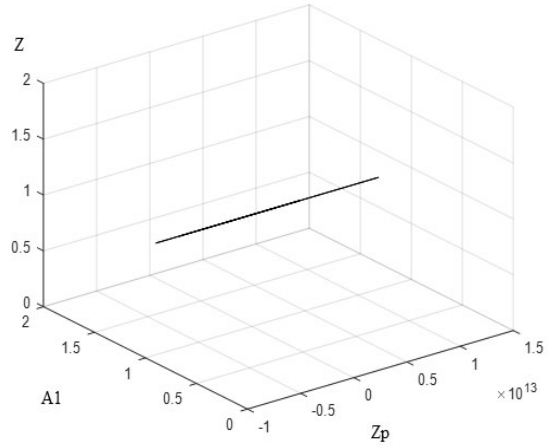
Система перебуває в стаціонарному стані, коли її характеристики не змінюються з часом. У фізичних та математичних термінах це означає, що перші похідні функцій стану системи за часом дорівнюють нулю.

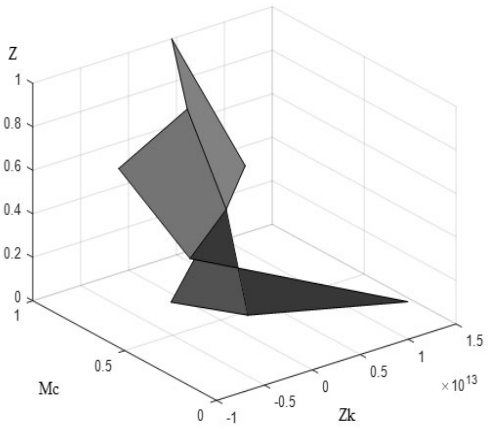
$$\begin{cases} \bar{I} = \dfrac{I_d A(D_c + M_c + N_c + S_c)}{(C_{d2} + C_{d1})} \\ \bar{Z} = \dfrac{I_d A(D_c + M_c + N_c + S_c) - (C_v + C_k)}{(Z_p + \mathrm{Q}_c + \mathrm{R}_c + \mathrm{W}_c + \mathrm{F}_c + \mathrm{Ad}_c + \mathrm{V}_c + \mathrm{A}_{rc} + \\ + \mathrm{C}_c + \mathrm{M}_c)(\mathrm{Z}_{\mathrm{pc}}\mathrm{Z}_{\mathrm{k}})(C_{d2} + C_{d1})} \end{cases} \quad (8)$$

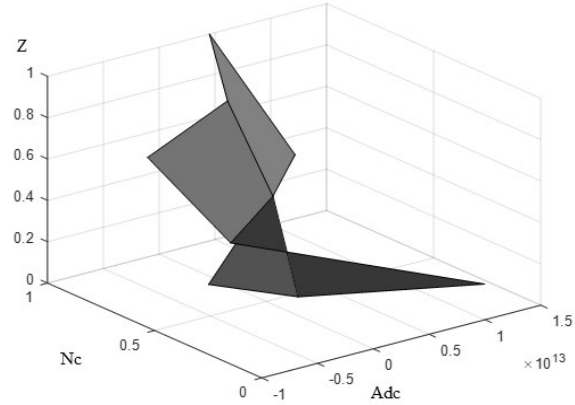
Щоб вирішити систему рівнянь (8) методом "малих відхилень", потрібно зазвичай припустити, що система знаходиться близько до стану рівноваги і здійснити розклад на малі відхилення від рівноважних значень.

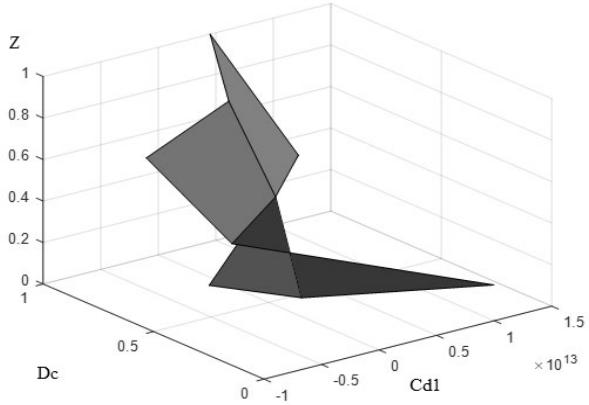
$I = \bar{I} + I; Z = \bar{Z} + Z$.;

