КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.776
УДК 004.738.5

Ахрамович Вадим Володимирович
Національна академія статистики, обліку та аудиту, Київ, Україна
ORCID ID: 0009-0003-2787-8745
12zstzi@gmail.com

СПОСІБ ДОСЛІДЖЕННЯ КІЛЬКІСНИХ ПОКАЗНИКІВ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

Анотація. 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.

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

ВСТУП

Швидкий розвиток інформаційних технологій та глобальної мережі Інтернет призвели до формування інформаційного середовища, що впливає на всі сфери людської діяльності. Корпоративні інформаційні системи (КІС) стають сьогодні найважливішим засобом виробництва сучасної компанії, вони дозволяють перетворити традиційні форми бізнесу в електронний бізнес. Електронний бізнес використовує глобальну мережу Інтернет та сучасні інформаційні технології для підвищення ефективності всіх сторін діяльності компаній, включаючи виробництво, маркетинг, продажі, платежі, фінансовий аналіз, пошук співробітників, підтримку клієнтів та партнерських відносин.

У світі інформаційної безпеки ключовим елементом функціонування стало обслуговування бізнесу. У 2024 році кількість кібератак в Україні зросла на 69,8%, досягнувши 4315 інцидентів у порівнянні з 2541 інцидентами роком раніше. Звіт Verizon

показує, що 82% порушень безпеки пов'язані з помилками співробітників: використанням слабких паролів та фішинговими атаками.

Важливою умовою існування електронного бізнесу є інформаційна безпека, під якою розуміється захищеність корпоративної інформації та підтримуючої інфраструктури від випадкових та навмисних впливів, здатних завдати шкоди власникам або користувачам інформації. Збитки від порушення інформаційної безпеки можуть призвести до великих фінансових втрат і навіть до повного закриття компанії. Тому проблеми забезпечення інформаційної безпеки залучають увагу як фахівців у галузі комп'ютерних систем і мереж, так і багатьох користувачів, включаючи компанії, що працюють у сфері електронного бізнесу. Завдання забезпечення безпеки корпоративних інформаційних систем вирішується шляхом побудови комплексної інформаційної системи безпеки.

Без знання та кваліфікованого застосування сучасних інформаційних технологій, стандартів, протоколів та засобів захисту інформації неможливо досягти необхідного рівня інформаційної безпеки комп'ютерних систем та мереж.

Перед тим, як перейти до впровадження безпосередніх методів та засобів захисту інформації, слід визначити реальні загрози інформації, що обробляється в корпоративній мережі, власник мережі повинен мати чітке уявлення про причини їх виникнення та про те, наскільки можливі наслідки вони можуть принести для бізнесу в цілому. Насамперед, порушення конфіденційності корпоративних даних (фінансових, технічних, клієнтських і т. д.) зазнає серйозної репутаційної та фінансової шкоди для компанії. Понад те, за вимогами українського законодавства організації мають дотримуватися норми, регулюючі захист даних та іншої конфіденційної інформації. Порушення цих норм може призвести до серйозних юридичних наслідків, включаючи штрафи та кримінальну відповідальність.

Нарешті, корпоративна інформація є невід'ємною частиною встановлених бізнес-процесів, її втрата чи спотворення можуть спричинити порушення всієї роботи організації.

Захистити корпоративну інформацію — означає своєчасно запобігти витоку або псуванню конфіденційних даних. Захист корпоративної інформації відіграє важливу роль у забезпеченні безпеки та надійності організації, її конкурентоспроможності. Запобігання витоку корпоративних даних та несанкціонованого доступу до конфіденційних даних допомагає зберегти унікальні знання, процеси та технології, які можуть бути ключовими перевагами компанії, а також лояльність клієнтів, які очікують, що їхні особисті дані будуть захищені від розголошення. Слід пам'ятати, що інциденти безпеки, пов'язані з корпоративними та клієнтськими даними, дуже швидко набувають розголосу в мережі та пресі, що негативно позначається на репутації організації будь-якого розміру.

Постановка проблеми. Корпоративні мережі стають дедалі складнішими та динамічнішими, інтегруючи новітні технології. Захист корпоративних мереж є критично важливим, оскільки ці інфраструктури забезпечують вирішення складних завдань у науці, промисловості та інших сферах. Безпека таких систем має стратегічне значення для забезпечення надійності та безперервності їх роботи, а також для мінімізації ризиків зловмисного втручання.

Захист корпоративної мережі — це не одноразовий захід, а постійний процес. Тільки комплексний підхід та регулярний моніторинг допоможуть звести до мінімуму ризики та забезпечити безпеку даних.

В результаті аналізу літературних даних [1] – [17] виявлено, що на даний момент часу відсутнє науково обгрунтоване дослідження, пов’язане з визначенням кількісних параметрів показника захисту інформації від параметрів факторів, що впливають на систему захисту корпоративних мереж.

Практичне та теоретичне значення мало б проведення аналізу моделі системи захисту та отримання кількісних показників системи захисту від впливу можливих факторів.

Причиною цього можуть бути складнощі врахування можливих параметрів взаємодії різних факторів на систему захисту.

Варіантом подолання відповідних труднощів може бути створення математичної моделі лінійної системи захисту та її дослідження, а також дослідження лінійності системи захисту локальної мережі.

Комплексний підхід передбачає, в тому числі, надання інструментів кількісного аналізу показника системи захисту мережі від можливих факторів впливу для адміністраторів мереж та обслуговуючого персоналу, а також для проектувальників та розробників корпоративних мереж.

Аналіз останніх досліджень та публікацій. В статті [1] розроблена математична модель захисту інформації в ПК на основі системи диференціальних рівнянь та проведено моделювання рішень в системі MatLab. Розглянуті три варіанти вирішення рівняння близько стаціонарної стану системи (виконано більш наочний аналіз поведінки системи, з переходом від диференціальної форми рівнянь до дискретної і моделювання деякого інтервалу існування системи), зроблено висновок, що, виходячи з умов співвідношення дисипації і власної частоти коливань величини, 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 [2] 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 [3] виконане дослідження лінійної моделі захисту від розширення соціальної мережі, дозволило отримати систему лінійних рівнянь захисту інформації в соціальних мережах залежно від типу та параметрів розширення мережі. Знайдено умови позиції стаціонарності системи, вирішено систему рівнянь методом «малих відхилень», отримані графічні залежності, проведено ітерацію коливань системи захисту. Застосування методу диференціювання функції захисту дозволило дослідити поведінку системи та отримати кількісні показники захисту від факторів впливу.

В роботі [4] проведено дослідження методів захисту корпоративної мережі, збір та аналіз інформації з приводу політик безпеки. Тому 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 роботі [5] В статті розглянуто методи та способи реалізації захищених каналів VPN, їх переваги та недоліки, розглянуто принципи роботи та призначення технології VPN передані в рамках розподіленої корпоративної мережі, що використовує мережі відкритого доступу.

В статті [6] розглянуто проблеми захисту корпоративних інформаційно-телекомунікаційних мереж, захист яких здійснюється в умовах неповної та нечіткої інформації про мережеві процеси. Тому необхідно повністю забезпечити безпечне функціонування КІТМ в умовах атак зловмисниками на інформаційні ресурси та процеси.

В статті [7] розглянуто методику забезпечення захисту корпоративної мережі зв'язку при віддаленому управлінні. Показано принципи підвищення безпеки корпоративних мереж з урахуванням розробленої методики. Виконано огляд сучасних технологій захисту корпоративних мереж та методів впливу зловмисників на них. Проаналізовано та систематизовано одержані результати. Досліджено доцільність виконання кожного із розглянутих методів захисту за конкретних умов.

В роботі [8] розглянуто сучасні підходи до захисту інформації в корпоративних мережах, що включають синтез типових алгоритмів і технологій, спрямованих на підвищення безпеки даних та забезпечення стійкості до зовнішніх і внутрішніх загроз. Особливу увагу приділено криптографічним методам захисту, що охоплюють шифрування даних, цифрові підписи та управління ключами. Розглянуто також системи виявлення та запобігання вторгнень, які дають змогу ідентифікувати підозрілі активності в мережі та вживати заходів для їх нейтралізації. Крім того, розглянуто технології автентифікації та контролю доступу, які забезпечують ідентифікацію користувачів і захищають корпоративну мережу від несанкціонованого доступу. Під час дослідження детально проаналізовано переваги й недоліки кожного з методів з урахуванням таких критеріїв, як ефективність, продуктивність, витрати на впровадження, а також сумісність із різними корпоративними середовищами. Окрему увагу приділено розгляду факторів, що впливають на вибір того чи іншого алгоритму залежно від специфіки корпоративної інфраструктури, таких як масштаб мережі, чутливість даних та наявність ресурсів. На основі проведеного аналізу сформульовано практичні рекомендації для підприємств щодо вибору оптимальних алгоритмів і засобів захисту інформації, які допомагають досягти високого рівня безпеки при мінімальному впливі на загальну продуктивність мережі.

В статті [9] розглянуті деякі механізми мережевої безпеки, використання яких допоможе забезпечити надійний захист активів корпоративної мережі. Основним завданням під час розроблення подібних рішень захисту є розгляд загальновідомих механізмів та їх комбінацій із подальшим застосуванням окремого рішення.

В роботі [10] відмічається, що навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області інформаційної та кібербезпеки. На базі здобутих знань та умінь фахівець зможе вирішувати професійні задачі, що базуються на сучасних технологіях та методах захисту інформації у сучасних корпоративних систем та мереж. Мета навчальної дисципліни: розкриття сучасних

методів захисту інформації в комп'ютерних системах та мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій.

