УДК 004.056.5:004.942 **DOI:** 10.31673/2412-9070.2026.056418

В. В. ЗІНЧЕНКО, аспірант;
ORCID: 0009-0000-7087-1678
С. В. ПРОКОПОВ, канд. техн. наук, доцент,
ORCID: 0009-0005-2251-9473
Державний університет інформаційно-комунікаційних технологій, Київ

МАТЕМАТИЧНА МОДЕЛЬ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Сучасна інформаційна система — це комплекс технічних засобів, програмного забезпечення, даних та користувачів. Такий комплекс призначений для ефективного збору, зберігання, обробки, передачі та захисту інформації з використанням сучасних цифрових технологій. У сучасних інформаційних системах основна увага спрямована на захист інформації. Основна функція захищеної інформаційної системи полягає у забезпеченні конфіденційності, цілісності та доступності інформації. Це дозволяє безпечно зберігати, обробляти та передавати дані, знижуючи ризик кібератак та інших загроз. В умовах стрімкого розвитку цифрових технологій, глобальної цифровізації економіки та поширення Інтернету захищені інформаційні системи (ЗІС) перестали бути виключно інструментом внутрішнього контролю — вони стали ключовим елементом стійкості, довіри та конкурентоспроможності організацій. Сучасний погляд на ЗІС вимагає виходу за межі традиційних підходів до кібербезпеки та переходу до комплексної, адаптивної та предиктивної моделі захисту інформації.

Стаття присвячена розробці математичної моделі захищених інформаційних систем, що складається з об'єкта захисту та систем безпеки, з урахуванням стану системи. З метою порушення роботи системи та отримання несанкціонованого доступу до захищених даних зловмисники здійснюють різного роду атаки. Оскільки процес функціонування системи має стохастичний характер, математичною моделлю є випадковий процес. Аналіз моделі, що розглядається в даній статті, дав змогу отримати такі оцінки: ймовірність того, що на циклі відновлення даного процесу аварії не відбулося; середній час напрацювання інформаційної системи до початка аварії. А також враховувати фактор помилкових та прихованих відмов.

Ключові слова: інформаційна система, математична модель, приховані відмови, помилкові відмови, системи захисту.

Вступ

Сучасна інформаційна система (ІС) — це комплекс програмного забезпечення, обладнання, даних, мереж та людей, призначений для збору, зберігання, обробки, передачі та аналізу інформації з метою забезпечення роботи організації або користувачів.

Основні компоненти сучасної інформаційної системи:

1. Апаратне забезпечення — комп'ютери, сервери, мобільні пристрої, мережеве обладнання.
2. Програмне забезпечення — операційні системи, бази даних, прикладні програми.
3. Дані — інформація, яка зберігається та обробляється системою.
4. Мережі та комунікації — локальні мережі, Інтернет, хмарні сервіси.
5. Користувачі — співробітники, адміністратори та кінцеві користувачі, які взаємодіють із системою.

Сучасне розуміння захищеної інформаційної системи вже не означає «система, яку неможливо зламати».

Еволюція поняття «захищена інформаційна система» (рис.1) відображає розвиток інформаційних технологій і зміну характеру загроз — від локальних технічних проблем до глобальних кібернетичних ризиків.

© Зінченко В. В., Прокопов С. В., 2026



Рис. 1. Еволюція поняття «захищена інформаційна система»

Натомість *захищена інформаційна система* – система, яка здатна попереджати, виявляти, витримувати та відновлюватися після атак, зберігаючи конфіденційність, цілісність і доступність даних.

Розвиток захищених інформаційних систем зробив актуальною проблему функціональної стійкості інформаційної безпеки. Для забезпечення захисту інформації від несанкціонованого доступу необхідно забезпечити певний рівень функціональної стійкості таких систем, включаючи функціональну стійкість апаратних засобів та програмного забезпечення. Математичні моделі функціональної стійкості систем захисту інформації розглядалися в різних роботах, наприклад у [1].

Постановка проблеми. Сучасні інформаційні системи функціонують в умовах постійного впливу внутрішніх і зовнішніх загроз, здатних порушувати конфіденційність, цілісність та доступність інформації, що обробляється. Ускладнення архітектури інформаційних систем, збільшення кількості взаємодіючих компонентів, використання розподілених обчислювальних ресурсів та зростання кількості потенційних каналів атак зумовлюють необхідність розробки адекватних математичних моделей, що дозволяють кількісно оцінювати рівень захищеності системи.

Традиційний підхід до забезпечення інформаційної безпеки, заснований на застосуванні набору окремих засобів захисту, не завжди дозволяє оцінити сукупний ефект їхньої взаємодії та визначити стійкість інформаційної системи до зміни умов функціонування. Зокрема, виникає проблема врахування взаємозв'язку між структурою системи, характеристиками використовуваних механізмів захисту, інтенсивністю та типами загроз, імовірністю виникнення відмов і атак, а також здатністю системи зберігати задані властивості в разі порушення роботи окремих компонентів.

