УДК 004.056(075.8) DOI: 10.31673/2412-4338.2021.046277

Ахрамович В.М., Батрак І.Г., Коліда В.П., Шворак К.В.
Державний університет телекомунікацій, Київ

ПОКАЗНИК ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ОКРЕМОГО КОМП'ЮТЕРА

Анотація: *З розвитком цифрових та інформаційних технологій стали з'являтися електронні крадіжки, підробки документів і т. п. Зловмисники освоїли новий простір і завдають шкоди, крадучи дані не лише у комерційних організацій, наприклад, боровиковських систем, а й особисті файли пересічного користувача.*

Послуга захисту інформації на ПК вже стала популярною. Користувачі все більше починають усвідомлювати, як важлива технічна безпека даних, що зберігаються на електронних пристроях. Не всі користувачі можуть самі подбати про безпеку приватних файлів і самостійно налаштувати захист на ПК.

Тому стаття присв'ячена питанню кількісного визначення показника захищеності інформації на комп'ютері, в залежності від впливу на інформаційну структуру різних видів внутрішніх та зовнішніх загроз (відображає: ідентифікацію та автентифікацію користувачів, контроль цілісності та автентичності даних, резервне копіювання даних, розмежування доступу до інформації, роботу Firewall (пакетний фільтр), аудит, антивірусне забезпечення, збої та відмови компонент програмного та апаратного забезпечення, швидкості витоку інформації, вплив кількості інформації на їх витік, вплив загроз безпеки інформації від втрати довіри між користувачами, вплив розмірів системи комп'ютера на захищеність, вплив захищеності комп'ютера на витік інформації).

Для вирішення вказаних завдань 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.

Ключові слова: *показник захисту, комп'ютер, загрози, система диференціальних рівнянь, рішення з захисту.*

Akhramovych V., Batrak I., Kolida V., Shvorak K.
State University of Telecommunications, Kyiv

INFORMATION SECURITY INDEX OF AN INDIVIDUAL COMPUTER

Annotation: *With the development of digital and information technologies, electronic theft, forgery of documents, etc. began to appear. Criminals have mastered a new space and cause damage, stealing data not only from commercial organizations, for example, Borovikov systems, but also personal files of the average user.*

The service of protecting information on a PC has already become popular. Users are increasingly becoming aware of the importance of technical security of data stored on electronic devices. Not all users can take care of the security of private files and configure protection on their PC.

Therefore, the article is devoted to the issue of quantifying the information security indicator on a computer, depending on the impact on the information structure of various types of internal and external threats (reflects: identification and authentication of users, control of data integrity and authenticity, data backup, delimitation of access to information, Firewall operation (packet filter), audit, antivirus, failures of software and hardware components, speed of information leakage, the effect of the amount of information on their leakage, the effect of information security threats from the loss of trust between users, the effect of the size of the computer system on security, the impact of computer security on information leakage).

To solve the specified tasks, a mathematical model of information protection in a PC based on a system of differential equations was developed and solutions were simulated in the MatLab system. Three options for solving the equation near the steady state of the system were considered (a more visual analysis of the system's behavior was performed, with a transition from the differential form of the equations to a discrete one and modeling of a certain interval of the system's existence), it was concluded that, based on the conditions of the ratio of dissipation and the natural frequency of fluctuations of the magnitude, damping the latter up to a certain value is carried out periodically, with a decaying amplitude, or according to an exponentially decaying law.

Taking into account the impact of the specified parameters on information protection and the possibility of determining a quantitative indicator of protection, PC users will be able to independently assess the impact of each component of threats and make adequate protection decisions.

Keywords: *protection indicator, computer, threats, system of differential equations, protection solutions.*

Ахрамович В.М., Батрак И.Г., Колида В.П., Шворак К.В.
Государственный университет телекоммуникаций, Киев

ПОКАЗАТЕЛЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТДЕЛЬНОГО КОМПЬЮТЕРА

Аннотация: *С развитием цифровых и информационных технологий стали появляться электронные воровства, подделки документов и т.п. Злоумышленники освоили новое пространство и наносят вред, воруя данные не только у коммерческих организаций, например, боровиковских систем, но и личные файлы рядового пользователя.*

Услуга защиты информации на ПК уже стала популярной. Пользователи все больше начинают понимать, как важна техническая безопасность данных, хранящихся на электронных устройствах. Не все пользователи могут позаботиться о безопасности частных файлов и самостоятельно настроить защиту на ПК.

Поэтому статья посвящена вопросу количественного определения показателя защищенности информации на компьютере, в зависимости от влияния на информационную структуру различных видов внутренних и внешних угроз (отображает: идентификацию и аутентификацию пользователей, контроль целостности и подлинности данных, резервное копирование данных, разграничение доступа к информации, работу Firewall (пакетный фильтр), аудит, антивирусное обеспечение, сбои и отказ компонент программного и аппаратного обеспечения, скорости утечки информации, влияние количества информации на их утечку, влияние угроз безопасности информации от потери доверия между пользователями , влияние размеров системы компьютера на защищенность, влияние защищенности компьютера на утечку информации)

Для решения указанных задач разработана математическая модель защиты информации в ПК на основе системы дифференциальных уравнений и проведено моделирование решений в системе MatLab. Рассмотрены три варианта решения уравнения около стационарного состояния системы (выполнен более наглядный анализ поведения системы, с переходом от дифференциальной формы уравнений к дискретной и моделирования некоторого интервала существования системы), сделан вывод, что, исходя из условий соотношения диссипации и собственной частоты колебаний величины, затухание последней до определенного значения осуществляется периодически, с затухающей амплитудой, или по экспоненциально угасающему закону.

С учетом влияния указанных параметров на защиту информации и возможности определения количественного показателя защиты, пользователи ПК могут самостоятельно оценить влияние каждой составляющей угроз и принять адекватные решения по защите.

Ключевые слова: *показатель защиты, компьютер, угрозы, система дифференциальных уравнений, решения по защите*

1. Вступ. За допомогою комп'ютера ми спілкуємося з людьми, отримуємо потрібні відомості, ведемо ділове листування, зберігаємо фінансову та особисту інформацію – довіряємо комп'ютеру те, до чого хотілося б обмежити доступ. У той же час сьогодні тільки і говорять про вірусні епідемії, хакерські атаки, крадіжку особистих даних.

Захист інформації має значення у повсякденні, тим паче у персональних комп'ютерах.

Персональні комп'ютери (ПК) мають всі властивості ЕОМ інших класів, тому, взагалі кажучи, всі проблеми захисту інформації в побудованих на їх основі системах і підходи до захисту аналогічні. Однак персональним комп'ютерам притаманний ряд таких властивостей, які, з одного боку, сприяють захисту, а з іншого - ускладнюють її.

Більшість користувачів впевнена в тому, що розуміє проблеми захисту інформації в комп'ютері, може оцінити вплив різних типів загроз на захист і відповідно правильно налагодити систему захисту. Проте це можливо лише в тому випадку коли є наявна можливість реально оцінити кількісний вплив кожної окремої із загроз на систему захисту та їх комплексний вплив. Наведемо деякі відомі типи загроз.