В статті [11] розглянуто особливості організації інформаційної безпеки (ІБ) корпоративної мережі промислової компанії, яка дає змогу їхнім керівникам впевнитися у тому, що конфіденційна інформація не потрапить до зловмисників чи до рук компаній-конкурентів і не завдасть шкоди самій компанії. 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 діяльності компанії. Тому керівникам служб ІБ корпоративних мереж компаній доводиться враховувати багато особливостей захисту інформації, а також знати, за допомогою яких засобів може забезпечуватися реалізація тих чи інших завдань ІБ.

В роботі [12] дослідженню технологій виявлення та ідентифікації порушників для захисту корпоративних мереж. У дослідженні аналізуються різноманітні підходи та технології, включаючи системи виявлення вторгнень (IDS), системи аналізу безпеки інформації (SIEM), машинне навчання та штучний інтелект. Розглядаються переваги та недоліки кожного підходу, а також їхні можливі застосування в різних сценаріях корпоративних мереж. Дослідження розглядає профіль порушників корпоративних мереж, а також їхні тактики та техніки, що використовуються для здійснення атак. Це включає аналіз типових атак, які найчастіше спрямовані на корпоративні мережі, такі як витік конфіденційної інформації, атаки з використанням шкідливих програм та фішингові атаки. Розуміння тактик та методів, які використовуються зловмисниками, є важливим для ефективного виявлення та запобігання таким атакам

В статті [13] аналізуються недоліки найбільш популярних традиційних засобів захисту корпоративних мереж та обґрунтовується необхідність переходу до нової концепції їхньої безпеки — до використання моніторингово-адаптивного методу їхнього захисту шляхом своєчасного виявлення і нейтралізації атак НСД.

В роботі [14] В сучасному світі з року в рік збільшується кількість кібератак. Ці атаки несуть за собою масові втрати конфіденційних даних, виведення зі стану працездатності критично важливої інфраструктури. Кількість кібератак лише підвищилась з початком пандемії і несе за собою значні фінансові та репутаційні ризики для будь яких компаній. В роботі розглянуті можливі методи проведення тестування безпеки корпоративної мережі організації 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 у корпоративних 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.

В статті [15] Розглянуто способи покращення безпеки мережевої інфраструктури підприємства в умовах сучасних викликів, основні етапи впровадження безпекових рішень, що дають змогу нівелювати потенційні вразливості системи та визначити можливі інформаційні втрати. Примітно, що глобальна цифровізація породжує розвиток нових технологій та підходів в інформаційній індустрії. Пристрої, механізми та аплікації, які раніше були автономними, стають вузлами глобальної інформаційної мережі. Така

трансформація інформаційних технологій значно розширює ландшафт реалізації кіберзагроз. З кожним роком традиційні моделі безпеки комп'ютерних мереж втрачають свою актуальність, тому для їх захисту від сучасних кіберзагроз стає потребою розроблення та впровадження нових підходів, які б підвищували ефективність захисту інформаційних систем. Проаналізовано потенційні вектори атак на мережеву інфраструктуру підприємства на основі традиційної моделі безпеки, розглянуто типові шляхи їх усунення, досліджено складові частини моделі безпеки Zero Trust Network Access та запропоновано низку заходів щодо підвищення стійкості мережевої інфраструктури підприємства до кіберзагроз.

Враховуючи сучасні тенденції поширення кіберзагроз та проведеного аналізу вибраних заходів їх протидії, визначено критичність реалізації загроз кожному з пропрацьованих шляхів підвищення рівня захищеності мережевої інфраструктури підприємства та запропоновано послідовність їх впровадження з урахуванням складності реалізації її захисту за обмежених ресурсів підприємства.

В статті [16] проведено аналіз сучасного впливу мереж зв'язку на безпеку в даній роботі представлена традиційна математична модель впливу на інформаційну безпеку. Виходячи з цього, додатково поєднуючи важливість ефективної реалізації захисту безпеки, заснованого на алгоритмі послідовної локалізації Монте-Карло, новий метод позиціонування може підвищити надійність, оптимізувати область вибірки та покращити точність позиціонування вузла на етапі прогнозування за рахунок інтеграції принципу RSSI та центроїда. 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.

В роботі [17] представлена організація дослідження математичної (стохастичної) моделі на базі ланцюгового апарату Маркова. Розробляються аналітичні моделі та визначаються їх шляхи вирішення. Кінцеві ймовірності для важливих станів визначаються на основі аналітичного розрахунку, а вищі значення для традиційної версії визначаються для обробки даних у регістрах («2»: доступ для запису/читання −0,353; «3»: оновлення персональних даних −0,212). Дослідження ситуацій, заснованих на хмарних обчисленнях, визначає зростаючу ймовірність отримати «2». Представлено обговорення отриманої оцінки на основі графічного представлення результатів аналізу, що дозволяє показати різницю між кінцевими ймовірностями для станів у двох версіях обробки персональних даних.

Метою статті є дослідження кількісних параметрів показника захисту корпоративної мережі та визначення її лінійності.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Втрата рівня захищеності інформації Z у корпоративній мережі є процесом, що відбувається в межах певного часового інтервалу. Позначимо загальний обсяг інформації в системі як I. Потік інформації за межі локальної мережі визначається як dI, а його

швидкість зміни — як $\frac{dI}{dt}$. Логічно припустити, що за відсутності потоку та його зміни витоку інформації не відбувається.

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

Що може впливати на витік інформації? Насамперед це рівень захищеності системи, який визначається впровадженими заходами щодо нейтралізації загроз безпеці персональних даних. Позначимо показник захищеності інформаційної системи як Z. Складемо відповідне рівняння:

$$\frac{dI}{dt} = Z((Z_p + Q_k + R_k + W_k + F_k + Ad_k + V_k + A_{rk} + C_k + B_k + E_k + T_k + Y_k + U_k)(Z_p Z_k) + (C_v + C_k)I \quad (2)$$

де: Z — показник захищенності системи; де Z_p — коефіцієнт, що відображає вплив додаткових заходів щодо захисту інформації (наприклад, боротьба з побічним електромагнітним випромінюванням, фізичний захист і т.п.) (значення 0…1); I — величина потоку інформації; Q_k — коефіцієнт, що відображає контроль цілісності та автентичності даних в мережі (значення 0…1); R_k — коефіцієнт, що відображає резервне копіювання даних (значення 0…1); W_k — коефіцієнт, що відображає розмежування доступу до інформації (значення 0…1); F_k — коефіцієнт, що відображає роботу Firewall (значення 0…1); A_{dk} — коефіцієнт, що відображає аудит (використовується для спостереження, протоколювання) (значення 0…1);. V_k — коефіцієнт, що відображає антивірусне забезпечення (значення 0…1) Z_{pk} — коефіцієнт, що відображає збої та відмови компонент програмного забезпечення, які відповідають за роботу мережі (0,1); Z_k — коефіцієнт, що відображає збої та відмови компонент апаратного забезпечення, які відповідають за роботу мережі (0,1); A_{rk} — коефіцієнт, що відображає систему мережевого резервування (значення 0…1); C_k — коефіцієнт, що відображає систему шифрування (значення 0…1); B_k — коефіцієнт, що відображає розмежування потоків інформації між сегментами мережі (значення 0…1); E_k — коефіцієнт, що відображає фільтрацію спаму (значення 0…1); T_k — коефіцієнт, що відображає фізичну безпеку мережі (значення 0…1); Y_k — коефіцієнт, що відображає підсистему сканування та діагностики (значення 0…1); U_k — коефіцієнт, що відображає підсистему диспетчеризації процесів контролю і забезпечення цілісності (значення 0…1); Cv — коефіцієнт, що відображає вплив швидкості витоку персональних даних; C_k — коефіцієнт, що відображає вплив кількості персональних даних на їх витік.

Інтерпретувати дане рівняння можна наступним чином. Витік інформації залежить:

- від розміру інформаційної системи (отже, в якійсь мірі і від кількості даних);
- від швидкості витоку даних
- витік інформації купірується захищенністю системи (заходами щодо нейтралізації загроз безпеки інформації).

Далі розглянемо, від чого залежить захищеність системи — Z. Визначимо захищеність системи як здатність системи протистояти несанкціонованому доступу до конфіденційних персональних і інших даних. Отже, захищеність системи буде залежати:

- від розмірів системи (як і від кількості даних);
- загроз безпеки інформації від взаємодієї між користувачами.