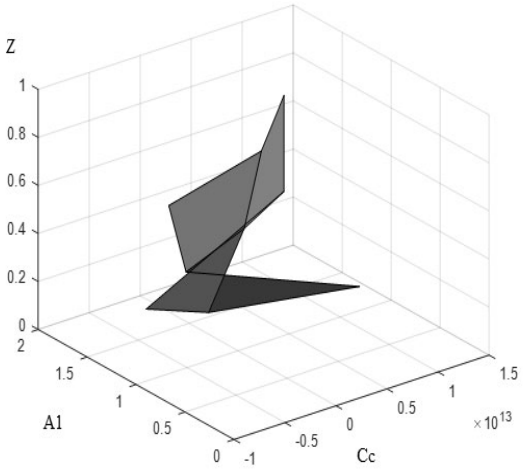


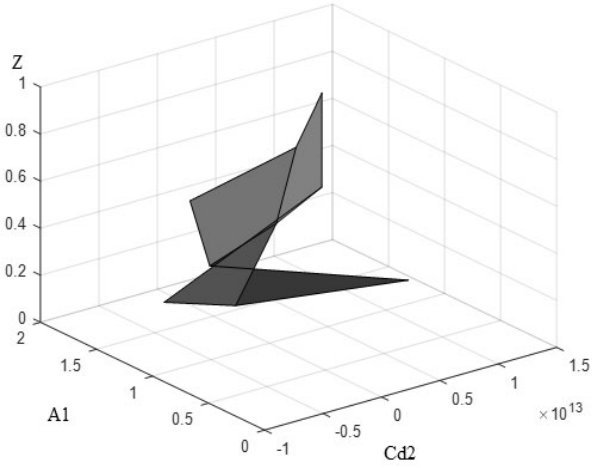












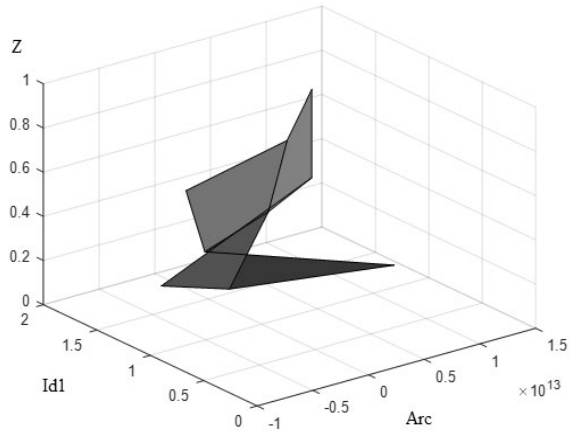


Рис. 1 Значення показника захисту інформації за залежністю (7)

$$\begin{cases} \dfrac{dI}{dt} = (\bar{Z} + Z)(Z_p + Q_c + R_c + W_c + F_c + Ad_c + \\ + V_c + A_{rc} + C_c + M_c)(Z_{pc} Z_k) + (C_v + C_k)(\bar{I} + I) \\ \dfrac{dZ}{dt} = I_d A(D_c + M_c + N_c + S_c) - \\ -(C_{d2} + C_{d1})(\bar{I} + I) \end{cases} \quad (9)$$

$$\begin{cases} \dfrac{dI}{dt} = Z(C_{d1} + C_{d2})(Z_p + Q_c + R_c + W_c + \\ + F_c + Ad_c + V_c + A_{rc} + C_c + M_c)(Z_{pc} Z_k) - \\ -(C_v + C_K) I \\ \dfrac{dZ}{dt} = -I(C_{d2} + C_{d1}) + I_d A(D_c + M_c + \\ + N_c + S_c)(C_v + C_k) \end{cases} \quad (10)$$

Диференціюємо перше рівняння системи (10), отримуємо нове рівняння або вираз для зміни функції в часі або за іншою змінною. Це дозволяє отримати рівняння для прискорення зміни величини, що міститься в першому рівнянні, та оцінити її зміну в контексті системи.

$$\frac{d^2 I}{dt^2} = -I(C_{d1} + C_{d2})(Z_p + Q_c + R_c + W_c + F_c + Ad_c + \\ + V_c + A_{rc} + C_c + M_c)(Z_{pc} Z_k)(C_v + C_k)) - (C_v + C_K)\frac{dI}{dt} \quad (11)$$

$$\frac{d^2 I}{dt^2} + (C_v + C_K)\frac{dI}{dt} + (C_{d1} + C_{d2})(Z_p + Q_c + R_c + \\ + W_c + F_c + Ad_c + V_c + A_{rc} + C_c + M_c)(Z_{pc} Z_k) \\ (C_v + C_k))I = 0 \quad (12)$$

Рівняння (12), яке є рівнянням гармонічного осцилятора з затухаючою амплітудою, описує рух об'єкта, який зазнає коливань з поступовим згасанням амплітуди через наявність сили тертя або опору середовища.

$$\omega_0 = \sqrt{\frac{(C_{d1} + C_{d2})(Z_p + Q_c + R_c + W_c + F_c + Ad_c + V_c + A_{rc} + \\ + C_c + M_c)(Z_{pc} Z_k) + I_d A(D_c + M_c + N_c + S_c}{}} \quad (13)$$

$$\omega = \sqrt{(C_{d1} + C_{d2})(Z_p + Q_c + R_c + W_c + F_c + Ad_c + \\ + V_c + A_{rc} + C_c + M_c)(Z_{pc} Z_k) - \frac{(C_v + C_K)^2}{4}} \quad (14)$$

$$T = \frac{2\pi}{\sqrt{(C_{d1} + C_{d2})(Z_p + Q_c + R_c + W_c + F_c + \\ + Ad_c + V_c + A_{rc} + C_c + M_c)(Z_{pc} Z_k) \\ (C_v + C_k) - \frac{(C_v + C_K)^2}{4}}}) \quad (15)$$