Інтегральні схеми, на яких заснована робота комп'ютерів, створюють високочастотні зміни рівня напруги та струмів. Коливання поширюються проводами і можуть трансформуватися в доступну для розуміння форму, і перехоплюватися спеціальними пристроями. У комп'ютер або монітор можуть встановлюватись пристрої для перехоплення інформації, яка виводиться на монітор або вводиться з клавіатури. Перехоплення можливе і при передачі інформації по зовнішніх каналах зв'язку, наприклад, по телефонній лінії.

Щодня, і навіть можна сказати безперервно, наш комп'ютер піддається всебічним атакам, різноманітності яких можна тільки дивуватися, але що вражає - 99% користувачів-початківців при цьому впевнені, що встановлений в їх комп'ютері антивірус це панацея від всіх бід і всіх видів загроз.

А насправді, щоб убезпечити комп'ютер повністю, йому необхідний комплексний захист, тобто. захист з усіх можливих напрямів та від усіх можливих загроз.

Для оцінки кількісного показника захищеності інформації окремого комп'ютера від різного виду загроз і створена дана стаття.

Стаття містить теоретичний та практичний матеріал із забезпечення захисту інформації,

Вона дозволить користувачеві прийняти відповідні режими захисту.

2. Аналіз останніх досліджень і публікацій. В роботі [1] розроблені моделі довіри та репутації користувачів, що дозволяє зрозуміти вплив їх параметрів на захист.

В статті [2] показані моделі ідентифікація й аутентифікація, керування доступом, що дозволяє зрозуміти вплив вказаних факторів на захист.

В роботі [3] представлена , в тому числі, послідовність дій з захисту ПК за допомогою програмного забезпечення (операційних систем, спеціального ПЗ, і т.п.) Захисту від несакціонованого доступу, вірусів, шкідливого ПЗ, створення резервних копій, методи комплексного захисту і т.п.).

В роботі [4] наведено кілька математичних принцип аналізу мережевих атак при використанні теорії ігор рівноваги Неша. Проаналізовано проникнення через випадкові процеси з дискретним часом. Використані приклади теорії ігор та дослідження операцій, які адаптовані до кібератак.

В роботі [5] була розроблена математична модель комп'ютерних вірусів, що заражають систему за різних умов. Математична модель 1 обговорює ситуацію для визначення ймовірності того, що в будь-який час t скільки компонентів програмного забезпечення заражено вірусом, припускаючи, що швидкість одужання та частка неінфікованої популяції, яка отримує інфекцію за одиницю часу, не змінюються з часом. Математична модель 2 призначена для оцінки частки зараженої популяції компонентів програмного забезпечення в будь-який час і в будь-який невизначений час у різних випадках.

В статті [6] представлено обговорення геометричної моделі, яка, є корисною для виконання багатьох дій, що використовуються в традиційному виявленні вторгнень, в комп'ютери, включаючи корисну візуалізацію.

В роботі [7] показано набір математичних моделей. Перший набір математичних моделей використовується для визначення умов, за яких можна довести, що типи систем безпечні. Матрична модель контролю доступу представляє загальний опис комп'ютерної системи, яку використовує цей тип моделі. Другий тип моделі описує, як комп'ютерна система застосовує елементи керування. Модель контролю доступу, керованого користувачем,

прив'язує контроль над даними до користувача, а не до власника, і має програми для систем керування цифровими правами. Модель керування доступом на основі ролей використовує службову функцію, а не ідентичність, щоб забезпечити елементи керування, і тому може реалізувати принцип найменших привілеїв.

В роботі [8] наведено процес математичного моделювання та принцип моделювання системи кіберзахисту. Оскільки атаки на комп'ютер є повністю стохастичними, модель розробки системи кіберзахисту базується на виявленні поведінка шкідливих об'єктів за допомогою функції розподілу ймовірностей і диференціальних рівнянь.

В статтях [9,10] представлено процесний алгебраїчний підхід до моделювання властивостей і політик безпеки. Використовується поняття секретності, також відомого як конфіденційність, і зокрема на невтручанні

В статті [11] розроблено математичну модель процесу тестування для проникнення в комп'ютерні системи. Запропонована модель відрізняється від відомих комп'ютерних систем спеціалізованих інформаційних платформ можливостями тестування безпеки, які дозволили оцінити час виконання алгоритму тесту на проникнення, що потрапляє в заданий інтервал ймовірності.

В статті [12] розглядається нова модель SIQR для розповсюдження вірусу Інтернет-хробака. Використовуючи теорію диференціальних рівнянь, проаналізовано динамічну властивість моделі та отримано закономірність розповсюдження вірусу Інтернет-хробака.

3. Ціль дослідження. Метою дослідження є створення математичної моделі кількісної оцінки впливу загроз на показник захисту інформації на ПК.

4. Результати дослідження. Позначимо кількість інформації в системі комп'ютера – I. Потік інформації за межі комп'ютера через *dI*–, швидкість зміни цього потоку – $\frac{dI}{dt}$. Якщо потік і швидкість зміни потоку дорівнюють нулю, то витоку інформації немає:

$$dI = 0; \frac{dI}{dt} = 0 \tag{1}$$

Від чого може залежати витік інформації? Перш за все від захищеності системи комп'ютера – вжитих заходів з нейтралізації загроз безпеки інформації. Z – показник захищеності інформаційної системи комп'ютера. Складемо рівняння:

$$\begin{cases} \frac{dI}{dt} = \text{IdA+((Q+R+W+F+Ad+V)ZpZk)} + (C_v + C_k)I \end{cases} \tag{2}$$

де: I_d -коефіцієнт, що відображає ідентифікацію користувачів (значення 0 або 1); A - коефіцієнт, що відображає автентифікацію користувачів(значення 0 або 1); Q- коефіцієнт, що відображає контроль цілісності та автентичності даних (0,1); R- коефіцієнт, що відображає резервне копіювання даних (0,1); W- коефіцієнт, що відображає розмежування доступу до інформації (0,1); F- коефіцієнт, що відображає роботу Firewall (пакетний фільтр) – використовується для контролю вхідного та вихідного трафіку (0,1); A_d - коефіцієнт, що відображає аудит (використовується для спостереження, протоколювання) (0,1);. V-коефіцієнт, що відображає антивірусне забезпечення (0,1) Z_p - коефіцієнт, що відображає збої та відмови компонент програмного забезпечення (0,1); Z_k - коефіцієнт, що відображає збої та відмови компонент апаратного забезпечення(0,1);

Причому I_d, A, Q, R, W, F, A_d - це в сутності захист комп'ютера засобами операційної системи.

Cv – коефіцієнт, що відображає вплив швидкості витоку інформації; C_k – коефіцієнт, що відображає вплив кількості інформації на їх витік.

Інтерпретувати дане рівняння можна наступним чином. Витік інформації залежить:

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

– від швидкості витоку інформації;

– витік інформації купірується захищенністю системи щодо нейтралізації загроз безпеки інформації.

Пояснимо інші складові рівняння.

Ідентифікація – один к компонентів найбільш поширеного способу доступу до інформації – реєстрації. Суть ідентифікації полягає, в тому що у кожному користувачеві при реєстрації, присвоюється унікальний ідентифікатор. За цим ідентифікатором можливо визначити ідентичність користувача.