ISSN 2663 - 4023

Складемо рівняння:

$$\frac{dZ}{dt} = I_d A_k (D_k + M_k + N_k + S_k + K_k + Q_k) - (C_{d2} + C_{d1})I \quad (3)$$

де: I_d — коефіцієнт, що відображає ідентифікацію користувачів в мережі (значення 0 або 1); A_k — коефіцієнт, що відображає автентифікацію користувачів в мережі (значення 0 або 1); D_k — коефіцієнт, що відображає proxy-сервери (значення 0…1); M_k — коефіцієнт, що відображає міжмережевий екран (значення 0…1); N_k — коефіцієнт, що відображає мережу VPN (значення 0…1); S_k — коефіцієнт, що відображає засоби, що виявляють неоднорідності та порушення, які виникають в мережі; (значення 0…1); C_{d1} — коефіцієнт, що відображає вплив захищеності на витік інформації) (значення 0…1);. C_{d2} — коефіцієнт, що відображає вплив розмірів системи на захищеність (значення 0…1);. K_k — коефіцієнт, що відображає системи виявлення й запобігання вторгненню, наприклад (IDS, IPS) (значення 0…1); O_k — коефіцієнт, що відображає підмережі захисту (значення 0…1);

Створимо систему із рівнянь (2) і (3).

$$\begin{cases} \frac{dI}{dt} = Z((Z_p + Q_k + R_k + W_k + F_k + Ad_k + V_k + A_{rk} + C_k + B_k + E_k + T_k + Y_k + U_k)(Z_p Z_k) + (C_v + C_k)I \\ \frac{dZ}{dt} = I_d A_k (D_k + M_k + N_k + S_k + K_k + Q_k) - (C_{d2} + C_{d1})I \end{cases} \quad (4)$$

Визначимо стаціонарний стан системи, яку описують рівняння (4). Для цього необхідно врахувати умови стаціонарності $dI = 0; \frac{dI}{dt} = 0$. Таким чином, отримуємо:

$$\begin{cases} Z((Z_p + Q_k + R_k + W_k + F_k + Ad_k + V_k + A_{rk} + C_k + B_k + E_k + T_k + Y_k + U_k)(Z_p Z_k) + \\ +(C_v + C_k)I \\ I_d A_k (D_k + M_k + N_k + S_k + K_k + Q_k) - (C_{d2} + C_{d1})I \end{cases} \quad (5)$$

З другого рівняння системи отримаємо:

$$\bar{I} = \frac{I_d A_k (D_k + M_k + N_k + S_k + K_k + Q_k)}{(C_{d2} + C_{d1})} \quad (6)$$

Розглядаючі перше рівняння системи рівнянь (5) отримаємо $\bar{Z}$.

$$\bar{Z} = \frac{I_d A_k (D_k + M_k + N_k + S_k + K_k + Q_k) - (C_{d2} + C_{d1})}{((Z_p + Q_k + R_k + W_k + F_k + Ad_k + V_k + A_{rk} + C_k + B_k + E_k + T_k + Y_k + U_k)(Z_{p1} Z_k)(C_{d2} + C_{d1})} \quad (7)$$

Отже, умови для досягнення стаціонарного стану системи такі:

$$\begin{cases} \bar{I} = \frac{I_d A_k (D_k + M_k + N_k + S_k + K_k + Q_k)}{(C_{d2} + C_{d1})} \\ \bar{Z} = \frac{I_d A_k (D_k + M_k + N_k + S_k + K_k + Q_k) - (C_v + C_k)}{((Z_p + Q_k + R_k + W_k + F_k + Ad_k + V_k + A_{rk} + C_k + B_k + E_k + T_k + Y_k + U_k)(Z_p Z_k)(C_{d2} + C_{d1})} \end{cases} \quad (8)$$

ISSN 2663 - 4023

Розв’яжемо систему рівнянь (8) за допомогою методу «малих відхилень» $I = \bar{I} + I; Z = \bar{Z} + Z$. Отже, система рівнянь набуде наступного вигляду:

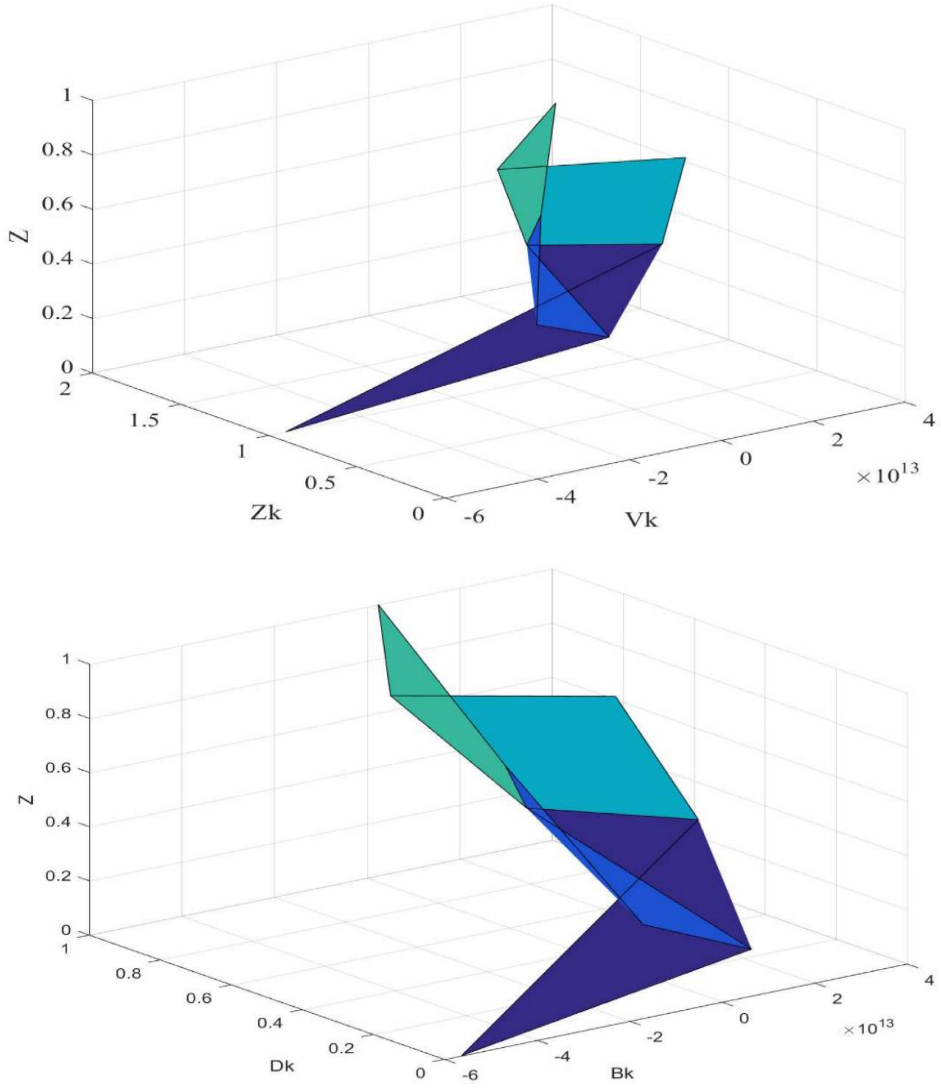

Рис. 1. Значення показника захисту інформації за залежністю (7)

$$\begin{cases} \dfrac{dI}{dt} = (\bar{Z} + Z)((Z_p + Q_k + R_k + W_k + F_k + Ad_k + V_k + A_{rk} + C_k + B_k + E_k + T_k + Y_k + U_k)(Z_p Z_k) + (C_v + C_k)(\bar{I} + I) \\ \dfrac{dZ}{dt} = I_d A_k (D_k + M_k + N_k + S_k + K_k + Q_k) - (C_v + C_k)(\bar{I} + I) \end{cases} \quad (9)$$

$$\begin{cases} \dfrac{dI}{dt} = Z(C_{d1} + C_{d2})((Z_p + Q_k + R_k + W_k + F_k + Ad_k + V_k + A_{rk} + C_k + B_k + E_k + T_k + Y_k + U_k)(Z_p Z_k) - (C_v + C_K)I \\ \dfrac{dZ}{dt} = -I(C_{d2} + C_{d1}) + I_d A_k (D_k + M_k + N_k + S_k + K_k + Q_k)(C_v + C_k) \end{cases} \quad (10)$$

ISSN 2663 - 4023

Диференціюючи перше рівняння системи (10) отримуємо:

$$\frac{d^2I}{dt^2} = -I(C_{d1}+C_{d2})((Z_p+Q_k+R_k+W_k+F_k+Ad_k+V_k+A_{rk}+C_k+B_k+E_k+T_k+Y_k+U_k)(Z_pZ_k)(C_v+C_k))- \\ -(C_v+C_K)\frac{dI}{dt} \quad (11)$$

$$\frac{d^2I}{dt^2}+(C_v+C_K)\frac{dI}{dt}+(C_{d1}+C_{d2})((Z_p+Q_k+R_k+W_k+F_k+Ad_k+V_k+A_{rk}+C_k+B_k+E_k+T_k+Y_k+ \\ +U_k)(Z_pZ_k)(C_v+C_k))I=0 \quad (12)$$

Рівняння (12) є рівнянням гармонічного осцилятора з амплітудою, що згасає, де:

$$\omega_0 = \sqrt{\begin{matrix}(C_{d1}+C_{d2})((Z_p+Q_k+R_k+W_k+F_k+Ad_k+V_k+A_{rk}+C_k+B_k+E_k+T_k+Y_k+U_k)(Z_pZ_k)+ \\ +I_dA_k(D_k+M_k+N_k+S_k+K_k+Q_k)\end{matrix}} \quad (13)$$

