УДК 004.056:519.6

М.В. КРИХІВСЬКИЙ, В.В. БАНДУРА, Т.О. ВАВРИК
Івано-Франківський національний технічний університет нафти і газу

МАТЕМАТИЧНІ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Широке проникнення математичних методів у розроблення інформаційних технологій характеризує сучасний етап нашого суспільства. Статтю присвячено проблемі застосування математичних моделей із нечіткістю та носить оглядовий характер. Порівняно ефективність різних математичних підходів до виявлення та запобігання кіберзагрозам. Серед математичних методів, що застосовують в інформаційній та кібернетичній безпеці, велику нішу займають моделі розмежування прав доступу в інформаційних системах. Цим і обґрунтовано вибір та актуальність даного дослідження. Розглянуто поєднання кластерної технології як математичної моделі найрізноманітніших об'єктів, явищ і зв'язків між ними з популярними сьогодні математичними моделями розмежування прав. У статті викладено основні елементи популярних математичних моделей для розмежування прав доступу в інформаційних системах. Аналіз наукових праць дав змогу визначити основні напрями застосування властивостей, характеристик нечітких множин та нечітких алгоритмів в інформаційній та кібернетичній безпеці. Серед них виділено дослідження, пов'язані із застосуванням різних підходів до безпеки. Доведено, що вміння оперувати методами представлення нечіткої інформації та технологій прийняття рішення сприяє розвитку програмних і технічних засобів захисту інформації. Поєднання кластерного підходу до розмежування прав із нечіткістю, яка буде динамічно змінюватися в процесі експлуатації інформаційної системи, дасть змогу гнучко та ефективно реалізовувати безпеку інформаційних систем. Проаналізовано роль математичних моделей у забезпеченні безпеки інформації та досліджено використання різних математичних підходів для аналізу та прогнозування загроз інформаційній безпеці. Автори розглядають сучасні техніки моделювання та їх застосування у сфері кібербезпеки. Використання математичних моделей може бути корисним для розроблення стратегій захисту даних в інформаційних системах. Дослідження указує на важливість розвитку математичних моделей для вдосконалення заходів захисту інформації та показує, як математичні моделі можуть допомогти вдосконалити системи захисту інформації.

Ключові слова: інформаційна безпека, математична модель, інформаційна система, моделі розмежування прав, нечітка інформація.

M.V. KRYKHIVSKYI, V.V. BANDURA, T.O. VAVRYK
Ivano-Frankivsk National Technical University of Oil and Gas

MATHEMATICAL MODELS OF INFORMATION SECURITY

Wide penetration of mathematical methods in the development of information technologies characterizes the modern stage of our society. The article is devoted to the problem of applying mathematical models with ambiguity and is of a review nature. The effectiveness of various mathematical approaches in detecting and preventing cyberthreats is compared. Among the mathematical methods used in information and cybernetic security, a large niche is made up of models of delimitation of access rights in information systems. This justifies the choice and relevance of this study. The combination of cluster technology as a mathematical model of a wide variety of objects, phenomena and connections between them with today's popular mathematical models of rights delimitation is considered. The article outlines the main elements of popular mathematical models for distinguishing access rights in information systems. The analysis of scientific papers made it possible to determine the main areas of application of properties, characteristics of fuzzy sets and fuzzy algorithms in information and cyber security. Among them, studies related to the use of various approaches to security are highlighted. It has been proven that the ability to operate with methods of presenting vague information and decision-making technologies contributes to the development of software and technical means of information protection. The combination of a cluster approach to the delimitation of rights with ambiguity, which will dynamically change during the operation of the information system, will allow flexible and effective implementation of the security of information systems. The article analyzes the role of mathematical models in ensuring information security and investigates the use of various mathematical approaches for analyzing and forecasting threats to information security. The authors consider modern modeling techniques and their application in the field of cyber security. Mathematical models can be used to develop data protection strategies in information systems. The study points to the importance of developing mathematical models for improving information protection measures and shows how mathematical models can help improve information protection systems.