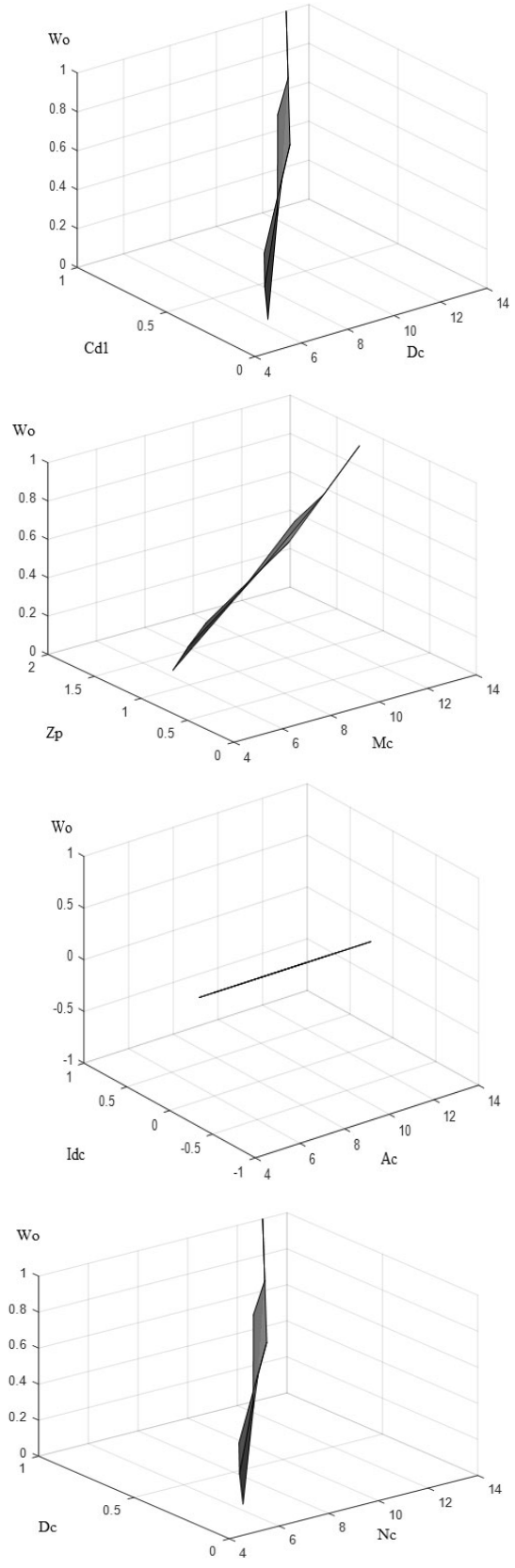


Рис. 2. Графік особистої частоти системи захисту за рівнянням (13).

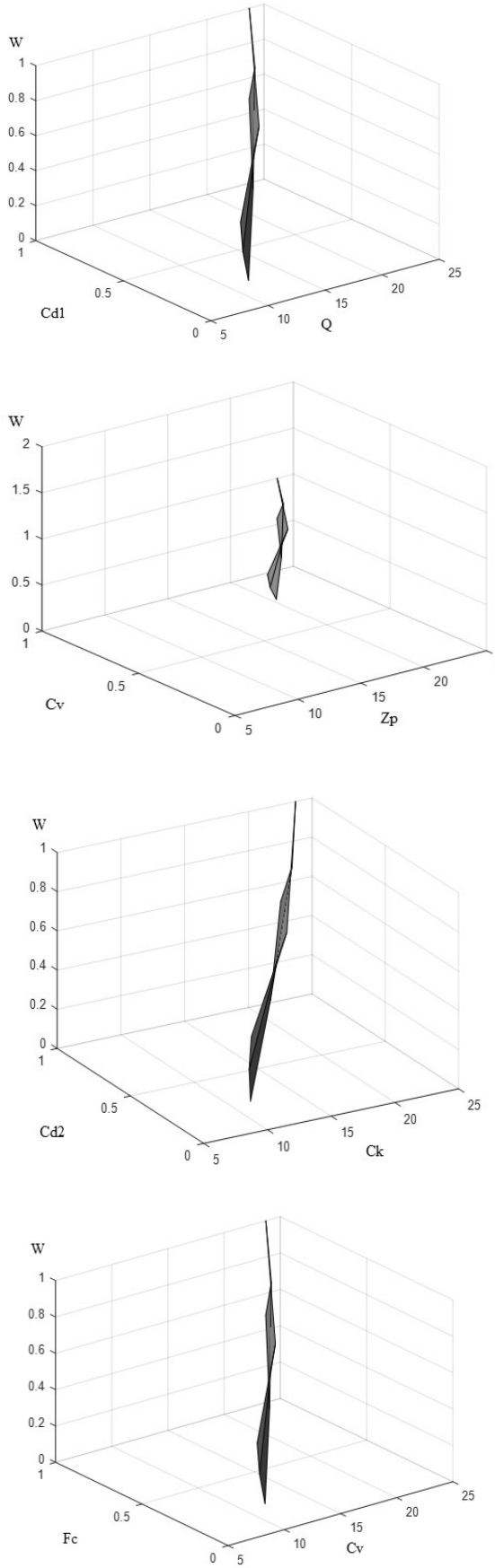


Рис. 3. Графік особистої частоти системи захисту за рівнянням (14).

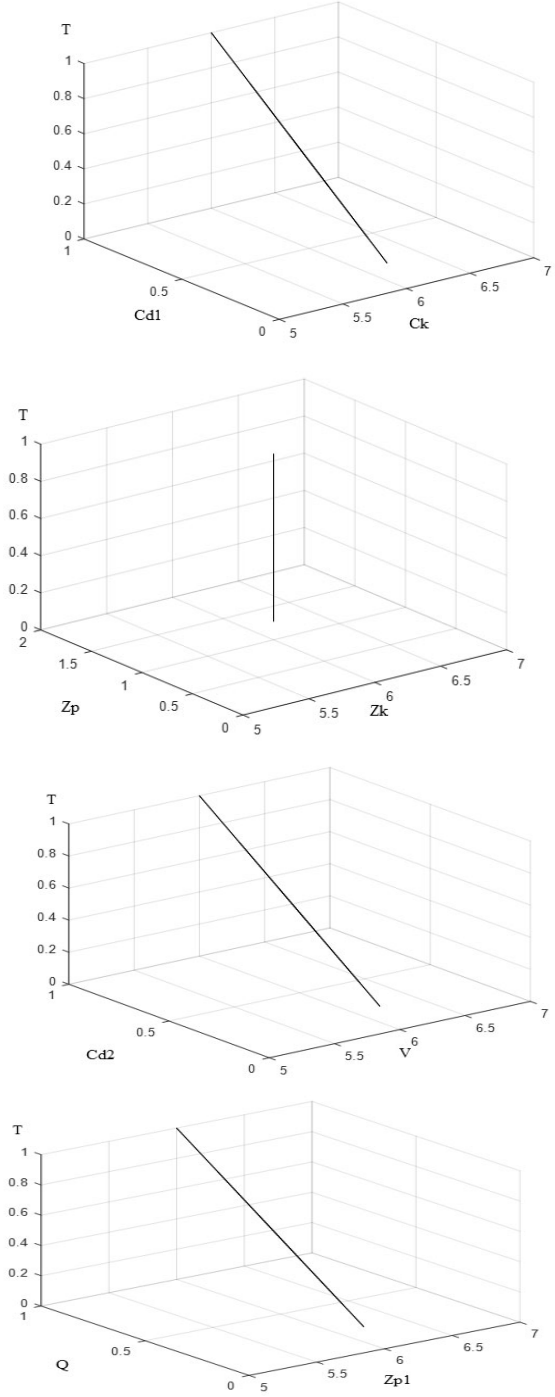


Рис. 4 Графік періоду коливань системи захисту за рівнянням (15)

$$\beta = \frac{(C_v + C_K)}{2} \tag{16}$$

Рішення рівняння гармонічного осцилятора з затуханням можна поділити на три основні випадки в залежності від значення коефіцієнта затухання.