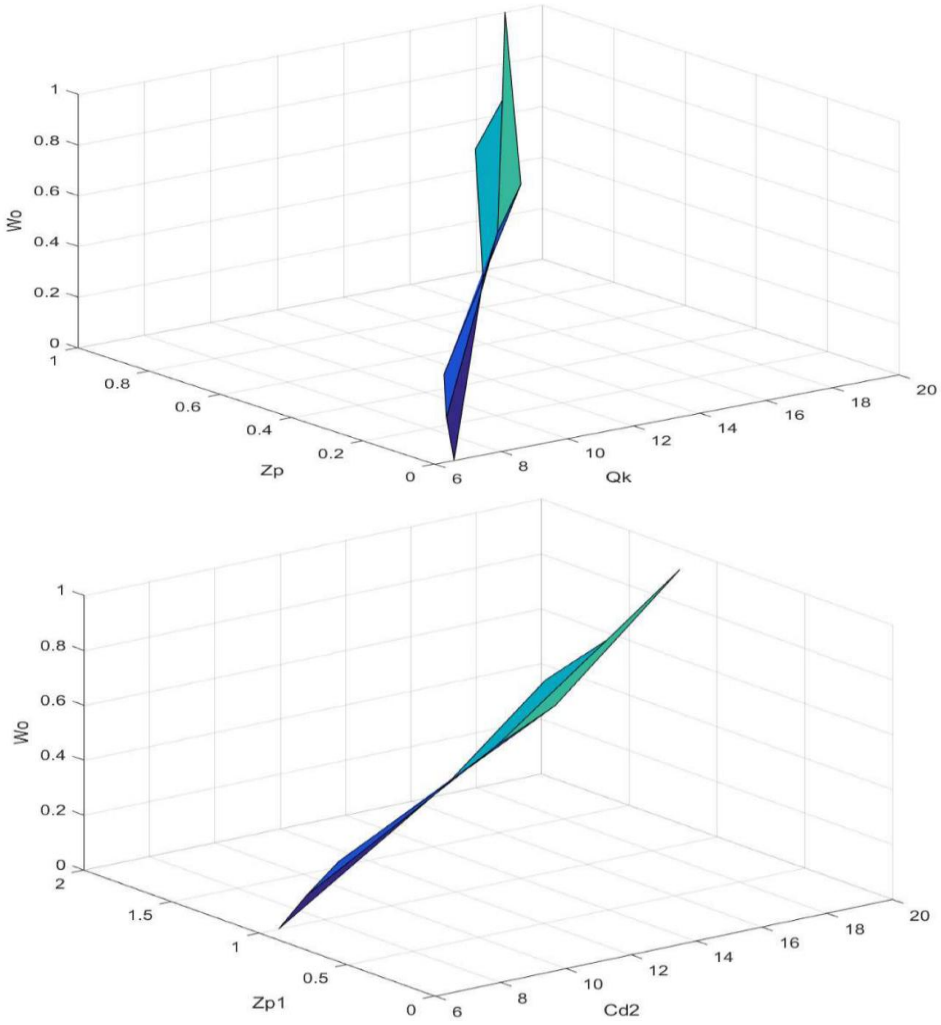

Рис. 2. Особиста частота системи захисту за (13)

ISSN 2663 - 4023

$$\omega = \sqrt{(C_{d1}+C_{d2})((Z_p+Q_k+R_k+W_k+F_k+Ad_k+V_k+A_{rk}+C_k+B_k+E_k+T_k+Y_k+U_k)Z_pZ_k)-\frac{(C_v+C_K)^2}{4}}) \quad (14)$$

$$T = \frac{2\pi}{\sqrt{(C_{d1}+C_{d2})((Z_p+Q_k+R_k+W_k+F_k+Ad_k+V_k+A_{rk}+C_k+B_k+E_k+T_k+Y_k+U_k)(Z_pZ_k)(C_v+C_k)-\frac{(C_v+C_K)^2}{4}}}) \quad (15)$$

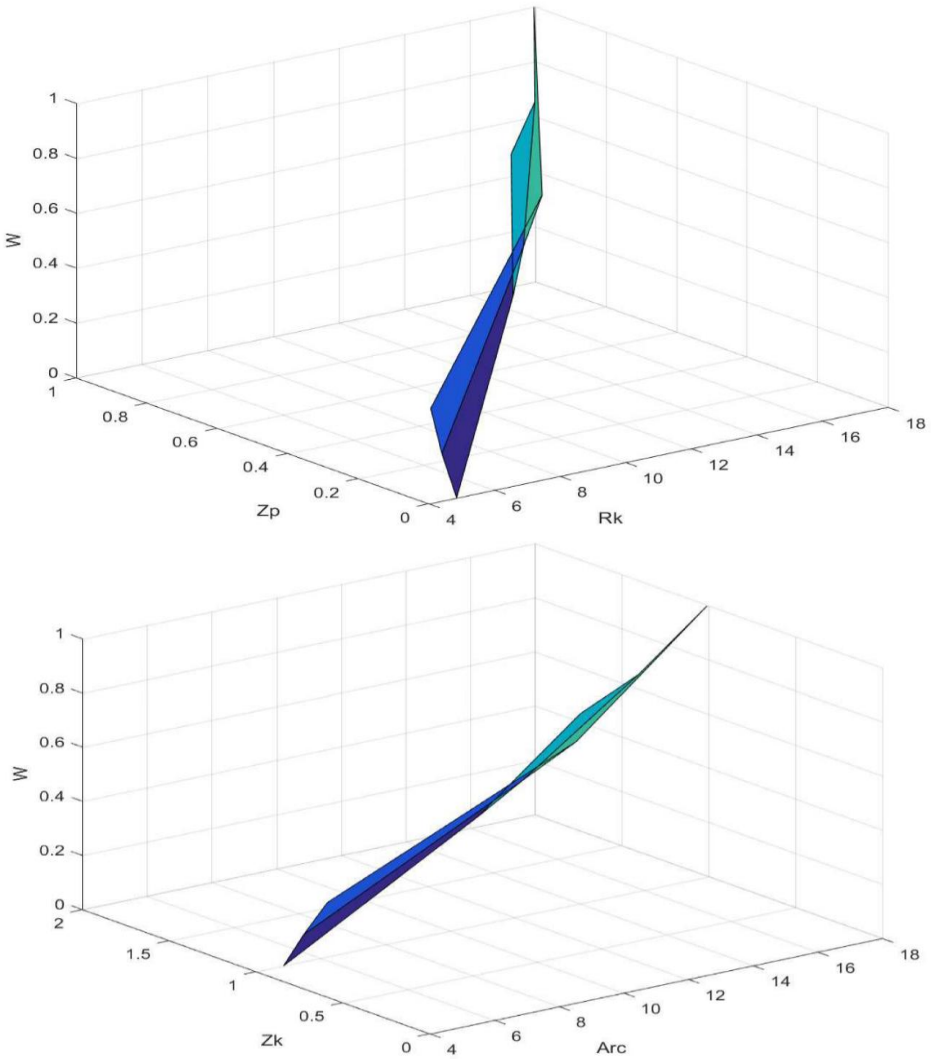

Рис. 3. Частота системи захисту за (14)

ISSN 2663 - 4023

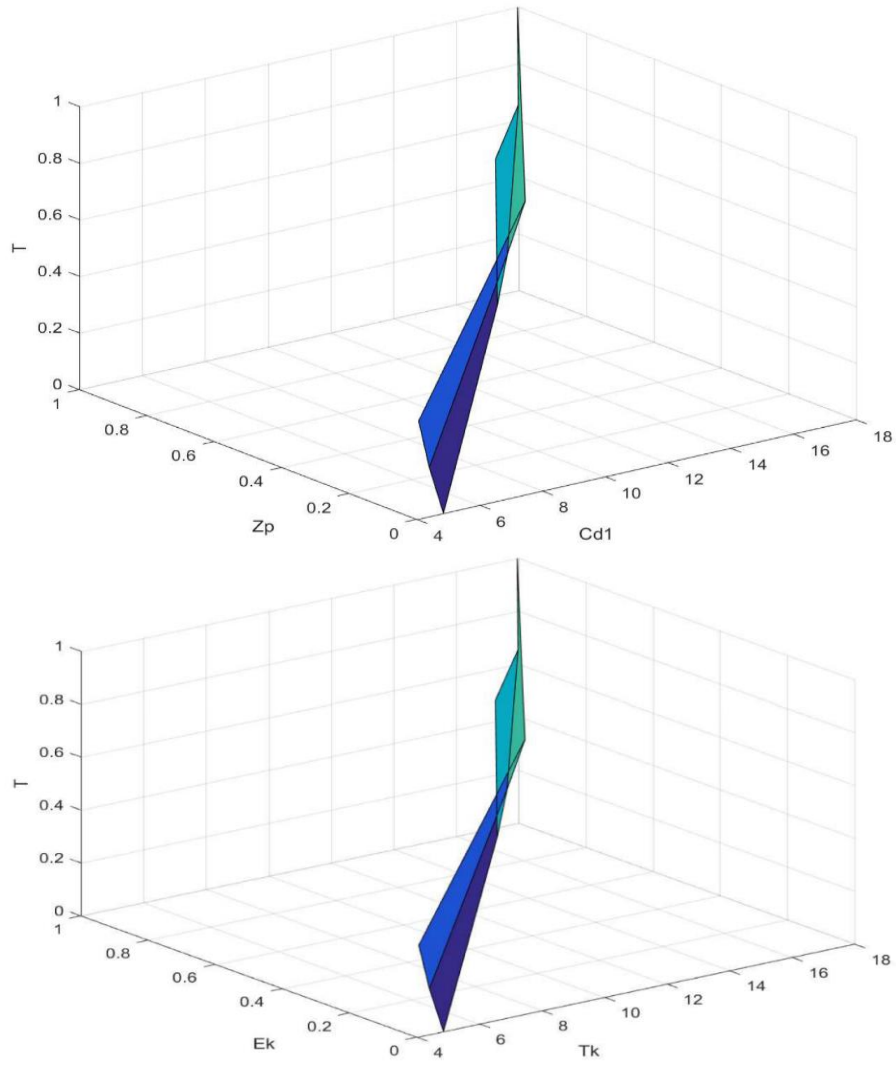

Рис. 4. Період коливань системи захисту за (15)