Key words: information security, mathematical model, information system, models of differentiation of rights, unclear information.

https://doi.org/10.32782/mathematical-modelling/2024-7-1-13

Постановка проблеми

У сучасному світі, де зростання технологій відбувається надзвичайно швидко, питання кібербезпеки стає усе більш актуальним. Зловмисні кібератаки можуть призвести до значних фінансових утрат, порушення приватності, а також загрози національній безпеці. У цьому контексті математичні моделі відіграють ключову роль у розробленні ефективних заходів кіберзахисту. Вони дають змогу не лише аналізувати та прогнозувати потенційні кіберзагрози, а й розробляти стратегії для їх нейтралізації.

Характерною особливістю сучасних інформаційних технологій є застосування кібернетичних систем із програмним забезпеченням. Такі системи часто зазнають атак із метою зміни алгоритму їхньої роботи або заволодіння та знищення інформації. Особливо це актуально в умовах воєнного стану.

Запобігання таким загрозам є актуальною проблемою та повинно використовувати системний підхід із використанням математичних моделей, які слід удосконалювати з метою адаптації до нових методів проникнення, що виявляються у процесі застосування комп'ютерних систем. У цьому напрямі важливим є аналіз математичних моделей інформаційної безпеки для виявлення недоліків та можливості вдосконалення.

Ця стаття присвячена аналізу сучасних математичних моделей кібербезпеки, їх класифікації, виділенню сильних та слабких боків. Ми розглянемо різні підходи до моделювання кіберзагроз, включаючи стохастичні моделі, теорію ігор та системи масового обслуговування. Особлива увага буде приділена аналізу ефективності цих моделей у реальних умовах та їх застосуванню у розробленні комплексних систем кіберзахисту.

Аналіз останніх досліджень та публікацій

В інформаційних системах безпека передбачає розмежування прав доступу, яке класифікують [1] на дискреційні, мандатні та рольові. Усі вони мають як переваги, так і недоліки, що впливає на рівень захищеності від атак. Як правило, регулюється можливість доступу суб'єктів до об'єктів.

Дискреційні математичні моделі базуються на матриці доступу, рядки якої визначаються множиною суб'єктів S, а рядки – множиною об'єктів O. Бінарне відношення R на множині S×O визначає права доступу, що зумовлені деяким зовнішнім правилом. Модель Харрісона – Руззо – Ульмана (модель HRU) була реалізована для аналізу системи захисту та використовує скінченний автомат і є також прикладом дискреційної моделі розмежування прав доступу. Модель HRU функціонує згідно з визначеними правилами переходу автомата. Ще в одному типовому представнику дискреційного доступу – моделі п'ятивимірного простору Хартсона – простір безпеки визначається множинами встановлених повноважень, користувачів, операцій, ресурсів і станів. Модель Take-Grant також є моделлю дискреційного розмежування прав доступу і надає можливість аналізувати й перевіряти стан безпеки інформаційної системи. У ній як основні елементи використовують графи доступу їх перетворення. Модель допускає наявність прав доступу не лише у суб'єктів до об'єктів, а й в об'єктів до об'єктів. Основними перевагами дискреційних моделей розмежування прав доступу є простота реалізації системи розмежування доступу, універсальність і висока гнучкість. Проте основними недоліками є їх статичність, сильний вплив людського чинника на надійність системи захисту інформації та проблема «троянських» програм.

Мандатна модель поєднує для кожного суб'єкту з його рівнем доступу, який відповідає рівню конфіденційності, кожен об'єкт із його рівнем таємності за допомогою автомату відповідно до політики безпеки. Типовим представником такої моделі розмежування прав доступу є модель Белла – ЛаПадула. Формально вона описується множиною суб'єктів S, множиною об'єктів O ($S \subset O$), множиною прав доступу R={read,write}, множиною рівнів таємності L={U (відкрито), SU (для службового користування), S (таємно), TS (цілком таємно)}, решіткою