Автентифікація – використовується для підтвердження доступу до інформації, що прив'язана або надається за унікальним ідентифікатором. Зазвичай автентифікація відбувається способом надання:

− Унікального предмету або атрибуту (електронний ключ, старт-карта, криптографічний сертифікат тощо);

− Паролю (найбільш розповсюджений вид автентифікації); − Біометричних даних (голос, відбитки пальців, підпис, форма долоні тощо).

Контроль цілісності та автентичності даних – використовується для контролю важливих складових системи (наприклад: системних файлів) на пошкодження, або спотворення. Необхідний механізм для виявлення порушень та забезпечення стабільної роботи системи.

Резервне копіювання – виконується для забезпечення можливості відновлення оригіналу інформації або важливих компонент системи на випадок спотворення або пошкодження.

Розмежування доступу до інформації – виконується шляхом обов'язкової авторизації користувачем в системі. Використовується для надання авторизованому користувачу доступу і прав на користування інформацією та функціями системи, встановлених адміністратором системи.

Шифрування – використовується для шифрування важливої інформації на носії. Для зашифровки використовується криптографія. Система активує односторонню функцію, яку не важко обчислити, але дуже важко підібрати зворотну ді.;

Firewall (пакетний фільтр) – використовується для контролю вхідного та вихідного трафіку. Забезпечує контроль за заданими правилами.

Аудит – використовується для спостереження. Система веде протоколювання: − дій користувачів системи (авторизація, використання системних функцій); − помилки та повідомлення системи; − помилки та повідомлення програмного забезпечення; − помилки та повідомлення центру безпеки.

Далі розглянемо, від чого залежить захищеність системи комп'ютера – Z. Визначимо захищеність системи як здатність системи протистояти несанкціонованому доступу до конфіденційної інформації. Отже, захищеність системи комп'ютера буде залежати:

– від розмірів системи (як і від кількості інформації);

– загроз безпеки інформації від втрати довіри між користувачами даного комп'ютера.

Складемо рівняння:

$$\frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) \tag{3}$$

де: D_i – коефіцієнт, що відображає вплив загроз безпеки інформації від втрати довіри між користувачами на захищеність комп'ютера, в тому випадку коли користувачами даного комп'ютера є два і більше користувачі; C_{d2} – коефіцієнт, що відображає вплив розмірів

системи комп'ютера на захищеність; C_{d1} – коефіцієнт, що відображає вплив захищеності комп'ютера на витік інформації.

Об'єднаємо рівняння (2) і (3) в систему:

$$\begin{cases} \dfrac{dI}{dt} = \text{IdA+((Q+R+W+F+Ad+V)ZpZk)} + (C_v + C_k)I \\ \dfrac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) \end{cases} \tag{4}$$

Знайдемо стаціонарну позицію системи комп'ютера, що описується рівняннями (5). Умови стаціонарності $dI = 0; \dfrac{dI}{dt} = 0$. Отже:

$$\begin{cases} \text{IdA+((Q+R+W+F+Ad+V)ZpZk)} + (C_v + C_k)I = 0 \\ D_i - I(C_{d2} + C_{d1}) = 0 \end{cases} \tag{5}$$

З другого рівняння системи слідує:

$$\bar{I} = \frac{D_i}{(C_{d2} + C_{d1})} \tag{6}$$

Далі з першого рівняння системи рівнянь (4) з врахуванням (6) знаходимо:

$$\text{Id1} * \text{A1+((Q+R+W+F+Ad+V)} * \text{Zp} * \text{Zk}) - \frac{(C_v + C_K)D_i}{(C_{d2} + C_{d1})} = 0 \tag{7}$$

Позначимо показник захисту інформації комп'ютера:

$$\bar{Z} = \text{IdA+((Q+R+W+F+Ad+V)ZpZk)} \tag{8}$$

Результати обрахунку за залежністю (8) представлені на рис. 1.

Аналіз графічних залежностей на рис. 1 показує нелінійні та нелінійні залежності захисту систем комп'ютера від параметрів захисту. Як бачимо з графіку при зростанні – значень параметрів коефіцієнт захисту інформації збільшується, що підтверджує вірогідність одержаних результатів.

Тоді можна записати:

$$\bar{Z} = \frac{(C_v + C_K)D_i}{(C_{d2} + C_{d1})} = 0 \tag{9}$$

Отже, умови позиції стаціонарності системи:

$$\begin{cases} \bar{I} = \dfrac{D_i}{C_{d2} + C_{d1}} \\ \bar{Z} = \dfrac{(C_v + C_K)D_i}{(C_{d2} + C_{d1})} \end{cases} \tag{10}$$

Вирішимо систему рівнянь (4) методом «малих відхилень» $I = \bar{I} + I; Z = \bar{Z} + Z$:, отже, система рівнянь прийме вигляд:

$$\begin{cases} \dfrac{dI}{dt} = (\bar{Z} + Z) + (C_v + C_K)(\bar{I} + I) \\ \dfrac{dZ}{dt} = D_i - (\bar{I} + I)(C_{d2} + C_{d1}) \end{cases} \quad (11)$$