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

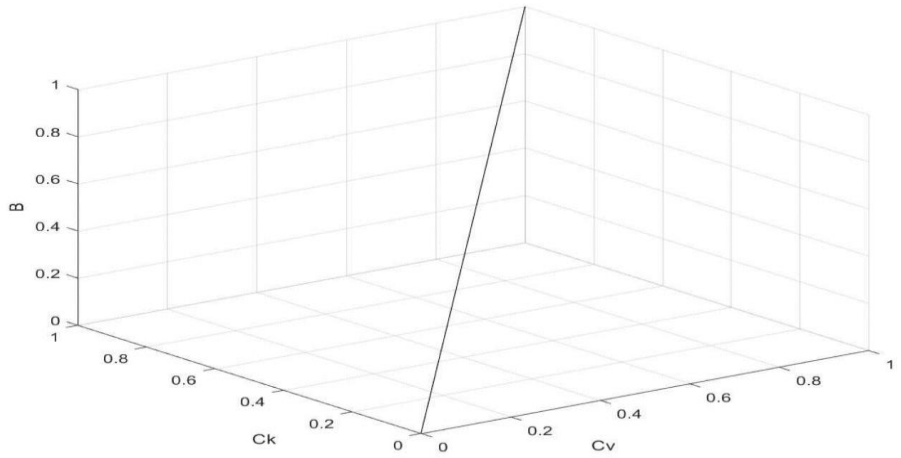

Рис. 5. Коефіцієнт демпфування системи захисту за (16)

ISSN 2663 - 4023

Рішення рівняння гармонічного осцилятора поділяється на три можливі випадки:

1. $$\beta \prec \omega_0 : I = A_0 \exp(-\frac{(C_v + C_K)}{2} \cos(\sqrt{\begin{matrix}(C_{d1} + C_{d2}) + ((Z_p + Q_k + R_k + W_k + F_k + Ad_k + V_k + A_{rk} + C_k + \\ + B_k + E_k + + T_k + Y_k + U_k)(Z_p Z_k)(C_v + C_k) - \frac{(C_v + C_K)^2}{4} t + \varphi_0)\end{matrix}} \quad (17)$$

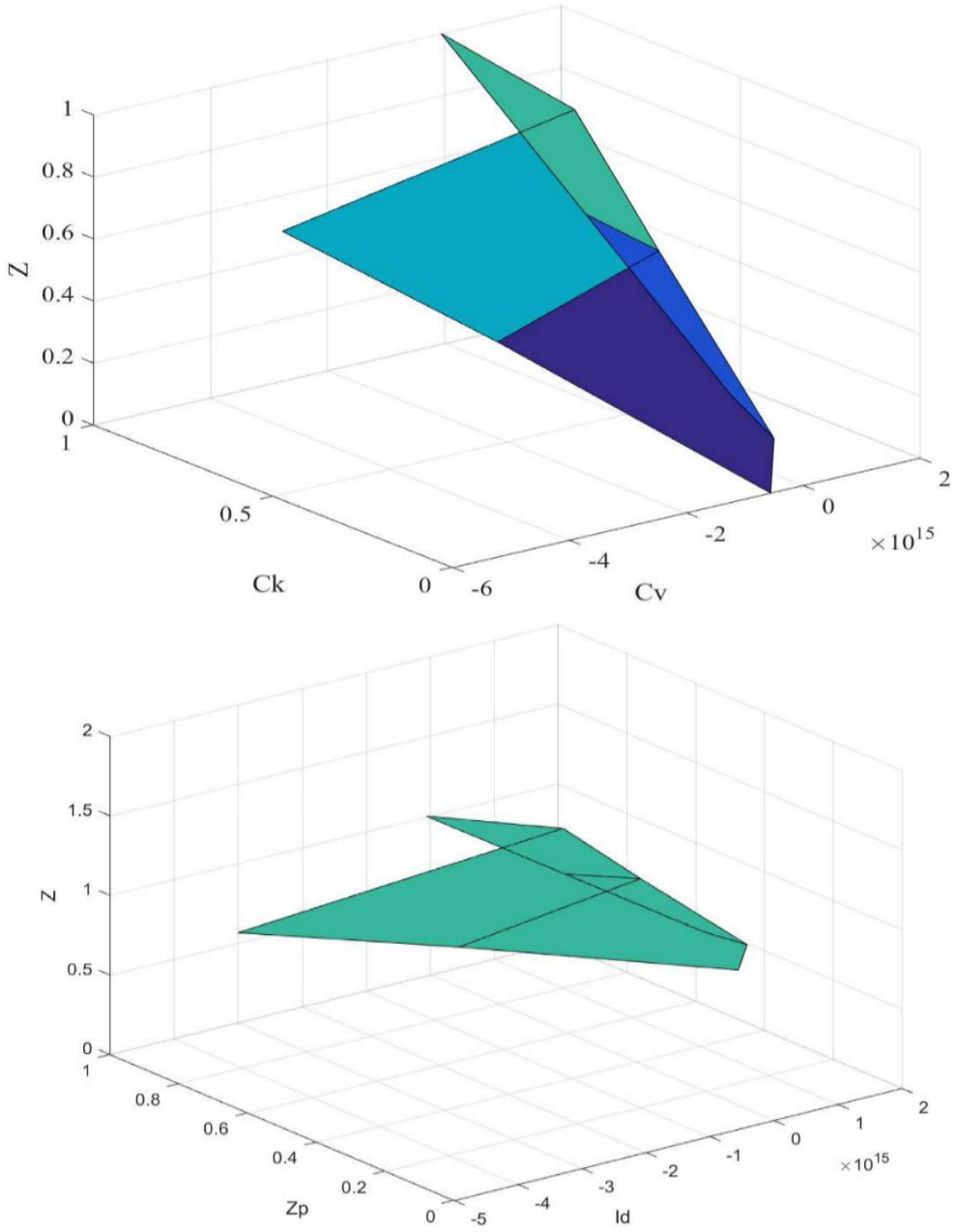

Рис. 6. Показник захисту інформації в системі захисту за (5)

ISSN 2663 - 4023

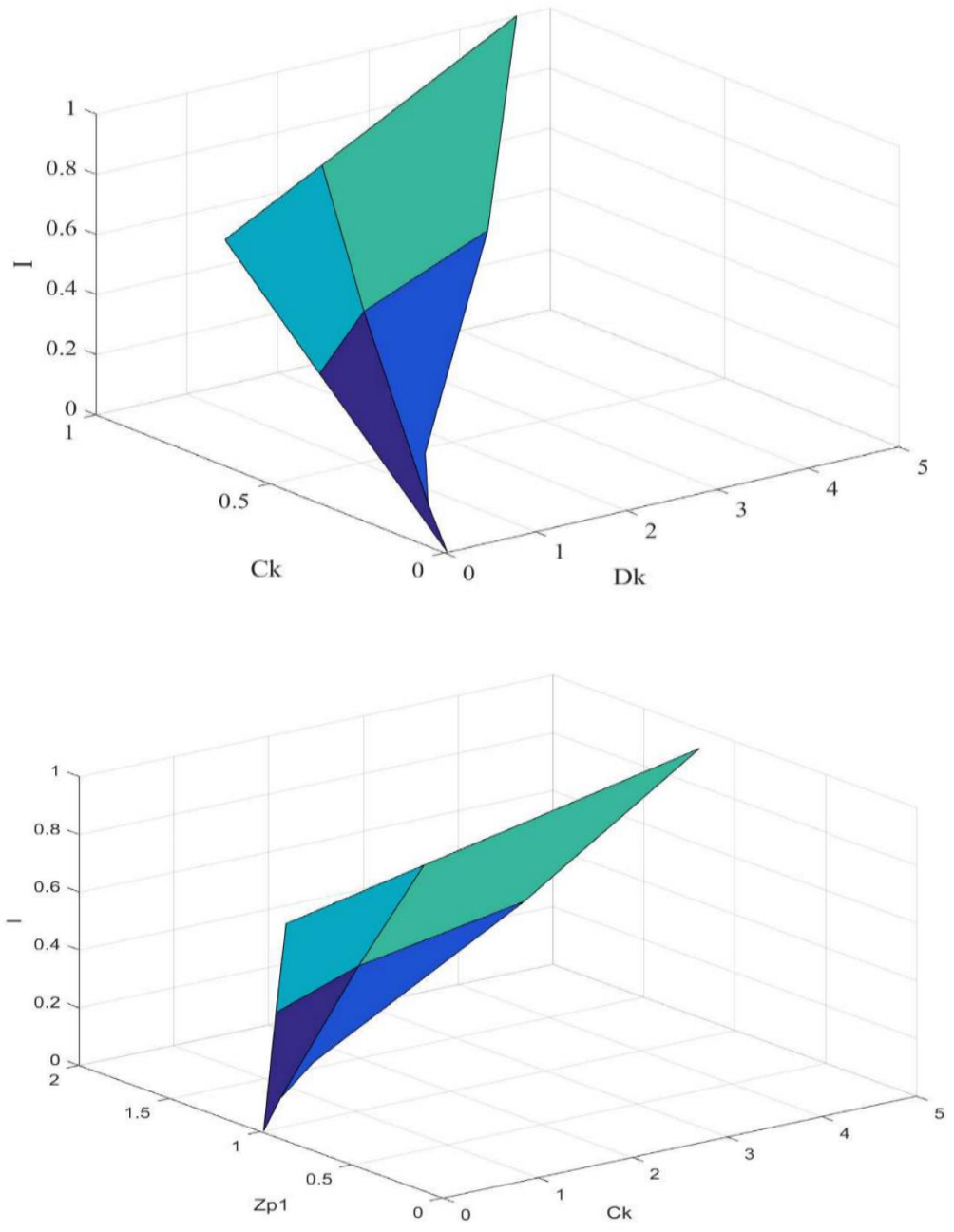

Рис. 7. Величина потоку інформації за (17)