https://doi.org/10.32782/mathematical-modelling/2024-7-1-13

рівнів секретності $\Lambda=(L, \leq$ (оператор часткового несуворого відношення порядку рівнів таємності), • (оператор найменшої верхньої межі), $\otimes$ (оператор найбільшої нижньої межі)), матриця поточних прав доступу M і множиною станів системи, що представляється у вигляді впорядкованих пар (F,M), де: $F:S\cup O\rightarrow L$ (функція рівнів таємності, яка ставить у відповідність кожному об'єкту і суб'єкту в системі певний рівень таємності). Позитивним боком моделі Белла – ЛаПадули є автоматичне вирішення проблеми «троянських» програм. Відомі основні розширення моделі: модель із безпечною функцією переходу, уповноважені суб'єкти, груповий доступ – LowWatermark.

Рольова модель (Role-Based Access Control – RBAC) передбачає призначення ролей із відповідними дозволами суб'єктам, а не напряму, що призводить до простішого контролювання відносин між суб'єктами. Це забезпечує керування доступом як на основі матриці прав доступу для ролей, так і за допомогою правил, які регламентують призначення ролей користувачам. У цій моделі безпека інформаційної системи формується за допомогою множини користувачів S (суб'єкт – людина або автоматизований агент, множини ролей R (роль – робоча функція або назва, яка визначається на рівні авторизації), множини прав доступу до об'єктів системи P (дозволи – затвердження режиму доступу до ресурсу), сесії SE (відповідність між S, R та / або P), призначення суб'єкта SA, PA: $R \rightarrow 2p$ – функції, що визначає для кожної ролі множину прав доступу (для кожного $p \in P$ існує $r \in R$ така, що $p \in PA$ (r) і RH (частково впорядкованої ієрархії ролей).

У роботі [1] запропоновано модель розмежування прав доступу, яка, використовуючи особливості процесу хешування, дає змогу обмежити перелік робочих станцій, із яких користувачеві дозволено отримувати віддалений доступ до інформаційних ресурсів.

Дослідженню й аналізу інформаційних атак в умовах війни присвячено оглядову статтю [2], що є однією з найгостріших проблем сучасності. Результати дослідження розкрили основні особливості інформаційних війн та їхній вплив на кібербезпеку в глобальному масштабі та в окремих організаціях і державах.

Серія статей [3–8] пропонує аналіз застосування математичних методів та методологій до інформаційної та кібернетичної безпеки. Кластерний аналіз як основний підхід до кібербезпеки [3] можна використати для формалізації інформаційних ризиків. Описані етапи процедури кластеризації, вибору міри відстані та міри подібності для інформаційних об'єктів. Запропоновано застосовувати такі методи кластерного аналізу: алгоритм «найближчого сусіда», «k-means», «fuzzy c-means», «cosine similarity». Фрактальні моделі для захисту інформації можуть бути використані [4] в алгоритмах криптографічних і стеганографічних методів захисту інформації. Добре досліджені та описані алгоритми на графах також можуть бути корисними [5] у кібербезпеці. Оцінювання рівня захищеності інформаційної системи доречно досліджувати за допомогою математичних моделей теорій конфліктології [6], катастроф [7] та ігор [8].

Важливим завданням є виявлення та попередження вторгнень в інформаційну систему, що неможливо без застосування математичних методів. Авторами статті [9] «розглянуто такі математичні методи: сигнатурні методи; статистичні методи, а саме: приховані марковські моделі, метод опорних векторів, сплайни багатовимірної адаптивної регресії, методи кластеризації, байєсовські мережі; методи природних обчислень, такі як штучні нейронні мережі, штучні імунні мережі, генетичні алгоритми; біометрія поведінки; методи нечіткої логіки; експертні системи; теорія графів; теорія фракталів; теорія ігор». Ці методи проаналізовані й охарактеризовані. Відзначено, що поки не вдалося створити ідеальної IDPS, яка б не вимагала змін, доповнень та вдосконалень.