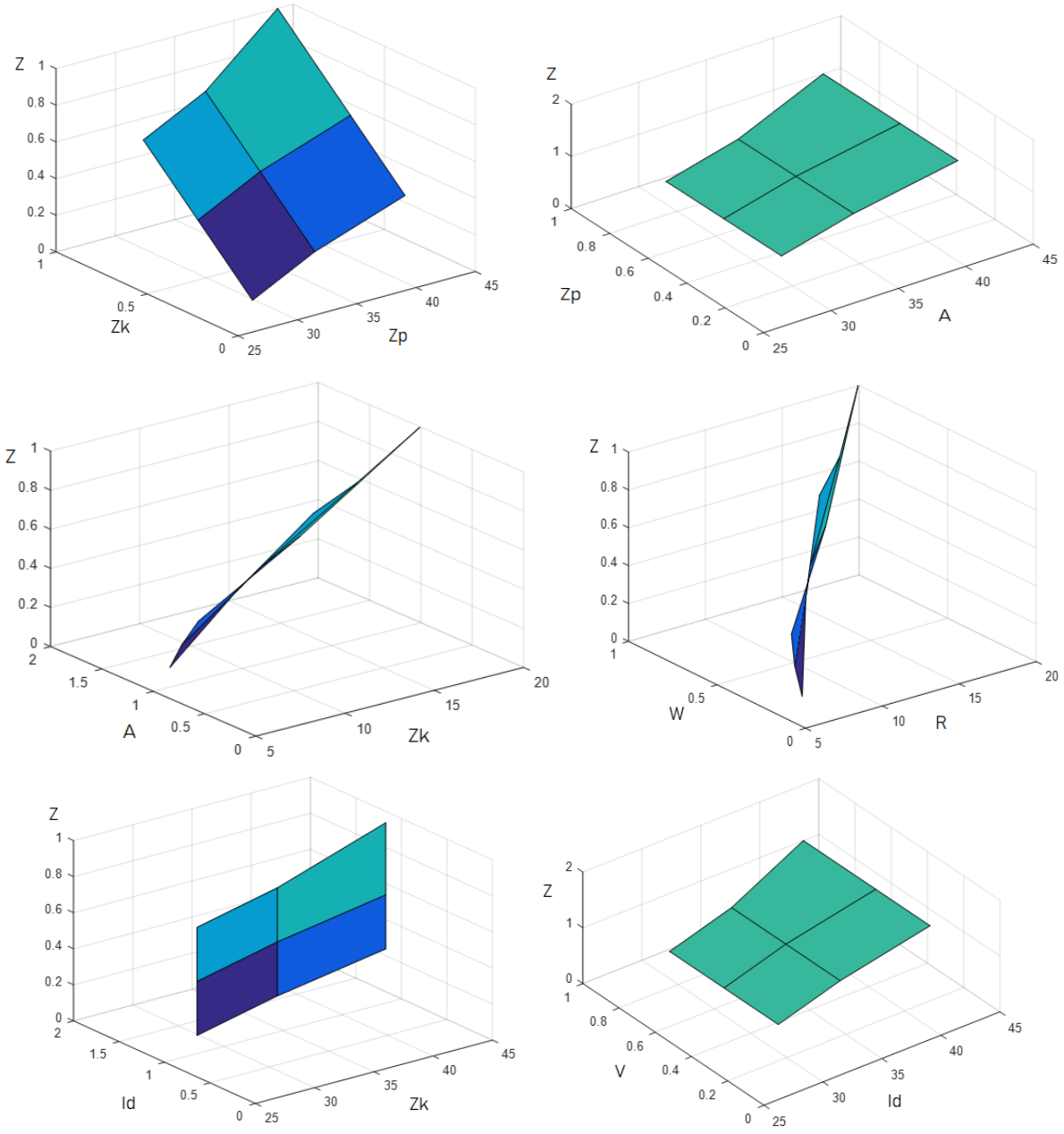

Рис. 1. Залежність захисту комп'ютера від різних складових за залежністю (8)

Рішення представимо у вигляді графіка рис.2. При лінійній залежності коефіцієнтів параметрів соціальної мережі, ця залежність практично лінійна:

$$\begin{cases} \dfrac{dI}{dt} = (C_{d1} + C_{d2})Z - (C_v + C_K)I \\ \dfrac{dZ}{dt} = -I(C_{d2} + C_k) + D_i) \end{cases} \quad (12)$$

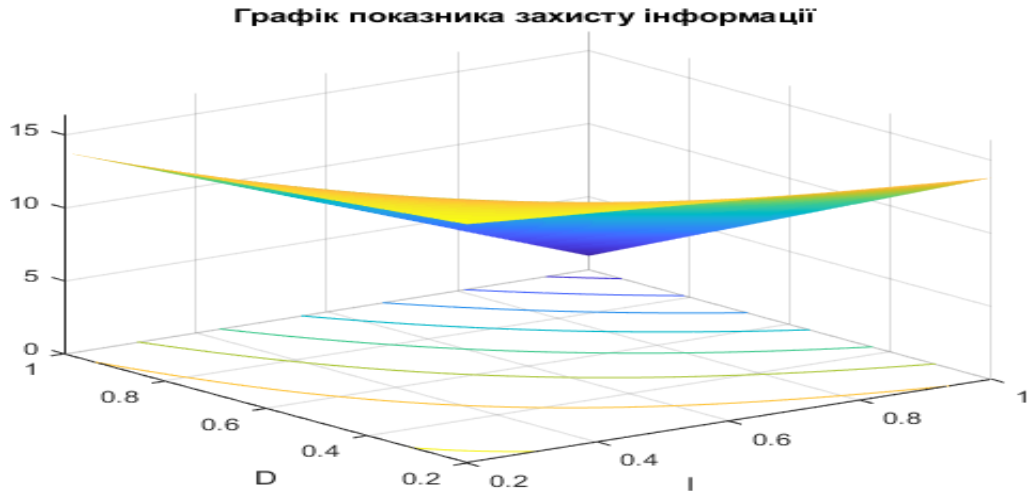

Рис. 2. Результати обрахунку за системою рівнянь (11)

Диференціюючи перше рівняння системи (12) отримуємо:

$$\frac{d^2I}{dt^2} = -ID_i(C_{d1} + C_{d2}) - (C_v + C_K)\frac{dI}{dt}, \tag{13}$$

$$\frac{d^2I}{dt^2} + (C_v + C_K)\frac{dI}{dt} + (C_{d1} + C_{d2})D_iI = 0. \tag{14}$$

Результати обрахунку за системою рівнянь (14), показані на рис. 3. Як бачимо з графіку при зростанні коефіцієнту, що відображає вплив кількості інформації на їх витік, довіра до інформації зменшується, що підтверджує вірогідність одержаних результатів. При лінійній залежності коефіцієнтів параметрів захисту комп'ютера, ця залежність теж практично лінійна.

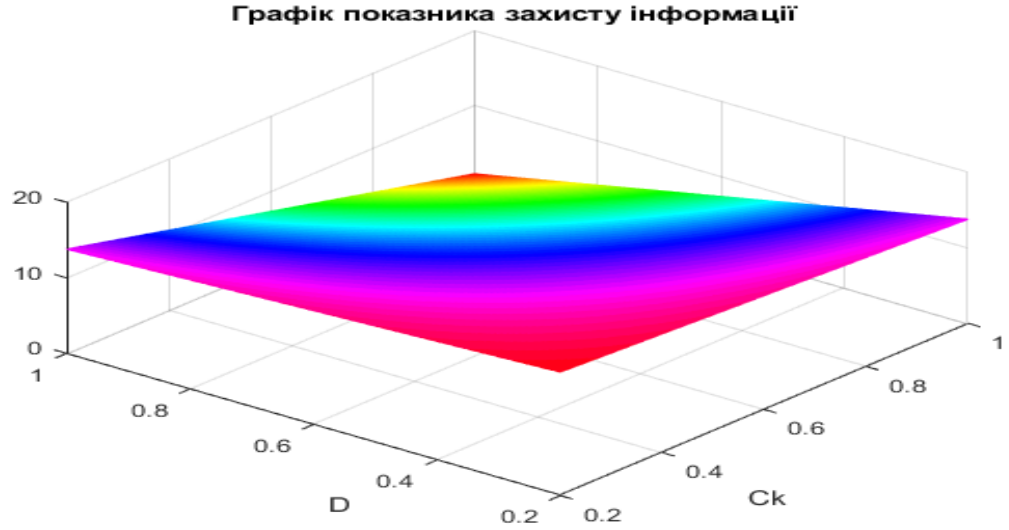

Рис. 3. Графік залежності коефіцієнта захисту інформації від коефіцієнту, впливу кількості інформації на їх витік за системою рівнянь (12)

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

$$\omega_0 = \sqrt{(C_{d1} + C_{d2})D_i} \tag{15}$$

Як бачимо з графіку (рис. 4), при зростанні коефіцієнту, що відображає довіру до інформації, коефіцієнт захисту інформації збільшується, що підтверджує вірогідність одержаних результатів.