$$\beta \prec \omega_0 : I = A_0 \exp(-\frac{(C_v + C_K)}{2}$$
$$\cos(\sqrt{\begin{matrix}(C_{d1} + C_{d2}) + +(Z_p + \mathrm{Q}_c + \mathrm{R}_c + \mathrm{W}_c + \mathrm{F}_c + \mathrm{Ad}_c + \\ + \mathrm{V}_c + \mathrm{A}_{rc} + + \mathrm{C}_c + \mathrm{M}_c)(\mathrm{Z}_{\mathrm{pc}}\mathrm{Z}_{\mathrm{k}})(C_v + C_k) - \\ - \frac{(C_v + C_K)^2}{4}\end{matrix}} t + \varphi_0) \tag{17}$$

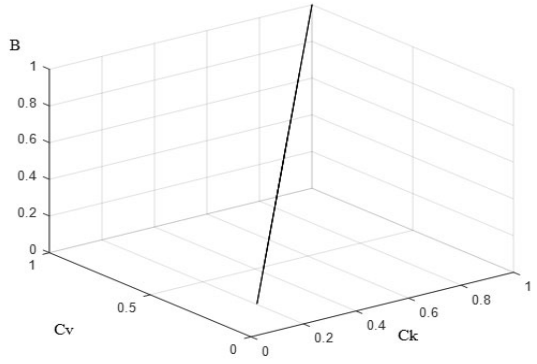
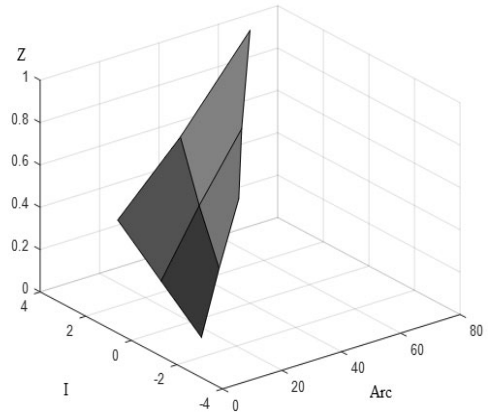
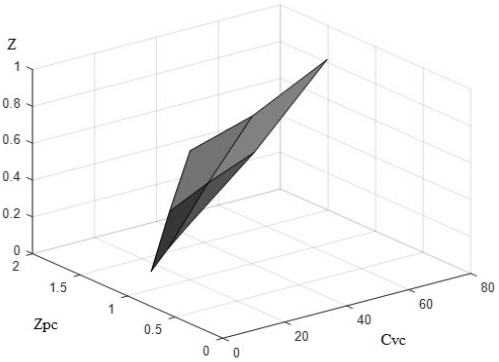
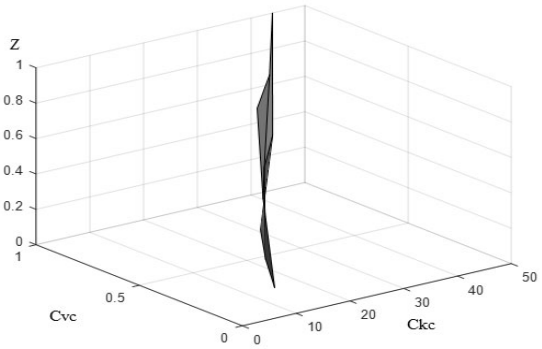
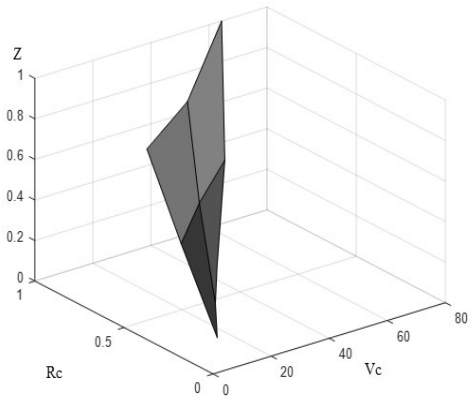


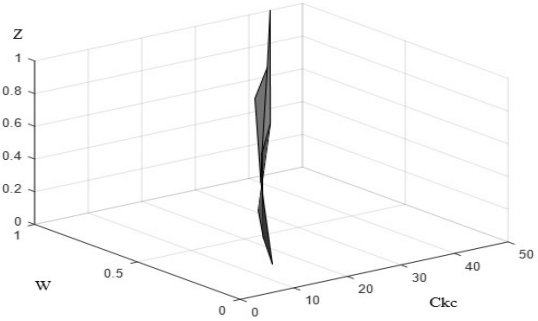
Рис. 5 Графік коефіцієнту затухання системи захисту за (16)