Дослідження математичних моделей у ракурсі оптимізації показало велику складність наукової проблеми безпеки інформації [10]. Класифіковано їх у моделі трансформації станів кінцевого автомата, моделі запозичення і передачі повноважень, семантичні моделі та моделі

https://doi.org/10.32782/mathematical-modelling/2024-7-1-13

інформаційних потоків. Показано, що актуальність розробок у галузі кібербезпеки буде зростати.

Проблеми організації прав доступу та захисту облікових даних користувачів мережевих операційних систем Widows досліджено в [11]. Запропоновано встановлювати «максимальне обмеження адміністративних привілеїв для адміністратора, надання користувачам та групам підтримки лише тих прав, які необхідні для виконання ними повсякденних завдань, використання облікових записів адміністраторів домену організації лише для керування контролерами домену».

У результаті огляду статей із кібербезпеки можна зробити висновок, що сучасні методи не є досконалими. Існує нагальна потреба досліджень у цій галузі, особливо математичного моделювання інформаційних систем для запобігання вторгненням або хоча б мінімізації втрат. Важливим у цьому напрямі нам представляється можливість прогнозування небезпеки.

Мета дослідження

Основною метою цього дослідження є розроблення та аналіз інтегрованих математичних моделей, які можуть ефективно виявляти, оцінювати та протидіяти кіберзагрозам. Це включає у себе:

− вивчення сучасних методів моделювання кіберзагроз та оцінки ризиків;

− розроблення нових оптимізаційних стратегій для підвищення рівня кібербезпеки;

− аналіз ефективності існуючих моделей кібербезпеки та їх застосування в реальних умовах;

− підвищення розуміння динаміки кіберінцидентів та розроблення прогностичних моделей для їх передбачення.

Дослідження спрямоване на забезпечення глибшого розуміння кібербезпеки з математичного погляду та створення основи для розроблення більш надійних систем захисту інформації, виділення підходів до вдосконалення математичного моделювання безпеки інформаційних програмних комп'ютерних систем.

Виклад основного матеріалу дослідження

Математичні моделі кібербезпеки умовно можна розділити за призначенням:

− моделі автентифікації, цифровий підпис;

− моделі розмежування прав доступу;

− моделі захисту програмного коду від несанкціонованого дослідження;

− моделі моніторингу та виявлення вторгнень.

Кожна із цих частин є важливою в умовах, коли атаки на інформаційні системи здійснюють державні інституції з великими обсягами фінансування. Особливо нагальним є створення безпечних умов функціонування у воєнний час.

Для вирішення цього завдання слід використовувати комплексний підхід до розроблення та аналізу математичних моделей кібербезпеки. Методологія базується на таких ключових принципах:

− Моделювання загроз: із використанням теорії ігор та стохастичних процесів для моделювання поведінки атакуючих та захисних стратегій.

− Аналіз ризиків: застосування квантитативних методів для оцінки ймовірності та потенційного впливу кібератак.

− Оптимізація захисту: розроблення оптимізаційних моделей для визначення найбільш ефективних стратегій кіберзахисту.

− Валідація моделей: перевірка моделей на реальних даних та сценаріях для забезпечення їх точності та придатності.

Дискреційні математичні моделі кібербезпеки, які базуються на матриці доступу, є важливим інструментом для управління правами доступу в інформаційних системах. Матриця доступу дає змогу визначити та контролювати, які користувачі мають доступ до певних ресурсів системи.

https://doi.org/10.32782/mathematical-modelling/2024-7-1-13

Кожен рядок матриці представляє суб'єкт (наприклад, користувача), а кожен стовпець – об'єкт (наприклад, файл). Елементи матриці вказують на тип доступу, який суб'єкт має до об'єкта.

Застосування нечітких множин до цієї моделі дає змогу ввести градацію прав доступу, що є більш гнучким та реалістичним підходом, аніж традиційні бінарні (дозволено/заборонено) системи. Нечіткі множини дають змогу визначити ступінь приналежності суб'єкта до множини користувачів, які мають доступ до певного ресурсу, що може змінюватися від 0 до 1. Це дає змогу моделювати різні рівні довіри та авторизації.