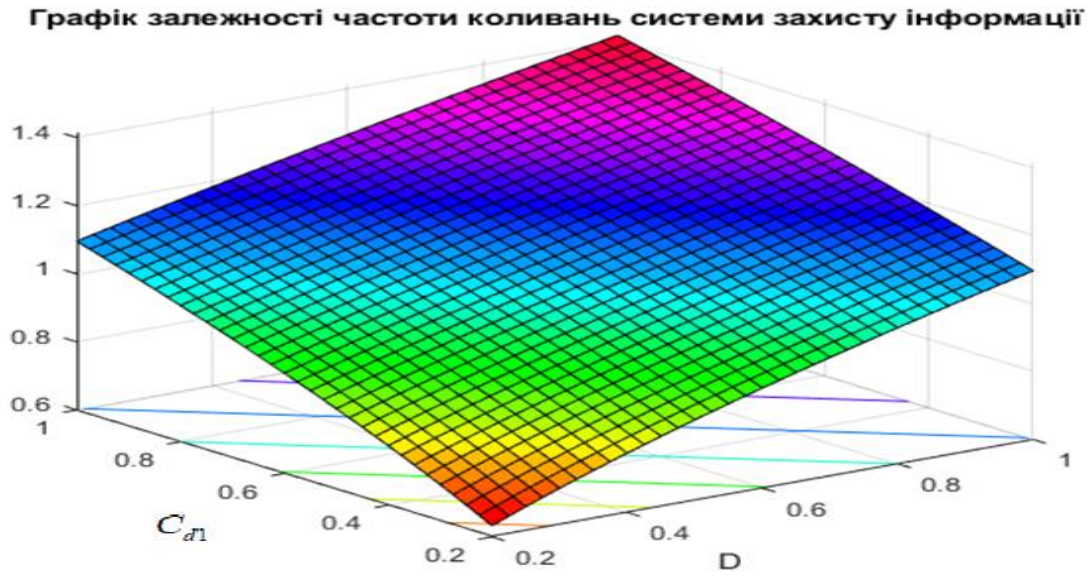

Рис. 4. Графік залежності коефіцієнта довіри від коефіцієнту захисту інформації для випадку (15)

Результати обрахунку за рівнянням (16), показані на рис. 5:

$$\omega = \sqrt{(C_{d1} + C_{d2})D_i - \frac{(C_v + C_K)^2}{4}} \tag{16}$$

Як бачимо з графіку при зростанні коефіцієнту, що зображає довіру до інформації, коефіцієнт захисту інформації збільшується, але у цьому випадку коефіцієнт захисту збільшується повільніше. Це пояснюється зменшенням коефіцієнтів взаємовпливу та кореляції параметрів захисту інформації.

Графік рис.5. відрізняється від рис. 4. тільки значенням амплітуди функції, це правдивий результат тому, що період коливань та частота коливань мають подібну функціональну залежність. Отримані результати підтверджують вірогідність одержаних результатів.

Результати обрахунку за рівнянням (17), показані на рис. 6. Як бачимо з графіку при зростанні коефіцієнту, що зображає довіру до інформації, коефіцієнт захисту інформації збільшується. Період коливань збільшується при збільшуваних зовнішніх впливів. Отримані результати підтверджують вірогідність одержаних результатів.

$$T = \frac{2\pi}{\sqrt{(C_{d1} + C_{d2})D_i - \frac{(C_v + C_K)^2}{4}}} \tag{17}$$

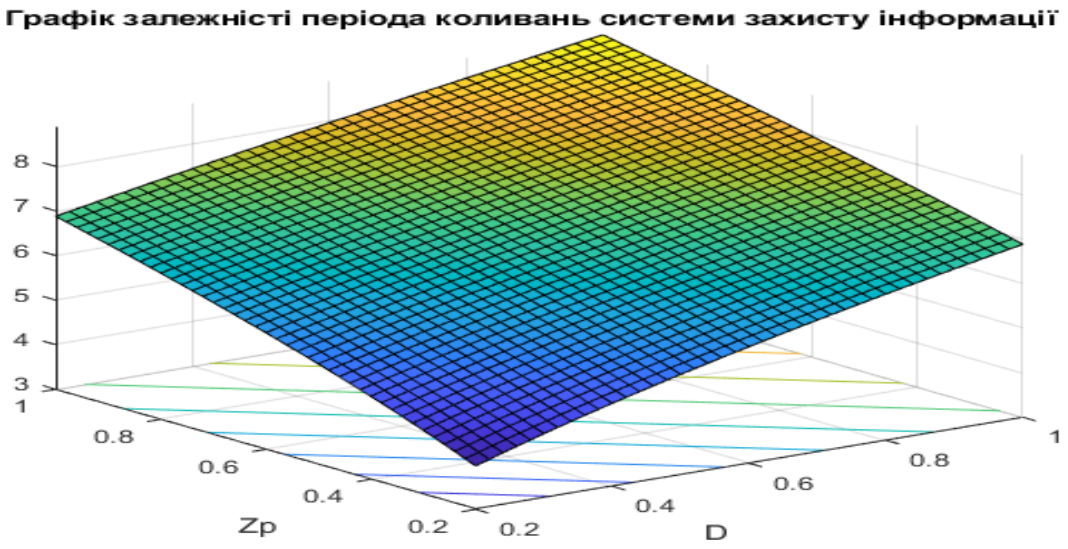

Рис. 5. Графік залежності коефіцієнта довіри від коефіцієнту захисту інформації для випадку (16)

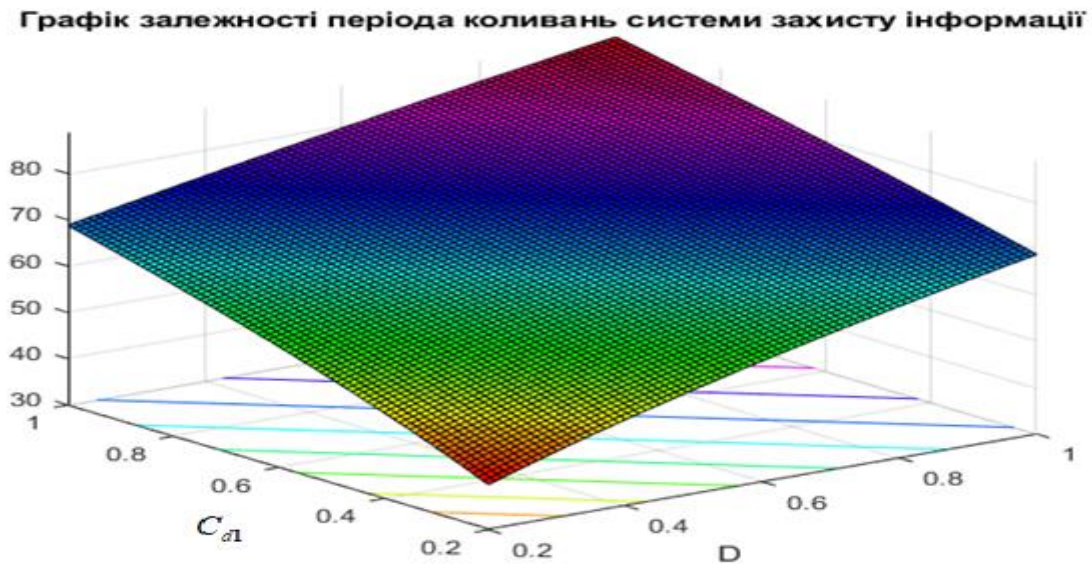

Рис. 6. Графік залежності періоду коливань від коефіцієнта довіри та коефіцієнту захисту інформації для випадку (17)

Коефіцієнт затухання визначається залежністю (18):

$$\beta = \frac{(C_V + C_K)}{2} \tag{18}$$

Результати графічного моделювання за залежністю (18) наведено на рис.7.