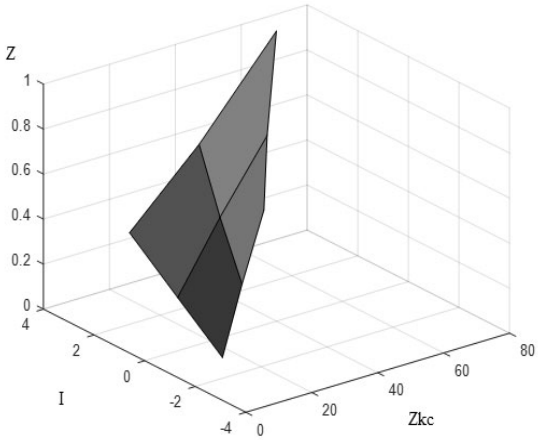


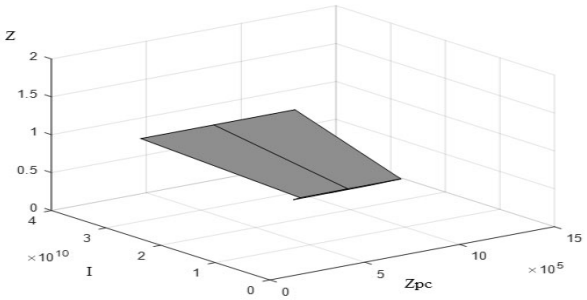


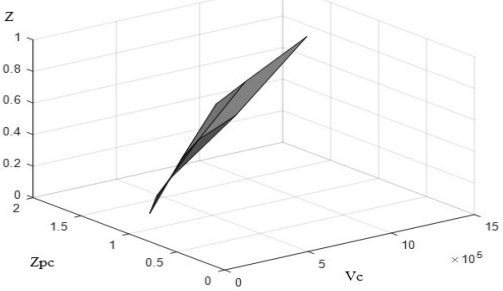












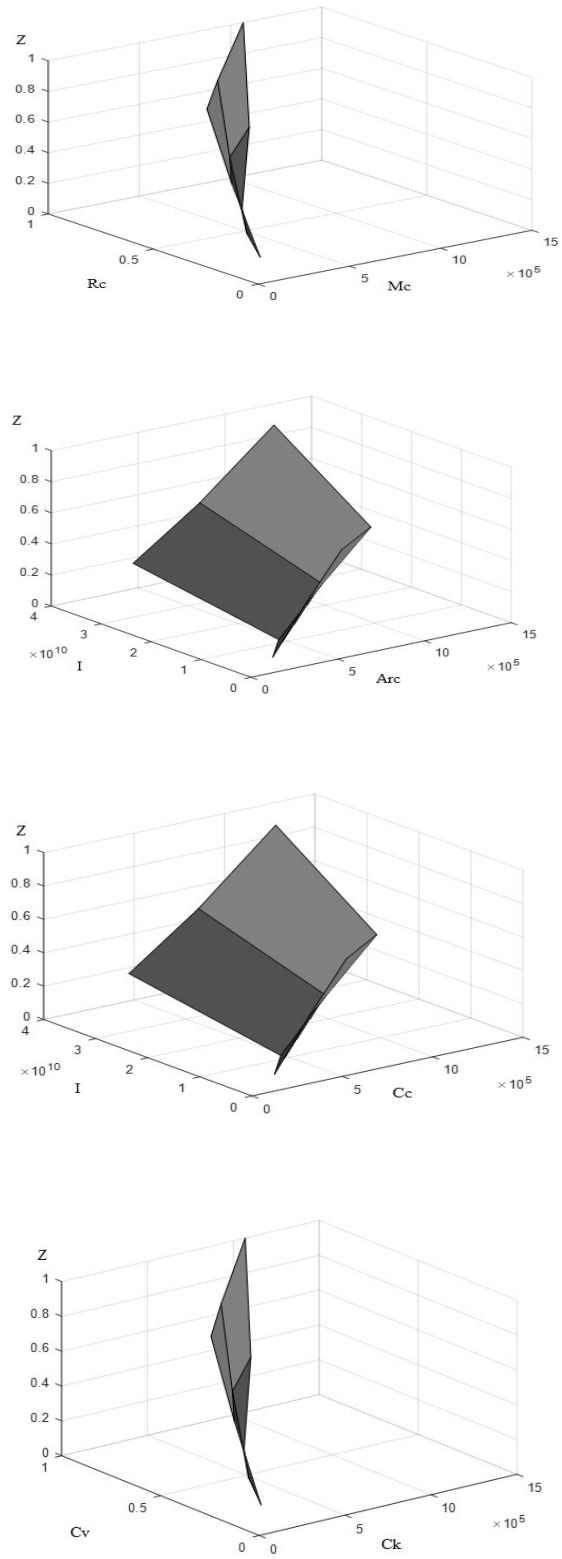


Рис. 6 Графік показника безпеки інформації в системі захисту за рівнянням (5)

2.

$$\beta = \omega_0 : I = (A_0 + B_0 t \exp(-\frac{(C_v + C_K}{2} t) \quad (18)$$

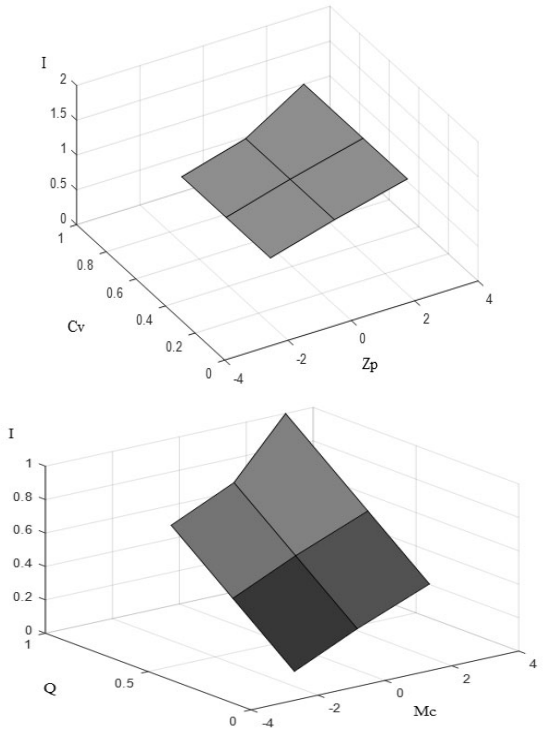


Рис. 7 Графік величини потоку інформації в системі безпеки за (17)