Розглянемо систему, де необхідно контролювати доступ до конфіденційних документів. За допомогою нечіткої логіки можна встановити, що деякі користувачі мають повний доступ (ступінь приналежності 1), інші – частковий доступ (ступінь приналежності між 0 та 1), а решта не мають доступу взагалі (ступінь приналежності 0).

Такий підхід дає змогу більш тонко налаштовувати політики безпеки, ураховуючи різні рівні ризику та необхідність доступу до інформації. Він також забезпечує можливість динамічної зміни прав доступу залежно від змін у ролі користувача або політиках безпеки. Також з’явиться можливість відслідковувати надмірну активність користувачів у знищенні великої кількості інформації, що не змогли передбачити у компанії «Київстар», яка зазнала потужної атаки.

Організаційно технічна модель кіберзахисту як комплекс заходів, суб’єктів і дій спрямована на розвиток спроможностей національної системи кібербезпеки для оперативного реагування на кібератаки та кіберінциденти. Ця модель має такі характеристики:

1. Організаційно-керівний рівень: включає основні суб’єкти національної системи кібербезпеки.

2. Технологічний рівень: забезпечує взаємодію технологічних підрозділів, обмін інформацією, моніторинг та сталу безпеку кіберпростору.

3. Базовий рівень: включає захищену інформаційну інфраструктуру та суспільство (громаду).

Застосування організаційно-технічної моделі кіберзахисту дасть змогу підвищити функціональність системи кіберзахисту України, зменшити уразливість інформаційних та комунікаційних систем, розвинути партнерство держави та приватного сектору у сфері кібербезпеки, ефективніше реагувати на кіберінциденти та кібератаки, здійснювати постійний контроль за станом кіберзахисту об’єктів критичної інфраструктури.

В організаційно-технічній моделі кіберзахисту існують поняття, які не завжди можна точно виміряти або визначити. Теорія нечітких множин дає змогу виразити ці поняття як нечіткі множини з функціями приналежності. Наприклад, поняття «рівень загрози» можна виразити нечіткою множиною, де елементи вказують на рівень небезпеки.

Теорія нечітких множин може допомогти враховувати нечіткість даних під час прийняття рішень. Наприклад, під час оцінки ризиків можна використовувати нечіткі множини для визначення рівня небезпеки.

Організаційно-технічна модель містить параметри, які можуть мати нечіткі значення. Теорія нечітких множин дає змогу аналізувати ці параметри, ураховуючи їх нечіткість. Наприклад, під час визначення ефективності заходів кіберзахисту можна враховувати нечіткість вимірювань.

Ця модель включає взаємодію різних суб'єктів. Теорія нечітких множин може допомогти моделювати нечіткі відносини між суб'єктами. Наприклад, взаємодія між різними відділами організації може бути виражена нечіткою множиною.

Отже, застосування теорії нечітких множин допоможе покращити адаптивність та гнучкість організаційно-технічної моделі кіберзахисту, особливо під час роботи з нечіткими даними та параметрами.

Модель Бела – ЛаПадули є моделлю розмежування доступу до інформації, що захищається. Вона базується на мандатній моделі керування доступом. Основні аспекти цієї моделі:

https://doi.org/10.32782/mathematical-modelling/2024-7-1-13

1. Проста властивість безпеки: забезпечує, що суб'єкт із рівнем доступу може читати інформацію з об'єкта лише тоді, коли його рівень перевищує рівень таємності об'єкта. Це правило також відоме як «Немає читання зверху».

2. Властивість: суб'єкт може писати інформацію в об'єкт тільки тоді, коли рівень таємності об'єкта перевищує рівень доступу суб'єкта.

3. Сильна властивість: ця властивість вимагає, щоб суб'єкт мав доступ до об'єкта тільки в тому разі, якщо його рівень доступу точно відповідає рівню таємності об'єкта.

4. Принцип стійкості: система знаходиться у безпечному стані, якщо кожен суб'єкт має доступ лише до об'єктів, до яких йому дозволено на основі поточної політики безпеки.