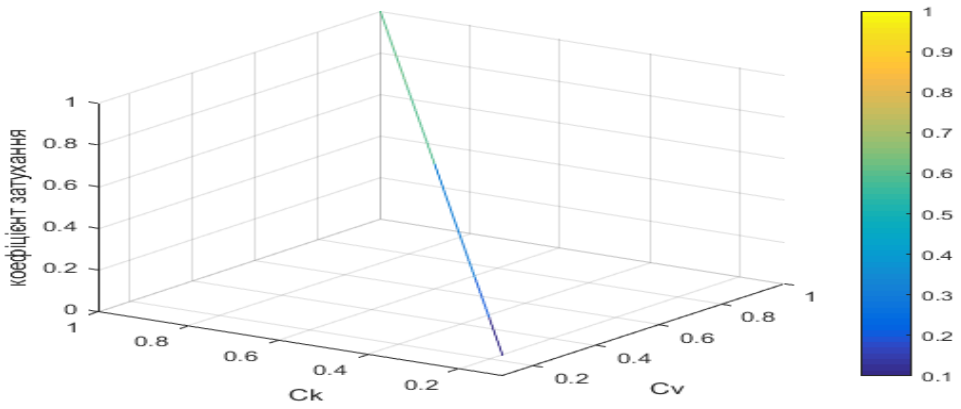

Рис. 7. Результати обрахунку за рівнянням (18)

Рішення рівняння гармонічного осцилятора розпадається на три випадки (19), (20), (21):

$$\beta \prec \omega_0 : I = A_0 \exp(-\frac{(C_v + C_K)}{2} \times \times \cos(\sqrt{(C_{d1} + C_{d2} + D_i) - \frac{(C_v + C_K)^2}{4}} t + \varphi_0) \quad (19)$$

$$\beta = \omega_0 : I = (A_0 + B_0 t \exp(-\frac{(C_v + C_K}{2} t) \quad (20)$$

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

де

$$y_{12} = \beta \pm \sqrt{\frac{(C_v + C_K)^2}{4} - (C_{d1} + C_{d2} + D_i)} \quad (21)$$

Результати графічного моделювання за залежностями (19), (20), (21) наведено на рис.8, 9, 10.

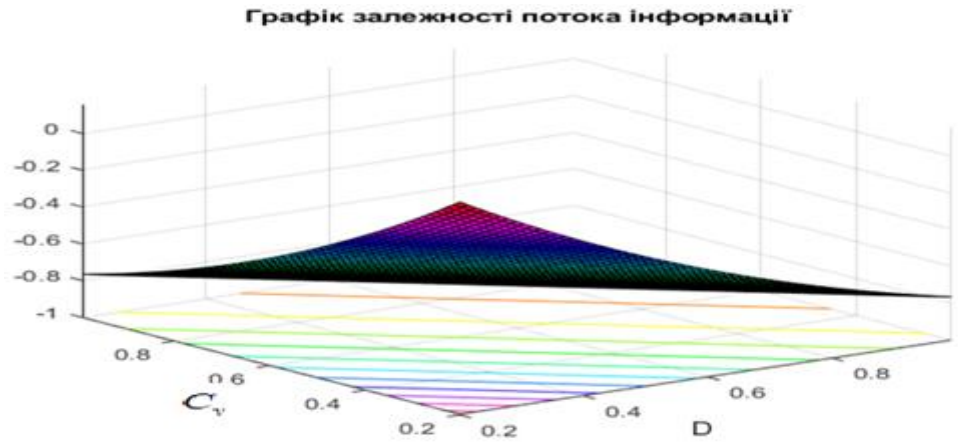

Рис. 8. Залежність потоку інформації при умові (19)

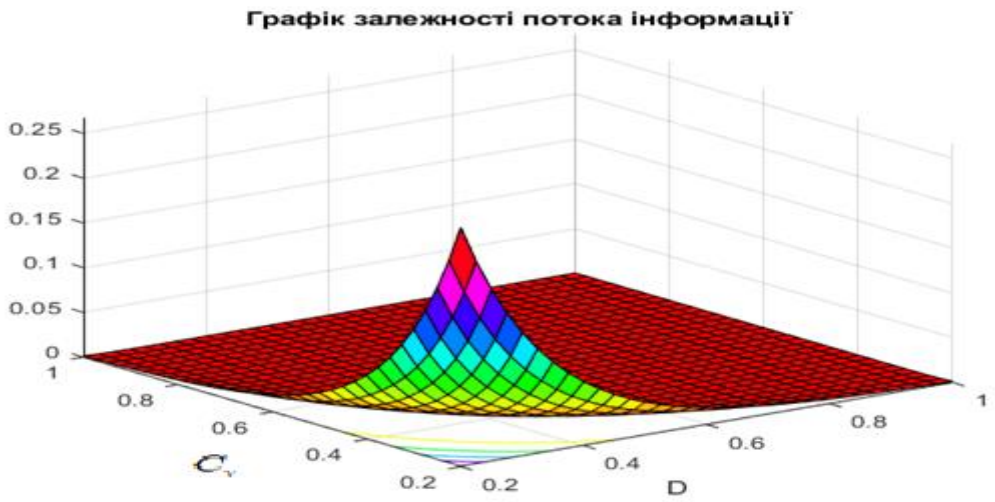

Рис. 9. Залежність потоку інформації при умові (20)

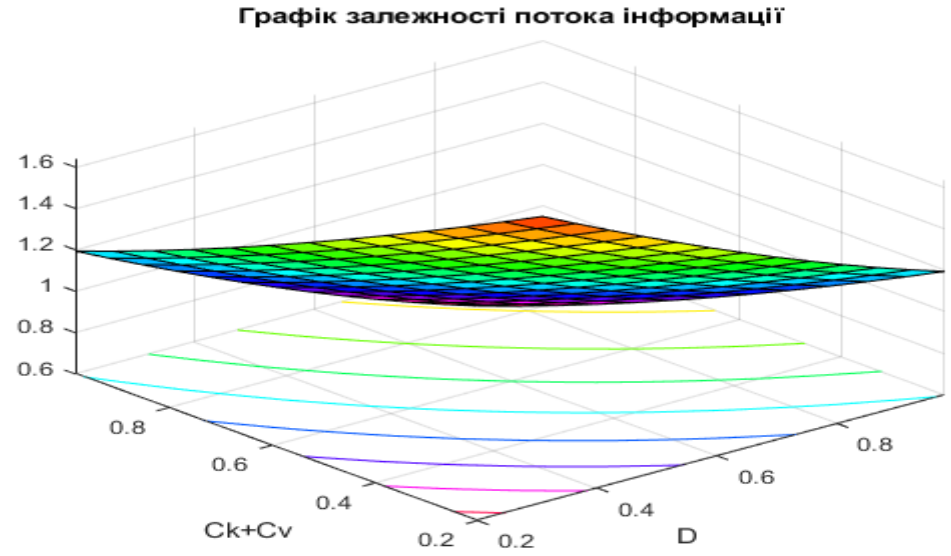

Рис. 10. Залежність потоку інформації при умові (21)