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

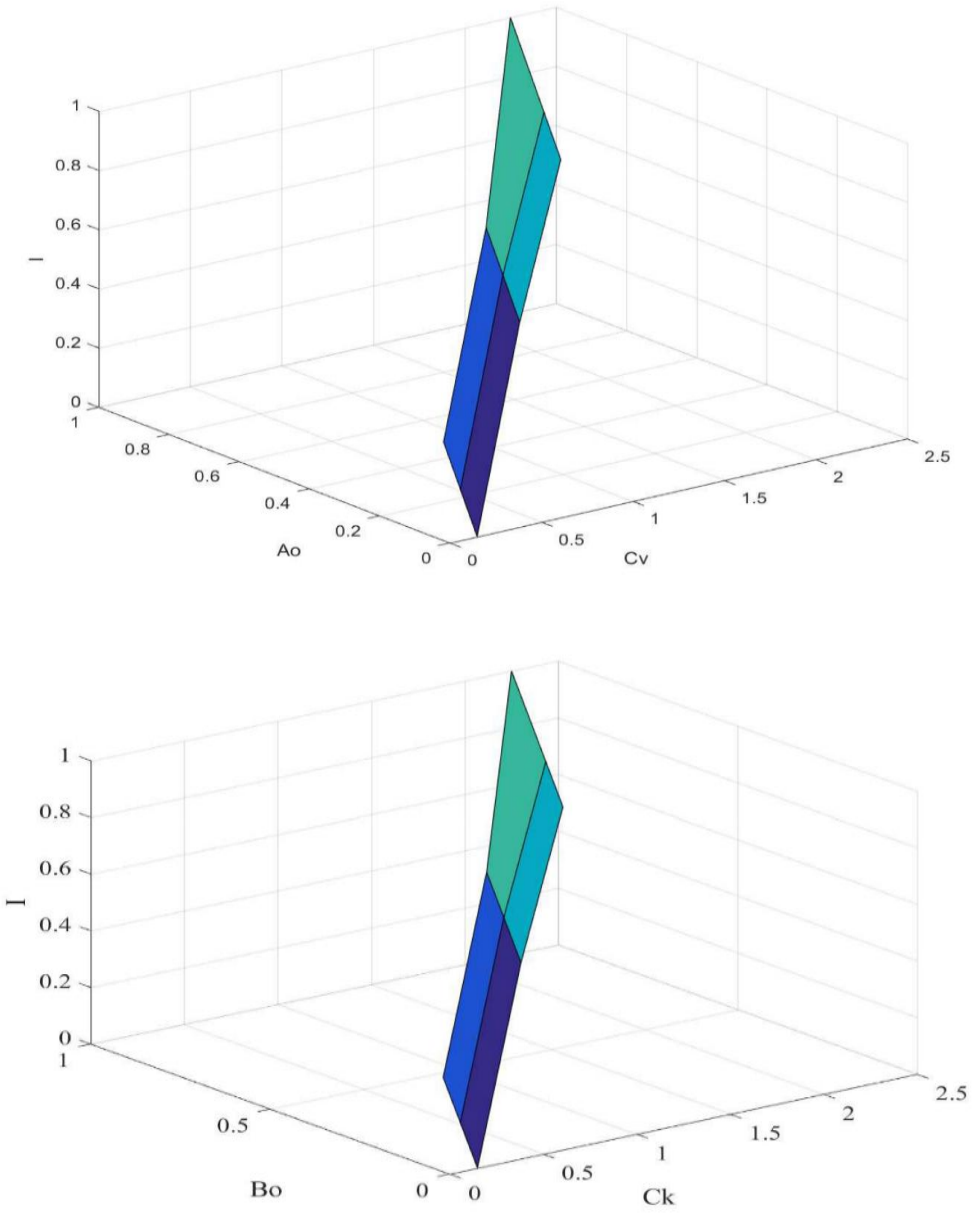

Рис. 8. Величина потоку інформації за (18)

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

3. *де*

$$y_{12} = \beta \pm \sqrt{\frac{(C_v + C_K)^2}{4} - (C_{d1} + C_{d2})((\mathrm{Z}_p + \mathrm{Q}_k + \mathrm{R}_k + \mathrm{W}_k + \mathrm{F}_k + \mathrm{Ad}_k + \mathrm{V}_k + \mathrm{A}_{rk} + \mathrm{C}_k + \mathrm{B}_k + \mathrm{E}_k + \mathrm{T}_k + \mathrm{Y}_k + \mathrm{U}_k)(\mathrm{Z}_p \mathrm{Z}_k)(C_v + C_k)} \quad (19)$$

ISSN 2663 - 4023

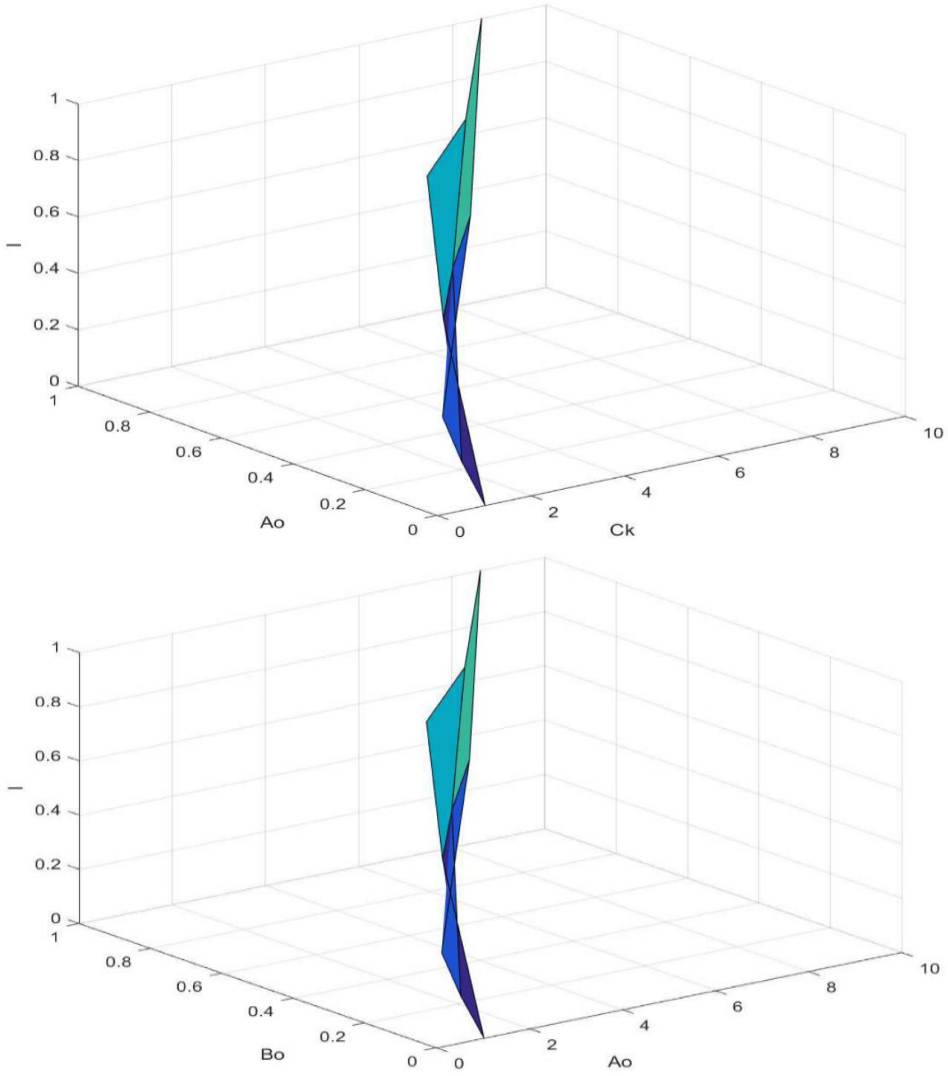

Рис. 9. Величина потоку інформації в системі захисту за (19)

Розглянувши три варіанти розв'язку рівняння поблизу стаціонарного стану системи, можна зробити висновок, що, з огляду на співвідношення дисипації та власної частоти коливань, загасання амплітуди відбувається періодично, з поступовим зменшенням амплітуди, або за експоненційним законом. Для більш детального аналізу поведінки системи перейдемо від диференціальної форми рівнянь (8, 9) до дискретної і проведемо моделювання на певному інтервалі існування системи. А саме:

$$\begin{cases} \dfrac{I_{n+1}-I_n}{\Delta t} = (C_{d1}+C_{d2})((\mathrm{Z}_p+\mathrm{Q}_k+\mathrm{R}_k+\mathrm{W}_k+\mathrm{F}_k+\mathrm{Ad}_k+\mathrm{V}_k+\mathrm{A}_{rk}+\mathrm{C}_k+\mathrm{B}_k+\mathrm{E}_k+ \\ +\mathrm{T}_k+\mathrm{Y}_k+\mathrm{U}_k)(\mathrm{Z}_p\mathrm{Z}_k)-(C_v+C_K)I_n) \\ \dfrac{Z_{n+1}-Z_n}{\Delta t} = I_d A_k(D_k+M_k+N_k+S_k+K_k+Q_k)-(C_{d2}+C_{d1})(\bar{I}+I)-(C_{d2}+C_{d1})I_n+ \\ +((\mathrm{Z}_p+\mathrm{Q}_k+\mathrm{R}_k+\mathrm{W}_k+\mathrm{F}_k+\mathrm{Ad}_k+\mathrm{V}_k+\mathrm{A}_{rk}+\mathrm{C}_k+\mathrm{B}_k+\mathrm{E}_k+\mathrm{T}_k+\mathrm{Y}_k+\mathrm{U}_k)(\mathrm{Z}_p\mathrm{Z}_k) \\ (C_v+C_k)(C_v+C_k)I_n) \end{cases} \quad (20)$$