Це є важливим інструментом безпеки інформаційних систем, особливо в контексті розмежування доступу та захисту конфіденційної інформації. Теорія нечітких множин може допомогти врахувати нечіткість та невизначеність у знаннях та рішеннях.

Рольова модель розмежування доступу (RBAC) в інформаційних системах передбачає надання права доступу через ролі, ієрархії та обмеження. Ролі визначають, які дії можуть виконувати користувачі в системі. Це спрощує управління індивідуальними правами користувачів, оскільки привілеї призначаються через ролі, а не безпосередньо користувачам. Теорія нечітких множин дає змогу враховувати неоднозначність та невизначеність в оцінках.

У контексті RBAC нечіткі множини можуть використовуватися для визначення ролей та їхніх привілеїв. Наприклад, можна використовувати нечіткі множини для визначення, наскільки «сильно» користувач може виконувати певні дії.

RBAC часто використовується у системах, де чітко визначено посадові повноваження користувачів. Це дає змогу гнучко та динамічно змінювати права доступу в процесі функціонування системи. У цілому RBAC спрощує управління доступом, а теорія нечітких множин допомагає враховувати неоднозначність в оцінках, що може бути корисним у контексті визначення ролей та привілеїв.

Висновки

Статтю присвячено проблемі застосування математичних моделей із нечіткістю та носить оглядовий характер. Широке проникнення математичних методів у розроблення інформаційних технологій характеризує сучасний етап нашого суспільства. Серед математичних методів, що застосовують в інформаційній та кібернетичній безпеці, велику нішу займають моделі розмежування прав доступу технології, поєднання кластерної технології як математичної моделі найрізноманітніших об'єктів, явищ і зв'язків між ними з популярними сьогодні математичними моделями розмежування прав. Цим і обґрунтовано вибір та актуальність даного дослідження.

У статті викладено основні елементи популярних математичних моделей для розмежування прав доступу в інформаційних системах. Аналіз наукових праць дав змогу визначити основні напрями застосування властивостей, характеристик нечітких множин та нечітких алгоритмів в інформаційній та кібернетичній безпеці. Серед них виділено дослідження, пов'язані із застосуванням різних підходів до безпеки.

Доведено, що вміння оперувати методами представлення нечіткої інформації та технологій прийняття рішення сприяє розвитку програмних і технічних засобів захисту інформації. Поєднання кластерного підходу до розмежування прав із нечіткістю, яка буде динамічно змінюватися у процесі експлуатації інформаційної системи, дасть змогу гнучко та ефективно реалізовувати безпеку інформаційних систем.

Список використаної літератури

1. Баришев Ю.В., Каплун В.А., Неуйміна К.В. Дискреційна модель та метод розмежування прав доступу до розподілених інформаційних ресурсів. *Наукові праці ВНТУ*.