Розглянувши три варіанти вирішення рівняння близько стаціонарної 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 затухаючою амплітудою, або за експоненціально загасаючим законом. Виконаємо більш наочний аналіз поведінки системи, перейшовши від диференціальної форми рівнянь (15), (16) та (17) до дискретної і промоделювавши деякий інтервал існування системи. А саме:

$$\begin{cases} \dfrac{I_{n+1}-I_n}{\Delta t} = (C_{d1}+C_{d2})Z_n - (C_v + C_K)I_n) \\ \dfrac{Z_{n+1}-Z_n}{\Delta t} = Z_p - (C_{d2}+C_{d1})I_n - (Z_p + D_i)I_n) \end{cases} \quad (22)$$

$$\begin{cases} I_{n+1} = I_n + (C_{d1} + C_{d2})Z_n - (C_v + C_K)I_n)\Delta t \\ Z_{n+1} = Z_n + (Z_n - I_n(C_{d2} + C_{d1} + Z_p + D_i))\Delta t \end{cases} \quad (23)$$

Спочатку приймемо коефіцієнти $C_{d1}, C_v, C_{d2}, D_i, C_K$ за одиницю. Слідуючи з умови стаціонарної позиції системи, I і Z будуть рівні 0.5 і 0.5. Крок моделювання приймемо за 0.1 для всіх ітерацій моделювання, тому в таблиці відображати його не будемо. Величини I_{sp}, Z_{sp} відображають стаціонарні значення параметрів, якщо такі були досягнуті за кінцеве число ітерацій. Далі проведемо імітаційне моделювання для значень $\beta \prec \omega_0, \beta = \omega_0, \beta \succ \omega_0$ з відхиленням від стаціонарної позиції системи. Інформацію представимо в табл. 1 .

Таблиця 1

Параметри моделювання

№ з/п	I	Z	C_v	C_{d1}	D_i	C_{d2}	C_K	Параметри
1	0,5	1	0,5	1	1	1	0,5	$\beta \prec \omega_0$
2	0,5	1	2	1	1	1	2	$\beta = \omega_0$
3	0,5	1	4	1	1	1	5	$\beta \succ \omega_0$

Візуалізація результатів.

З аналізу рис. 11. можемо зробити висновок про те, що коефіцієнт захисту інформації має згасний характер. Перехідний процес згасний, що свідчить про стійкість системи захисту інформації при зовнішніх впливах.

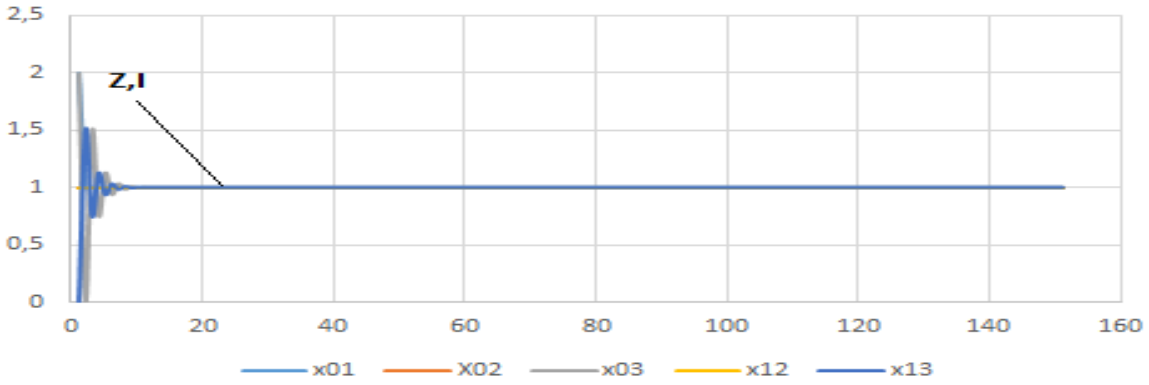

Рис. 11. Залежність інтенсивності та захисту інформації від кількості ітерацій (140). Інформація складових взяті з табл. 1. $\beta \prec \omega_0$, через і позначено кількість ітерацій

Аналіз рис. 12 та 13, графіків залежності інтенсивності та захисту інформації від коефіцієнта ітерацій. Дозволяє зробити висновок, що при стійкої системи захисту інформації кількість ітерацій не приводить до злому системи захисту інформації. Але моделювання проводилось при припущені, що ітерації стабільні та однотипні за амплітудою. Моделювання при зовнішніх впливах різній інтенсивності та нерівномірного розповсюдження в часі не розглядається.

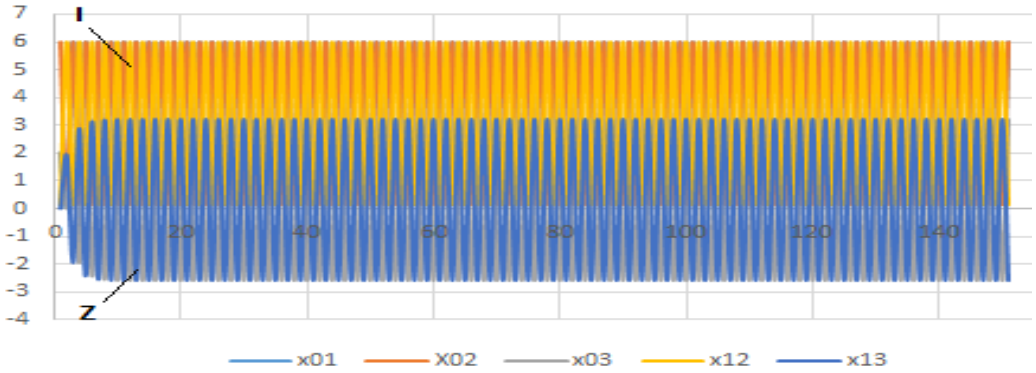

Рис. 12. Залежність інтенсивності та захисту інформації від кількості ітерацій (140). $\beta = \omega_0$, Di=0,5

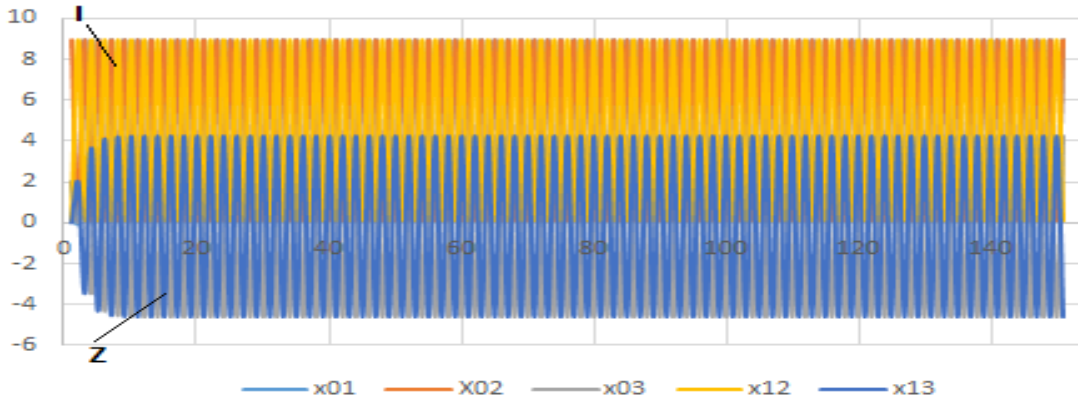

Рис 13.Залежність інтенсивності та захисту інформації від кількості ітерацій (140). $\beta \succ \omega_0$, Di=0,1

5. Обговорення результатів проведеного дослідження.