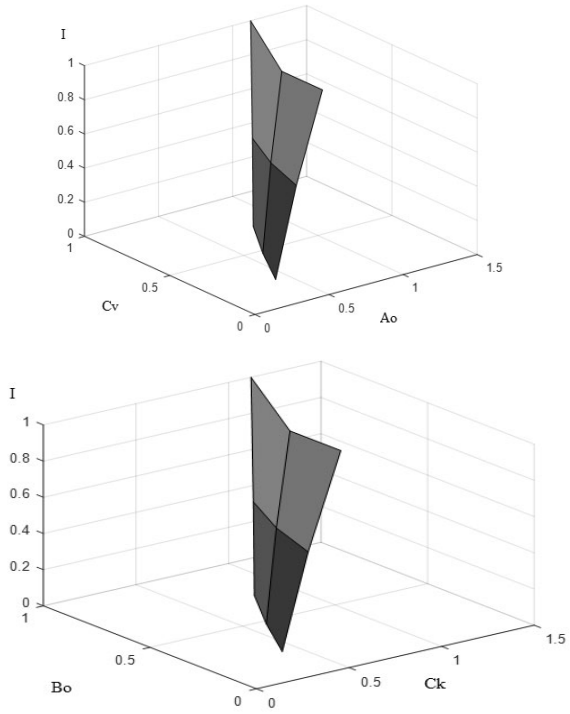


Рис. 8 Графік величини потоку інформації в системі безпеки за (18)

3.

$$\beta \succ \omega_0 : I = A_0 \exp(-y_1 t) + B_0 \exp(-y_2 t)$$

де

$$y_{12} = \beta \pm \sqrt{\frac{(C_v + C_K)^2}{4} - (C_{d1} + C_{d2})(Z_p + \\ + Q_c + R_c + W_c + F_c + Ad_c + V_c + \\ + A_{rc} + C_c + M_c)(Z_{pc} Z_k)(C_v + C_k)} \quad (19)$$

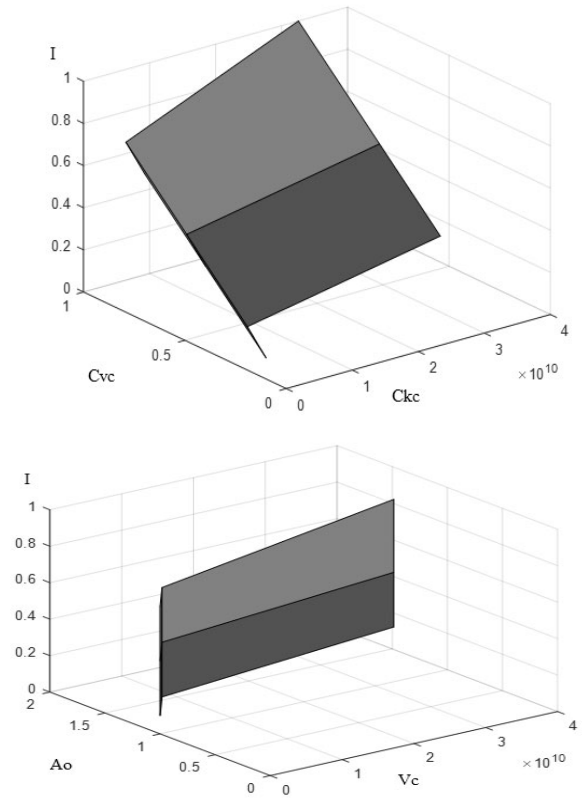


Рис. 9 Графік величини потоку інформації в системі безпеки за (19)

Розглянувши три можливі варіанти вирішення рівняння біля стаціонарного стану системи, можна зробити висновок, що, залежно від співвідношення між дисипацією (втратою енергії) та власною частотою коливань, загасання амплітуди коливань може відбуватися по-різному: або періодично, з поступовим зменшенням амплітуди, або за експоненціальним законом, коли амплітуда згасає швидше.

Для кращого розуміння поведінки системи та для наочного аналізу її руху ми можемо перейти від диференціальної форми рівнянь (8, 9) до дискретної, тобто розглядати систему через певні дискретні моменти часу. Це дозволить здійснити чисельне моделювання для певного інтервалу існування системи.

А саме:

Перехід від диференціальної форми до дискретної: Для аналізу в дискретному часі ми можемо замінити похідні на різницеві оператори, що дозволить апроксимувати рівняння для конкретних значень часу (наприклад, через кроки часу Δt).

Моделювання інтервалу існування системи: Після цього можна буде провести моделювання руху системи протягом певного періоду часу, спостерігаючи, як змінюються параметри, такі як амплітуда, швидкість і інші характеристики.

Це дасть можливість побачити, як змінюються характеристики системи в часі і краще зрозуміти, який тип загасання (поступове чи експоненціальне) буде домінувати в залежності від початкових умов та параметрів системи.

$$\begin{cases} \dfrac{I_{n+1}-I_n}{\Delta t}=(C_{d1}+C_{d2})(Z_p+Q_c+R_c+W_c+F_c+ \\ +Ad_c+V_c+A_{rc}+C_c+M_c)(Z_{pc}Z_k)-(C_v+C_K)I_n) \\ \dfrac{Z_{n+1}-Z_n}{\Delta t}=I_d A(D_c+M_c+N_c+S_c)- \\ -(C_{d2}+C_{d1})\overline{(I+I)}-(C_{d2}+C_{d1})I_n+ \\ +(Z_p+Q_c+R_c+W_c+F_c+Ad_c+V_c+A_{rc}+ \\ +C_c+M_c)(Z_{pc}Z_k)(C_v+C_k)(C_v+C_k)I_n) \end{cases} \quad (20)$$

Розглянемо кроки для моделювання:

1. Умови стаціонарної позиції:

- Для системи задано значення I=0.5 I = 0.5 і Z=1. Ці значення є стаціонарними і визначають початкові умови для подальшого аналізу.

2. Крок моделювання:

- Крок моделювання обрано рівним Δt=0.1 для кожної ітерації. Це означає, що ми будемо розглядати зміни параметрів на кожному кроці часу через інтервали 0.1 одиниці часу.