https://doi.org/10.32782/mathematical-modelling/2024-7-1-13

2017. № 2. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/26676/506-Текст%20статті-560-1-10-20170912.pdf?sequence=1&isAllowed=y (дата звернення: 10.04.2024).
2. Kravchenko, O., Veklych, V., Krykhivskyi, M., Madryha, T. Cybersecurity in the face of information warfare and cyberattacks. *Multidisciplinary Science Journal*. 2024. 6. URL: https://malque.pub/ojs/index.php/msj/article/view/1938 (дата звернення: 10.04.2024).
3. Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці / С.М. Шевченко та ін. *Кібербезпека: освіта, наука, техніка.* 2024. № 3(23). С. 258–273.
4. Математичні методи в кібербезпеці: фрактали та їх застосування в інформаційній та кібернетичній безпеці / С.М. Шевченко та ін. *Кібербезпека: освіта, наука,* техніка. 2019. №1(5). С. 31–39.
5. Шевченко С.М., Жданова Ю.Д., Складанний П.М., Спасітєлєва С.О. Математичні методи в кібербезпеці: графи та їх застосування в інформаційній та кібернетичній безпеці. *Кібербезпека: освіта, наука, техніка*. 2021. № 1(13). С. 133–144.
6. Шевченко С.М., Складанний П.М., Негоденко О.В., Негоденко В.П. Дослідження прикладних аспектів теорії конфліктів у системах безпеки. *Кібербезпека: освіта, наука, техніка*. 2022. № 2. С. 150–162.
7. Шевченко С.М., Жданова Ю.Д., Спасітєлєва С.О. Математичні методи в кібербезпеці: теорія катастроф. *Кібербезпека: освіта, наука, техніка*. 2023. № 3(19). С. 165–175.
8. Шевченко С.М., Жданова Ю.Д., Складанний П.М., Бойко С.В. Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*. 2023. № 2(22). С. 168–178.
9. Огляд математичних методів у системах виявлення та попередження кіберзагроз / Н.О. Лисенко та ін. *Актуальні проблеми автоматизації та інформаційних технологій*. 2021. № 25. С. 91–102.
10. Лаптєв О.А., Степаненко В.І., Тихонов Ю.О. Формальні математичні моделі для забезпечення безпеки інформації. *Сучасний захист інформації*. 2019. №1(37). С. 59–63.
11. Тишик І.Я. Забезпечення безпеки облікових записів корпоративних користувачів. *Кібербезпека: освіта, наука, техніка*. 2023. № 2(22). С. 214–225.

References

1. Baryshev, Yu.V., Kaplun, V.A., & Neuimina, K.V. (2017). Dyskretsiina model ta metod rozmezhuvannia prav dostupu do rozpodilenykh informatsiinykh resursiv [Discretionary model and method of distinguishing access rights to distributed information resources]. *Naukovi pratsi VNTU*, 2. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/26676/506-Текст%20статті-560-1-10-20170912.pdf?sequence=1&isAllowed=y [in Ukrainian].
2. Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. *Multidisciplinary Science Journal*, 6. 2024ss0219. https://doi.org/10.31893/multiscience.2024ss0219 [in English].
3. Shevchenko, S.M., Zhdanova, Yu.D., Spasitielieva, S.O., Mazur, N.P., Skladannyi, P.M., & Nehodenko, V.P. (2024). Matematychni metody v kiberbezpetsi: klasternyi analiz ta yoho zastosuvannia v informatsiinii ta kibernetychnii bezpetsi [Mathematical methods in cyber security: cluster analysis and its application in information and cyber security]. *Kiberbezpeka: osvita, nauka, tekhnika*, 3(23), 258–273. DOI: 10.28925/2663-4023.2024.23.258273 [in Ukrainian].
4. Shevchenko, S.M., Zhdanova, Yu.D., Spasitielieva, S.O., Nehodenko, V.P., Mazur, N.P., & Kravchuk, K.V. (2019). Matematychni metody v kiberbezpetsi: fraktaly ta yikh zastosuvannia v informatsiinii ta kibernetychnii bezpetsi [Mathematical methods in cyber security: fractals and their application in information and cyber security]. *Kiberbezpeka: osvita, nauka, tekhnika*, 1(5), 31–39. DOI: 10.28925/2663-4023.2019.5.3139 [in Ukrainian].