Проведене дослідження дозволяє отримати кількісні показники захисту інформації від кількісного визначення показника захищеності інформації на комп'ютері, в залежності від впливу на інформаційну структуру різних видів внутрішніх та зовнішніх загроз (ідентифікації та автентифікації користувачів, контролюь цілісності та автентичності даних, резервного копіювання даних, розмежування доступу до інформації, роботи Firewall (пакетний фільтр), аудиту, антивірусного забезпечення, збові та відмов компонент програмного та апаратного забезпечення, швидкості витоку інформації, впливу кількості інформації на їх витік, впливу загроз безпеці інформації від втрати довіри між користувачами, впливу розмірів системи комп'ютера на захищеність, вплив захищеності комп'ютера на витік інформації).

Внаслідок аналізу трьох варіантів вирішення рівняння близько стаціонарної стану системи, отмали висновк, 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.

Аналіз графіків залежності інтенсивності та захисту інформації від коефіцієнта ітерацій, дозволяє зробити висновок, що при стійкої системи захисту інформації кількість ітерацій не приводить до злому системи захисту інформації. Але моделювання проводилось при припущені, що ітерації стабільні та однотипні за амплітудою. Моделювання при зовнішніх впливах різній інтенсивності та нерівномірного розповсюдження в часі не розглядається.

6. Висновки. Дослідження математичної моделі оцінки кількісного показника захищеності інформації окремого комп'ютера (системи диференціальних рівнянь), дозволило отримати математичні залежності між можливими загрозами та показником захисту. В результаті дослідження отримані рівняння гармонічного осцилятора з затухаючою

амплітудою. Це дозволило визначити частоти коливань, період, коефіцієнт затухання системи захисту. Отримано математичні залежності поведінки системи захисту в дорезонансній, резонансній та післярезонансній областях. Такий підхід дозволив перейти до дослідження лінійності системи захисту.

Перевірка на лінійність системи захисту інформації вказала на її нелінійність. Це доведено шляхом розгляду трьох варіантів розв'язку рівняння осцилятора близько стаціонарного стану системи. Це дозволило зауважити, що виходячи з умов співвідношення дисипації і власної частоти коливань величини, затухання останньої, до певного значення, здійснюється періодично. Амплітуда коливань є затухаючою амплітудою за експоненціально загасаючим законом. Виконано більш наочний аналіз поведінки системи, шляхом переходу від диференціальної форми рівнянь до дискретної і моделювання деякого інтервалу існування системи. В результаті аналізу ітерації коливань системи захисту виявлено її нелінійність. Це дозволить в майбутньому перейти до дослідження нелінійної системи захисту.

Список використаної літератури

1. Ахрамович В.М.. Моделі довіри та репутації користувачів в соціальних мережах / Сучасний захист інформації. К. ДУТ:-2019 .-№4 - с. 45-51.

2. Ахрамович. В.М. Ідентифікація й аутентифікація, керування доступом. Сучасний захист інформації. К. ДУТ:-2016 .-№4.- с. 47-51

3. Ахрамович В.М., Чегренець В.М. Інформаційна безпека. Практикум/ В.М. Ахрамович, В.М. Чегренець.-К.: ДУТ, 2017.-396с.

4. Alexey Stefanov , Iliyan Ivanov , Ivan Trenchev , Radoslav Stoev , Miglena Trencheva. Usage of Mathematical Models for Cybersecurity Analysis. https://conference.pixel-online.net/FOE/files/foe/ed0010/FP/6778-HED4764-FP-FOE10.pdf.

5. Bimal Kumar Mishra, Dinesh Saini. Applied Mathematics and ComputationVolume. 187Issue VOL. 3 NO. 2. 2April, 2007. pp. 929–936. https://doi.org/10.1016/j.amc.2006.09.062.

6. Greg Vert Deborah A. Frincke Jesse C. McConnell. A. Visual Mathematical Model for Intrusion Detection. https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/paperf3.pdf.

7. Matt Bishop. Mathematical Models of Computer Security. https://onlinelibrary.wiley.com.

8. T. Gencoglu. Muharrem Tuncay GENÇOĞLU. Mathematical Modeling in Cyber Defense. International journal of engineering science and application m., Vol.4, No.4, December 2020. pp. 124-131.

9. P. Ryan. Mathematical Models of Computer Security. Published in FOSAD. 1 September 2000 Computer Science. https://www.semanticscholar.org/paper/Mathematical-Models-of-Computer-Security-Ryan/ff368bc3521ec4b8ceaa42fe02f8da0f017b601c.

10. Peter Y. A. Ryan. Mathematical Models of Computer Security. https://link.springer.com/content/pdf/10.1007/3-540-45608-2_1.pdf

11. Serhii Semenov, Cao Weilin. Ttesting process for penetration into computer systems mathematical model modification. Advanced information systems VOL. 4 NO. 3 (2020). pp. 34-45.

12. Shao-Jie Wang, Chen Liang and Qi-Ming LIU. Analysis of a mathematical model for worm virus propagation. Computer and Network Technology, VOL. 2 NO. 1 (2009). pp. 3-6

References

1. Akhramovych V. Models of user trust and reputation in social networks / Modern information protection. K. SUT:-2019 .-№4 - p. 45-51.

2. Akhramovych V. Identification and authentication, access control. Modern information protection. K. SUT:-2016 .-№4.- p. 47-51

3. Akhramovych V. Chehrenets V. Informational security. Workshop/ V. Akhramovych, V. Chehrenets. - K. SUT, 2017.-396p.

4. Alexey Stefanov , Iliyan Ivanov , Ivan Trenchev , Radoslav Stoev , Miglena Trencheva. Usage of Mathematical Models for Cybersecurity Analysis. https://conference.pixel-online.net/FOE/files/foe/ed0010/FP/6778-HED4764-FP-FOE10.pdf.

5. Bimal Kumar Mishra, Dinesh Saini. Applied Mathematics and ComputationVolume. 187Issue VOL. 3 NO. 2. 2April, 2007. pp. 929–936. https://doi.org/10.1016/j.amc.2006.09.062.

6. Greg Vert Deborah A. Frincke Jesse C. McConnell. A. Visual Mathematical Model for Intrusion Detection. https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/paperf3.pdf.

7. Matt Bishop. Mathematical Models of Computer Security. https://onlinelibrary.wiley.com.

8. T. Gencoglu. Muharrem Tuncay GENÇOĞLU. Mathematical Modeling in Cyber Defense. International journal of engineering science and application m., Vol.4, No.4, December 2020. pp. 124-131.

9. P. Ryan. Mathematical Models of Computer Security. Published in FOSAD. 1 September 2000 Computer Science. https://www.semanticscholar.org/paper/Mathematical-Models-of-Computer-Security-Ryan/ff368bc3521ec4b8ceaa42fe02f8da0f017b601c.

10. Peter Y. A. Ryan. Mathematical Models of Computer Security. https://link.springer.com/content/pdf/10.1007/3-540-45608-2_1.pdf

11. Serhii Semenov, Cao Weilin. Ttesting process for penetration into computer systems mathematical model modification. Advanced information systems VOL. 4 NO. 3 (2020). pp. 34-45.

12. Shao-Jie Wang, Chen Liang and Qi-Ming LIU. Analysis of a mathematical model for worm virus propagation. Computer and Network Technology, VOL. 2 NO. 1 (2009). pp. 3-6