- Відхилення від стаціонарної позиції:
  Подальше моделювання передбачає, що

$$\begin{cases} I_{n+1}=I_n+(C_{d1}+C_{d2})(Z_p+Q_c+R_c+W_c+ \\ +F_c+Ad_c+V_c+A_{rc}+C_c+M_c)(Z_{pc}Z_k)- \\ -(C_v+C_K)I_n)\Delta t \\ Z_{n+1}=Z_n+(Z_n-I_n)(C_{d2}+C_{d1})+ \\ +(Z_p+Q_c+R_c+W_c+F_c+Ad_c+V_c+ \\ +A_{rc}+C_c+M_c)(Z_{pc}Z_k)(C^2v+ \\ +2C_vC_k+C_k^2))\Delta t \end{cases} \quad (21)$$

- система відхиляється від своїх стаціонарних значень I=0.5 і Z=1, і ми будемо спостерігати, як змінюються ці параметри з часом після відхилення.

3. Імітаційне моделювання:

- Ми проводимо імітаційне моделювання, враховуючи зміни в параметрах з часом, виходячи з їхніх значень на кожному кроці часу.

4. Результати:

- Дані будуть представлені в таблиці 1, де для кожного кроку часу будуть зафіксовані значення параметрів, а також зміни в них. Це дозволить проаналізувати, як система наближається до стаціонарних значень, чи зберігається стійкість до відхилень, і як ці відхилення змінюються з часом.

.

Таблиця 1 Параметри моделювання

№ з/п	Z_p	I	Z	W_c	F_c	V_c	Z_k	Параметри
1	1	0,5	1	1	1	1	1	$\beta \prec \omega_0$
2	1	0,5	1	1	1	1	6	$\beta = \omega_0$
3	1	0,5	1	1	1	1	6	$\beta \succ \omega_0$
C_{d1}	C_{d2}	C_k	A_{dc}	Z_k	Q_c	C_c	M_c	Параметри
1	0,5	0,1	1	1	1	1	1	$\beta \prec \omega_0$
1	1	1	1	1	1	1	1	$\beta = \omega_0$
1	1	6	1	1	1	1	1	$\beta \succ \omega_0$

Графічне представлення результатів.

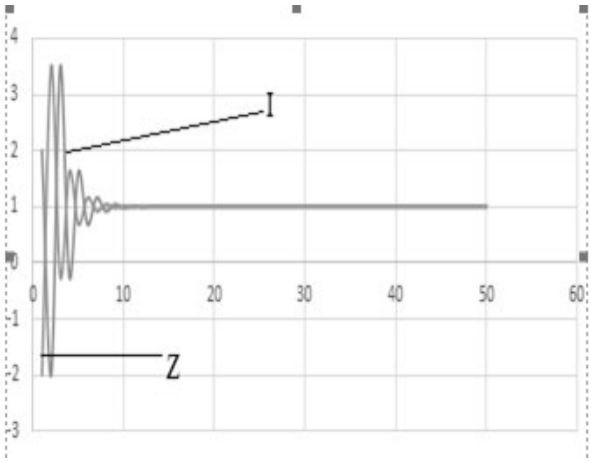


Рис. 10 Графічна залежність амплітуди коливань інтенсивності та захисту даних від кількості ітерацій. $\beta \prec \omega_0$

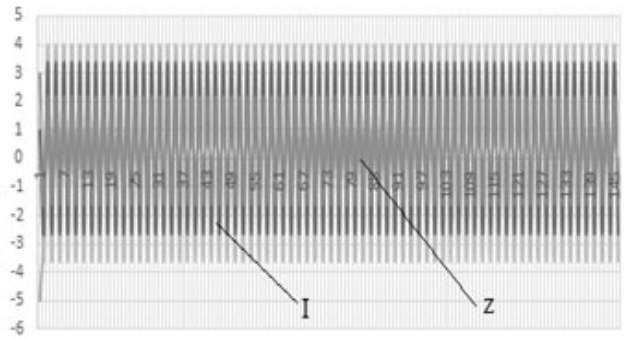


Рис. 11 Графічна залежність амплітуди коливань інтенсивності та захисту даних від кількості ітерацій $\beta = \omega_0$.

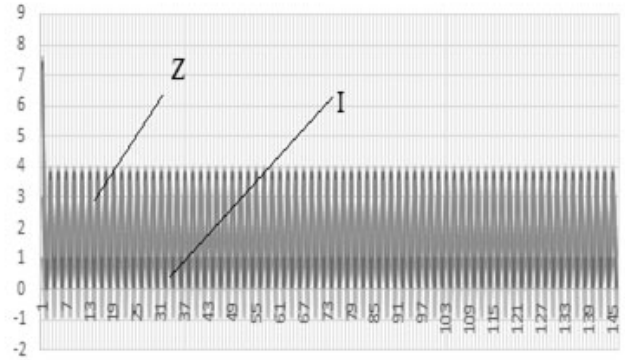


Рис. 12 Графічна залежність амплітуди коливань інтенсивності та захисту даних від кількості ітерацій. $\beta \succ \omega_0$.

ВИСНОВКИ.

Отже, в результаті проведеного дослідження та розробки математичної моделі захисту інформації в локальній мережі можна зробити кілька важливих висновків:

Математична модель захисту інформації:

Розроблена математична модель дозволила детально вивчити взаємозв'язок між параметрами локальної мережі (наприклад, швидкість передачі даних, навантаження на мережу) і ефективністю системи захисту інформації.

Нелінійність системи захисту:

За результатами моделювання було встановлено, що система захисту локальної мережі є нелінійною. Це означає, що зміни в параметрах мережі або інтенсивності передачі даних не призводять до пропорційних змін у ефективності захисту.

Нелінійність може виникати через різноманітні фактори, такі як насичення системи захисту, зростання складності атак в умовах високих навантажень на мережу чи інші фактори, які не піддаються простому лінійному опису.

Імітаційне моделювання:

Імітаційне моделювання, представлене на рисунку 12, підтвердило нелінійність моделі, оскільки результати моделювання показали складні, нелінійні взаємозв'язки між параметрами мережі та рівнем захисту. Це дозволяє з більшою впевненістю стверджувати, що система захисту працює за складним алгоритмом, який не можна описати через прості лінійні функції.