https://doi.org/10.32782/mathematical-modelling/2024-7-1-13

5. Shevchenko, S.M., Zhdanova, Yu.D., Skladannyi, P.M., & Spasitielieva, S.O. (2021). Matematychni metody v kiberbezpetsi: hrafy ta yikh zastosuvannia v informatsiinii ta kibernetychnii bezpetsi [Mathematical methods in cyber security: graphs and their application in information and cyber security]. *Kiberbezpeka: osvita, nauka, tekhnika*, 1(13), 133–144. DOI: 10.28925/2663-4023.2021.13.133144 [in Ukrainian].
6. Shevchenko, S.M., Skladannyi, P.M., Nehodenko, O.V., & Nehodenko, V.P. (2022). Doslidzhennia prykladnykh aspektiv teorii konfliktiv u systemakh bezpeky [Study of applied aspects of conflict theory in security systems]. *Kiberbezpeka: osvita, nauka, tekhnika*, 2, 150–162. DOI: 10.28925 /2663-4023.2022.18.150162 [in Ukrainian].
7. Shevchenko, S.M., Zhdanova, Yu.D., & Spasitielieva, S.O. (2023). Matematychni metody v kiberbezpetsi: teoriia katastrof [Mathematical methods in cyber security: disaster theory]. *Kiberbezpeka: osvita, nauka, tekhnika*, 3(19), 165–175. DOI: 10.28925/2663-4023.2023.19.16 5175 [in Ukrainian].
8. Shevchenko, S.M., Zhdanova, Yu.D., Skladannyi, P.M., & Boiko, S.V. (2023) Teoretyko-ihrovyi pidkhid do modeliuvannia konfliktiv u systemakh informatsiinoi bezpeky [Game-theoretic approach to modeling conflicts in information security systems]. *Kiberbezpeka: osvita, nauka, tekhnika*, 2(22), 168–178. DOI: 10.28925/2663-4023.2023.22.168178 [in Ukrainian].
9. Lysenko, N.O., Mazurenko, V.B., Fedorovych, A.I., Astakhov, D.S., & Statsenko, V.I. (2021). Ohliad matematychnykh metodiv u systemakh vyiavlennia ta poperedzhennia kiberzahroz. *Aktualni problemy avtomatyzatsii ta informatsiinykh tekhnolohii*, 25, 91–102. DOI: 10.15421/432110 [in Ukrainian].
10. Laptiev, O.A., Stepanenko, V.I., Tykhonov, & Yu.O. (2019). Formalni matematychni modeli dlia zabezpechennia bezpeky informatsii [Overview of mathematical methods in cyber threat detection and prevention systems]. *Suchasnyi zakhyst informatsii*, 1(37), 59–63. DOI: 10.31673/2409-7292.2019.015963 [in Ukrainian].
11. Tyshyk, I.Ya. (2023). Zabezpechennia bezpeky oblikovykh zapysiv korporatyvnykh korystuvachiv [Ensuring the security of corporate user accounts]. *Kiberbezpeka: osvita, nauka, tekhnika*, 2(22), 214–225. DOI: 10.28925/2663-4023.2023.22.214225 [in Ukrainian].

Крихівський Михайло Васильович – к.т.н., доцент кафедри інженерії програмного забезпечення Івано-Франківського національного технічного університету нафти і газу. E-mail: mykhailo.krykhivskyi@nung.edu.ua, ORCID: 0009-0000-3285-4308.

Бандура Вікторія Валеріївна – к.т.н., доцент, в. о. завідувача кафедри інженерії програмного забезпечення Івано-Франківського національного технічного університету нафти і газу. E-mail: viktoriia.bandura@nung.edu.ua, ORCID: 0000-0003-3143-0946.

Ваврик Тетяна Олександрівна – асистент кафедри інженерії програмного забезпечення Івано-Франківського національного технічного університету нафти і газу. E-mail: tetiana.vavryk@nung.edu.ua, ORCID: 0000-0002-0612-0084.

Krykhivskyi Mykhailo Vasyliovych – Candidate of Technical Sciences, Associate Professor at the Software Engineering Department of the Ivano-Frankivsk National Technical University of Oil and Gas. E-mail: mykhailo.krykhivskyi@nung.edu.ua, ORCID: 0009-0000-3285-4308.

Bandura Viktoriia Valeriivna – Candidate of Technical Sciences, Associate Professor, Acting Head at the Software Engineering Department of the Ivano-Frankivsk National Technical University of Oil and Gas. E-mail: viktoriia.bandura@nung.edu.ua, ORCID: 0000-0003-3143-0946.

Vavryk Tetiana Oleksandrivna – Assistant at the Software Engineering Department of the Ivano-Frankivsk National Technical University of Oil and Gas. E-mail: tetiana.vavryk@nung.edu.ua, ORCID: 0000-0002-0612-0084.

https://doi.org/10.32782/mathematical-modelling/2024-7-1-13