ISSN 2663 - 4023

$$\begin{cases} I_{n+1} = I_n + (C_{d1} + C_{d2})((Z_p + Q_k + R_k + W_k + F_k + Ad_k + V_k + A_{rk} + C_k + B_k + E_k + T_k + Y_k + \\ + U_k)(Z_p Z_k) - (C_v + C_K) I_n)\Delta t \\ Z_{n+1} = Z_n + (Z_n - I_n)(C_{d2} + C_{d1}) + ((Z_p + Q_k + R_k + W_k + F_k + Ad_k + V_k + A_{rk} + C_k + B_k + E_k + \\ + T_k + Y_k + U_k)(Z_p Z_k)(C^2_v + 2C_v C_k + C_k^2))\Delta t \end{cases} \quad (21)$$

Згідно з умовами стаціонарного стану системи, значення I і *Z* будуть дорівнювати 0.5 та 1 відповідно. Крок моделювання вибираємо рівним 0.1 для всіх ітерацій, тому в таблиці1 цей крок не буде зазначено. Величини I_{sp}, Z_{sp} відображають стаціонарні значення параметрів, якщо ці значення були досягнуті за кінцеву кількість ітерацій. Далі проведемо імітаційне моделювання для значень $\beta \prec \omega_0, \beta = \omega_0, \beta \succ \omega_0$ з відхиленням від стаціонарного стану системи. Дані будуть представлені в таблю 1.

Таблиця 1

Параметри моделювання

№ з/п	Z_p	I	Z	C_v	C_{d1}	C_{d2}	C_k	A_{dk}	A_{rk}	Параметри
1	1	0,5	0,5	0,1	1	0,5	0,1	1	1	$\beta \prec \omega_0$
2	1	0,5	0,5	1	1	1	1	1	1	$\beta = \omega_0$
3	1	0,5	0,5	6	1	1	6	1	1	$\beta \succ \omega_0$
№ з/п	W_k	F_k	V_k	Z_p	Z_k	Q_k	w_k	C_k	M_k	Параметри
1	1	1	1	1	1	1	1	1	1	$\beta \prec \omega_0$
2	1	1	1	6	1	1	1	1	1	$\beta = \omega_0$
3	1	1	1	6	1	1	1	1	1	$\beta \succ \omega_0$
№ з/п	R_k	F_k	B_k	E_k	T_k	Y_k	U_k			Параметри
1	1	1	1	1	1	1	1			$\beta \prec \omega_0$
2	1	1	1	6	1	1	1			$\beta = \omega_0$
3	1	1	1	6	1	1	1			$\beta \succ \omega_0$

ISSN 2663 - 4023

Візуалізація результатів

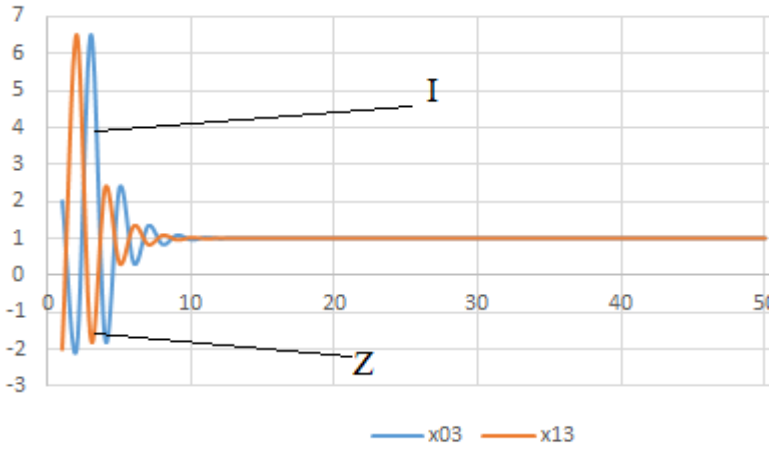

Рис. 10. Залежність інтенсивності та захисту даних від кількості ітерацій (140). Дані складових взяті з табл. 1. $\beta \prec \omega_0$

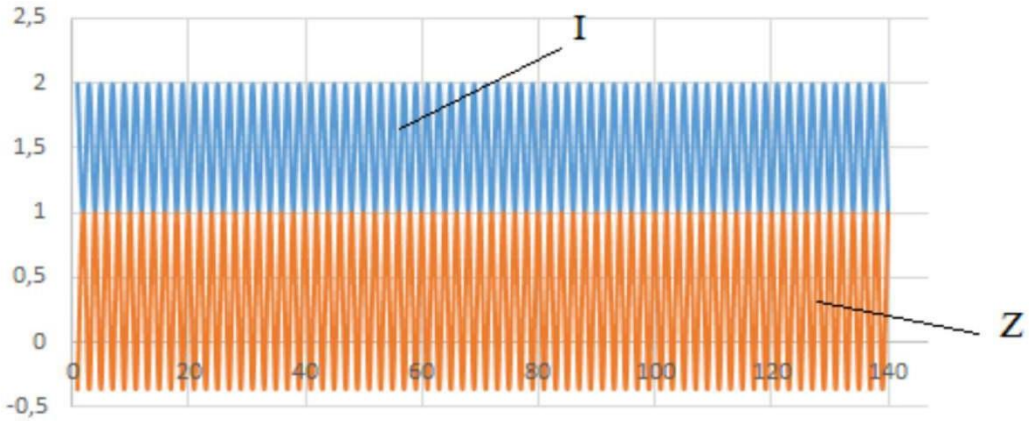

Рис. 11. Залежність інтенсивності та захисту даних від кількості ітерацій (140) Дані складових взяті з табл. 1. $\beta = \omega_0$

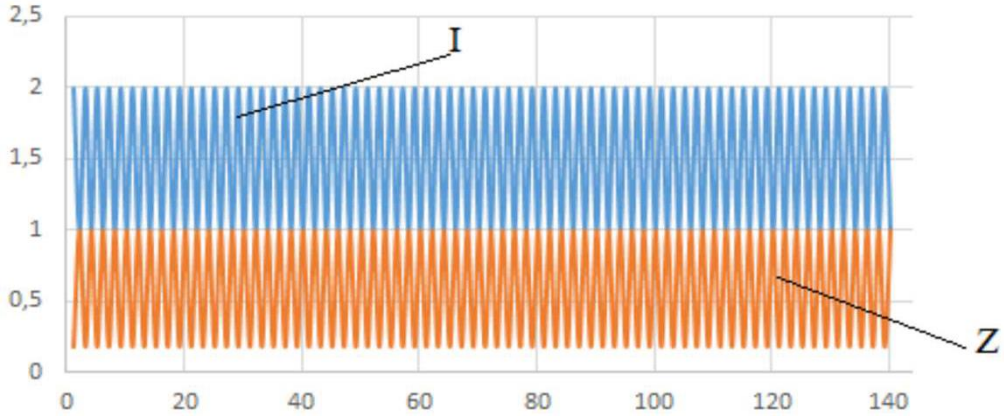

Рис. 12. Залежність інтенсивності та захисту даних від кількості ітерацій (140). Дані складових взяті з табл. 1. $\beta \succ \omega_0$.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ.

У результаті проведеного дослідження отримано систему лінійних рівнянь, яка описує залежність швидкості зміни потоку інформації від рівня захищеності корпоративної мережі та коефіцієнтів, що враховують вплив заходів безпеки. Зокрема, проаналізовано вплив додаткових заходів захисту інформації, таких як боротьба з побічним електромагнітним випромінюванням, фізичний захист, контроль цілісності та автентичності даних, розмежування доступу, робота Firewall та антивірусного забезпечення. Також враховано фактори, пов'язані із збоєм або відмовою програмних і апаратних компонентів, швидкістю витоку персональних даних, їх кількістю, а також процесами ідентифікації, автентифікації користувачів, резервного копіювання даних та аудиту. Досліджено вплив рівня захищеності на ймовірність витоку інформації та залежність захищеності мережі від її розмірів.

Розв'язання системи лінійних диференціальних рівнянь дозволило отримати кількісні математичні та графічні залежності показника захисту персональних даних у корпоративній мережі від різних факторів. Результати математичного моделювання підтвердили, що система захисту корпоративної мережі має нелінійний характер, що також підтверджено імітаційним моделюванням (рис. 12).