Необхідність подальших досліджень:

Оскільки модель захисту локальної мережі виявилась нелінійною, необхідно провести подальші дослідження, щоб краще зрозуміти її поведінку за різних умов і параметрів. Вивчення цих нелінійних ефектів дозволить розробити більш точні стратегії захисту, оптимізувати

роботу мережі та покращити стійкість системи до атак.

Отже, подальші дослідження повинні бути спрямовані на аналіз поведінки нелінійної моделі, вивчення можливих факторів, що призводять до нелінійних ефектів, а також оптимізацію системи захисту для підвищення її ефективності в умовах змінних параметрів мережі.

ЛІТЕРАТУРА.

[1] Akhramovich V., Hurenko M. Estimation of the indicator of protection of information in means of personal use and a local area network. / Colloquium-journal (Warszawa, Polska). №19 (116), 2020 /Część 1. Pp. 36-41. http://www.colloquium-journal.org.

[2] Ахрамович В.М., Батрак І.Г., Коліда В.П., Шворак К.В. Показник захищеності інформації окремого комп'ютера. Телекомунікаційні та інформаційні технології. ДУТ.- 2021. № 4 (73) -с. 62-77В роботі .

[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: http://doi.org/10.35784/iapgos.5720.2024.03.31

[4] Ахрамович В.М., Лазаренко С.В, Німченко Т.В., Рябова Л.В., Метод розрахунку захисту персональних даних від розширення соціальних мереж. Наукоємні технології. К. НАУ:-2022.Том 53, -№1.-с. 2-12.

[5] Захист інформації в комп'ютерних системах та мережах : навч. посіб. /С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251 с

[6] Локальна мережа як основа безпечної та стабільної роботи IT інфраструктури. https://techexpert.ua/local-measures-as-the-basis-for-safe-and-stable-operation-of-it-infrastructure.

[7] Матов О. Я., Василенко В. С., Будько М. М. Оцінка захищеності в локальних обчислювальних мережах. // К.: Вісті Академії інженерних наук України. 2005, № 2, с. 59 − 73;

[8] В'ячеслав Василенко. Варіанти захисту від загроз в комунікаціях розподілених мереж. https://ela.kpi.ua/server/api/core/bitstreams/d2c5ed53-68b1-40fa-a5a7-edc338667e90/content

[9] Сергій Євдокимов, Сергій Устенко. Розробка системи захисту інформації в локальній мережі підприємства. Геометричне моделювання та інформаційні технології ISSN 2520-2820 (online) К.:2019, № 1. с.20-25

[10] Л.В. Жила, С.В. Сомов. Аналіз систем захисту інформації в локальних обчислювальних мережах. https://journals.nupp.edu.ua › mist › article › view.

[11] Лахно Валерій Анатолійович, Каламан Єрболат, Ягаліева Багдат Есеновна. Криворучко Олена Володимирівна, Десятко Альона Миколаївна, Цюцюра Світлана Володимирівна, Цюцюра Микола Ігорович. Модель захисту локальної мережі навчального закладу серверної системи віртуалізації. Кібербезпека: освіта і наука. № 2 (18), 2022. с. 6-23.

[12] К. Ю. Чернобай, С. В. Грибков. Аналіз та шляхи вирішення проблем захисту комерційних бездротових локальних мереж WI-FI. https://dspace.nuft.edu.ua/server/api/core/bitstreams/5b328d77-e926-4827-912d-c86bcc211276/content.

[13] Togrul Rajabli. How to secure your LAN (Local Area Network. https://www.researchgate.net/publication/378869973_LAN_Security_Methods_and_Aspects_Systematic_Literature_Review

[14] Shakir A Sanni. Securing Local Area Networks with Firewalls: An Overview of its Application to Windows NT and UnixBased Networks. https://micsymposium.org/mics_2001/sanni.pdf

[15] Shakir A Sanni. Securing Local Area Networks with Firewalls: An Overview of its Application to Windows NT and UnixBased Networks. https://micsymposium.org/mics_2001/sanni.pdf

METHOD FOR DETERMINING THE EFFECTIVENESS OF LOCAL NETWORK SECURITY SYSTEM

A mathematical model has been developed and the model of local network protection has been studied. The dependencies of the information flow in the local network on the components of information protection, system security, the size of the threat system to information security, and the network clustering coefficient have been considered.

A system of linear equations has been obtained, which reflects the impact of the information flow change rate on the security of the local network and coefficients that characterize:

the impact of security measures, such as protection against electromagnetic radiation, physical security, data integrity and authenticity control, access control to information, firewall operation, antivirus protection, software and hardware component failures, the impact of personal data leakage rate, the amount of personal data, user identification and authentication, data backup, auditing, the effect of security on information leakage, and the effect of system size on security.

As a result of solving the system of differential equations, mathematical and graphical dependencies of the personal data protection indicator in the local network on various components have been obtained.

By considering three variants of solving the equation near the steady-state of the system, it was concluded that, depending on the ratio of dissipation and the system's own oscillation frequency, the decay of the amplitude to a certain value may occur periodically with a decaying amplitude or according to an exponentially decaying law. A more visual analysis of the system's behavior has been performed by transitioning from the differential form of the equations to the discrete form and modeling a certain interval of the system's existence.

Mathematical and graphical dependencies of the system's natural frequency, oscillation period, and damping coefficient are presented.

Simulation modeling has been carried out for values deviating from the system's steady-state. The simulation results demonstrate that the local network protection system is nonlinear.

Keywords: protection indicator; local network; flow; information; data; leakage; coefficient; system; equation.

Ахрамович Вадим Володимирович
завідувач комп'ютерним центром Національна академія статистики, обліку та аудиту, Київ, Україна

Akhramovych Vadym Volodymyrovych head of the computer center National Academy of Statistics, Accounting and Audit, Kyiv, Ukraine

E-mail 12zstzi@ukr.net

ORCID ID: 0009-0003-2787-8745