Подальші дослідження повинні бути спрямовані на розширення та вдосконалення нелінійної моделі захисту локальної мережі, зокрема на дослідження динамічних характеристик системи, оптимізацію механізмів захисту та оцінку впливу новітніх загроз на безпеку корпоративного середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Akhramovych, V. M., Batrak, I. H., Kolida, V. P., & Shvorak, K. V. (2021). Information Security Indicator of an Individual Computer. *Telecommunications and Information Technologies. DUT, 4(73),* 62–77.
2. Akhramovych, V., Pepa, Y., Zahynei, A., Akhramovych, V., Dzyuba, T., & Danylov, I. (2024). Method for Calculating the Information Security Indicator in Social Media with Consideration of the Path Duration Between Clients. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska – IAPGOS, 14(1),* 71–77. http://doi.org/10.35784/iapgos.5720.2024.03.31.
3. Akhramovych, V. M., Lazarenko, S. V., Nimchenko, T. V., & Ryabova, L. V. (2022). Method for Calculating Personal Data Protection Against Social Network Expansion. *Science-Intensive Technologies. K. NAU, 53(1),* 2–12.
4. Tkach, Yu. M., Yakovlev, O.O., & Lysytsia, T.A. (2021). Protection of Corporate Networks Against Human Influence Using Technical Means. *Informatics and Mathematical Methods in Simulation, 11(4),* 358–364.
5. Parkhomenko, I. I., Galkin V. V. (2020). Methods for Protecting Corporate Network Channels Based on VPN Solutions. *Modern Information Protection, 4,* 35–40.
6. Kostiuk, Yu.V. (2022). Problems of Corporate Information and Telecommunication Networks Protection. In *Modern Trends in the Development of Financial and Innovation-Investment Processes in Ukraine: Materials of the 5th International Scientific and Practical Conference,* 781–783.
7. Chernoshtan, A. M., & Vlasov, O. M. (2020). Methodology for Ensuring Corporate Network Security in Remote Management. *Scientific Notes of UNDI, 1(57),* 10–14.
8. Shkitov, A. A., & Kropyvnytskyi, D. R. (2021). Synthesis of Standard Information Security Algorithms in Corporate Networks. *Information Management Technologies, 2,* 129–135.
9. Chinchyk, D., Korobeinikova, T., & Zakharchenko, S. (2021). Methods and Means of Comprehensive Protection of Corporate Networks. *InterConf, (84),* 433–450. https://doi.org/10.51582/interconf.7-8.11.2021.043
10. Sachuk, Yu.V. (2018). *Information Security in Corporate Networks: Selective Academic Discipline Program for Bachelor's Training in the Field of Information Security, Specialty 125 Cybersecurity,*

Educational Program Information Security. Lesya Ukrainka Eastern European National University, Department of National Security. https://evnuir.vnu.edu.ua/handle/123456789/15562.

11. Milyan, K. V., & Hrytsiuk, Yu. I. (2022). Features of Organizing Information Security in the Corporate Network of an Industrial Company. *Scientific Bulletin of NLTU of Ukraine, 23(4),* 311–327.
12. Kostiuk, Yu. V., & Voitkevych, A. A. (2024). Research on Technologies for Detecting and Identifying Violators for Corporate Network Protection. *Science and Technology Today, 4(23),* 1017–1032. https://doi.org/10.52058/2786-6025-2024-4(32)-1017-1032
13. Khoroshko, V. A., & Shoroshev V. V. (2019). Shortcomings of Traditional Corporate Network Security Measures in Intranet and the Necessity of Implementing New Protection Methods. *Information Protection,* 5–17.
14. Tyshyk, I. Ya. (2022). Testing an Organization's Corporate Network for Unauthorized Access. *Cybersecurity: Education, Science, Technology, 2(18),* 39–46.
15. Syrotynskyi, R. M., & Tyshyk, I. Ya. (2024). Improving Enterprise Network Infrastructure Security Under Modern Challenges and Limited Resources. *COMPUTER SYSTEMS AND NETWORKS, 6(1),* 155–164.
16. Chong Tian a Siqiu Hu. (2020). Mathematical modeling of the analysis of the impact on the security of the communication network based on the Monte Carlo algorithm. *Computer Communications, 157,* 20–27.
17. Romansky, R. (2023). Mathematical Model Investigation of a Technological Structure for Personal Data Protection, *Axioms, 12(2).* https://doi.org/10.3390/axioms12020102

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Vadym Akhramovych
National Academy of Statistics, Accounting, and Auditing, Kyiv, Ukraine
ORCID ID: 0009–0003–2787–8745
12zstzi@gmail.com

METHOD FOR STUDYING QUANTITATIVE INDICATORS OF CORPORATE NETWORK SECURITY SYSTEM

Abstract. A mathematical model of corporate network security has been developed and analyzed. The dependence of the security level on the information flow in the corporate network has been examined, along with the influence of parameters affecting the security system and its overall functionality. The relationship between network security, system size, and security threats has been established. A system of linear equations has been derived, reflecting the change in the security level as a function of the information flow rate and the impact of various security measures: data integrity and authenticity control, access restrictions, antivirus protection, firewall functionality, data backup, auditing, physical security measures, protection against unintended electromagnetic emissions, as well as the effects of possible hardware and software failures. The impact of the volume of personal data on its leakage, leakage rate, and the effectiveness of security mechanisms has been analyzed. As a result of solving the system of linear differential equations, mathematical and graphical dependencies of the corporate network security level on various factors have been obtained. By considering three possible solutions to the equation near the system's stationary state, it has been concluded that, depending on the ratio of dissipation and the natural frequency of oscillations, attenuation to a certain value occurs either periodically with a damped amplitude or following an exponentially decaying law. A more illustrative analysis of system behavior has been performed by transitioning from the differential form of the equations to a discrete form and simulating the system's evolution over a selected time interval. Mathematical and graphical dependencies of the system's natural oscillation frequency, damping coefficient, and oscillation period are presented. Simulation modeling with deviations from the stationary state has confirmed the nonlinear nature of the corporate network security system.

Keywords: security indicator; corporate network; flow; information; data; leakage; coefficient; system; equation.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Akhramovych, V. M., Batrak, I. H., Kolida, V. P., & Shvorak, K. V. (2021). Information Security Indicator of an Individual Computer. *Telecommunications and Information Technologies. DUT, 4(73),* 62–77.
2. Akhramovych, V., Pepa, Y., Zahynei, A., Akhramovych, V., Dzyuba, T., & Danylov, I. (2024). Method for Calculating the Information Security Indicator in Social Media with Consideration of the Path Duration Between Clients. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska – IAPGOS, 14(1),* 71–77. http://doi.org/10.35784/iapgos.5720.2024.03.31.
3. Akhramovych, V. M., Lazarenko, S. V., Nimchenko, T. V., & Ryabova, L. V. (2022). Method for Calculating Personal Data Protection Against Social Network Expansion. *Science-Intensive Technologies. K. NAU, 53(1),* 2–12.
4. Tkach, Yu. M., Yakovlev, O.O., & Lysytsia, T.A. (2021). Protection of Corporate Networks Against Human Influence Using Technical Means. *Informatics and Mathematical Methods in Simulation, 11(4),* 358–364.
5. Parkhomenko, I. I., Galkin V. V. (2020). Methods for Protecting Corporate Network Channels Based on VPN Solutions. *Modern Information Protection, 4,* 35–40.
6. Kostiuk, Yu.V. (2022). Problems of Corporate Information and Telecommunication Networks Protection. In *Modern Trends in the Development of Financial and Innovation-Investment Processes in Ukraine: Materials of the 5th International Scientific and Practical Conference,* 781–783.
7. Chernoshtan, A. M., & Vlasov, O. M. (2020). Methodology for Ensuring Corporate Network Security in Remote Management. *Scientific Notes of UNDI, 1(57),* 10–14.
8. Shkitov, A. A., & Kropyvnytskyi, D. R. (2021). Synthesis of Standard Information Security Algorithms in Corporate Networks. *Information Management Technologies, 2,* 129–135.

9. Chinchyk, D., Korobeinikova, T., & Zakharchenko, S. (2021). Methods and Means of Comprehensive Protection of Corporate Networks. *InterConf, (84),* 433–450. https://doi.org/10.51582/interconf.7-8.11.2021.043
10. Sachuk, Yu.V. (2018). *Information Security in Corporate Networks: Selective Academic Discipline Program for Bachelor's Training in the Field of Information Security, Specialty 125 Cybersecurity, Educational Program Information Security*. Lesya Ukrainka Eastern European National University, Department of National Security. https://evnuir.vnu.edu.ua/handle/123456789/15562.
11. Milyan, K. V., & Hrytsiuk, Yu. I. (2022). Features of Organizing Information Security in the Corporate Network of an Industrial Company. *Scientific Bulletin of NLTU of Ukraine, 23(4),* 311–327.
12. Kostiuk, Yu. V., & Voitkevych, A. A. (2024). Research on Technologies for Detecting and Identifying Violators for Corporate Network Protection. *Science and Technology Today, 4(23),* 1017–1032. https://doi.org/10.52058/2786-6025-2024-4(32)-1017-1032
13. Khoroshko, V. A., & Shoroshev V. V. (2019). Shortcomings of Traditional Corporate Network Security Measures in Intranet and the Necessity of Implementing New Protection Methods. *Information Protection,* 5–17.
14. Tyshyk, I. Ya. (2022). Testing an Organization's Corporate Network for Unauthorized Access. *Cybersecurity: Education, Science, Technology, 2(18),* 39–46.
15. Syrotynskyi, R. M., & Tyshyk, I. Ya. (2024). Improving Enterprise Network Infrastructure Security Under Modern Challenges and Limited Resources. *COMPUTER SYSTEMS AND NETWORKS, 6(1),* 155–164.
16. Chong Tian a Siqiu Hu. (2020). Mathematical modeling of the analysis of the impact on the security of the communication network based on the Monte Carlo algorithm. *Computer Communications, 157,* 20–27.
17. Romansky, R. (2023). Mathematical Model Investigation of a Technological Structure for Personal Data Protection, *Axioms, 12(2).* https://doi.org/10.3390/axioms12020102