У зв'язку з цим виникає задача розробки математичної моделі захищеної інформаційної системи, що дозволяє формалізувати взаємозв'язок між параметрами системи, загрозами та механізмами захисту і на цій основі кількісно оцінювати рівень її захищеності та стійкості до дестабілізуючих впливів.

Аналіз останніх досліджень і публікацій. Питанням функціональної стійкості систем і механізмів завжди приділяється велика увага в наукових дослідженнях. Функціональна стійкість є невід'ємною частиною всіх галузей промисловості.

Функціональна стійкість досліджувалася в працях багатьох авторів, а саме: А. Пуанкаре, Л. Чезарі, А.М. Ляпунова, Ж. Ла Салля та С. Лефшице та інших.

Питаннями забезпечення функціональної стійкості інформаційних та телекомунікаційних систем в Україні присвячені дослідження О. В. Барабаша, В.В. Вишнівського, А. П. Мусієнко, О. Г. Додонова, О. С. Горбачик, М. Г. Кузнєцової, А. В. Шевченка, С. М. Іщерякова, С. В. Прокопова, Ю. В. Каргаполова та інших вчених. У їхніх працях розглядаються математичне моделювання функціональної стійкості, оцінювання ймовірності збереження працездатності інформаційних систем, структурна живучість, діагностування відмов, резервування, динамічна реконфігурація та протидія внутрішнім і зовнішнім дестабілізуючим факторам.

У статті [1] автори пропонують методику оцінки функціональної стабільності системи захисту спеціальних мереж. Запропоновано кількісні методи оцінки функціональної стійкості за зазначеними показниками. На основі цих оцінок можна надати рекомендації щодо побудови структури функціонально стійкої мережі або сформулювати обґрунтовані вимоги до структури бездротової сенсорної мережі.

Робота[2] присвячена вирішенню актуальної проблеми забезпечення функціональної стійкості бездротових сенсорних мереж та їх компонентів. В роботі запропоновано алгоритм пошуку оптимальної структури бездротової сенсорної мережі.

Робота [3] присвячена забезпеченню функціональної стійкості інформаційної системи об'єкта критичної інфраструктури. Автори пропонують використовувати граф станів послідовно.

Система показників та критеріїв для оцінки рівня функціональної стабільності гетерогенних інформаційних мереж запропонована в роботі [4].

Мета і задачі дослідження. Однак, незважаючи на значну кількість публікацій, присвячених питанням безпеки інформаційних систем, проблема функціональної стійкості захищеної інформаційної системи на сьогодні залишається невирішеною. Тому завдання забезпечення стійкої роботи інформаційних систем є актуальним.

Метою даної роботи є створення математичної моделі функціональної стійкості захищеної інформаційної системи з урахуванням контрольних профілактичних заходів. Надати рекомендації щодо побудови функціонально стійкої інформаційної системи, яка буде проектуватися та експлуатуватися з високим ступенем стабільності.

Теоретичні основи дослідження

Математична модель захищеної інформаційної системи (ЗІС) призначена для формального опису процесів обробки інформації, функціонування засобів захисту та протидії загрозам інформаційної безпеки.

Якщо розглядати це питання глибше з точки зору класичної теорії інформаційної безпеки, то математична модель захищеної інформаційної системи — це строгий формальний апарат (зазвичай на основі теорії графів, теорії автоматів, теорії множин і матриць), який доводить, що система не може перейти з безпечного стану в небезпечний.

Існує кілька фундаментальних, класичних математичних моделей, які лежать в основі сучасних захищених операційних систем та СУБД:

1. Мандатні моделі (акцент на рівнях секретності)

Модель Белла — Лападули (Bell-LaPadula)[6]. Це найвідоміша модель, спрямована на забезпечення конфіденційності. В її основі лежить ієрархія рівнів доступу (наприклад: «не секретно», «секретно», «цілком секретно»).

2. Модель Біба (Biba)[7]. Математично схожа на модель Белла — Лападули, але спрямована на забезпечення цілісності даних, а не їхньої конфіденційності.

3. Дискреційні моделі (акцент на матриці доступу).

Модель Гаррісона — Руззо — Ульмана (HRU)[8]. Базується на понятті кінцевого автомата. У системі є безліч суб'єктів (S), об'єктів (O) та матриця прав доступу (M). Будь-яка дія користувача описується як команда, яка змінює матрицю доступу. Основний математичний результат моделі HRU полягає в тому, що в загальному випадку задача перевірки безпеки сис-

теми (тобто гарантія того, що право доступу не потрапить до несанкціонованого суб'єкта) є алгоритмічно нерозв'язною (зводиться до проблеми зупинки машини Тюрінга).

Модель Take-Grant (Бери-Дай). Використовує теорію орієнтованих графів. Вершини графа — це суб'єкти та об'єкти, а ребра — права доступу. Модель математично описує, як права доступу можуть передаватися в системі за допомогою чотирьох базових правил: Take (брати права), Grant (надавати права), Create (створювати об'єкти), Remove (видаляти права). Вона дозволяє алгоритмічно швидко обчислити, чи може певний суб'єкт отримати певні права на об'єкт у майбутньому.

4. Рольові та прикладні моделі.

Модель Кларка — Вілсона (Clark-Wilson)[9]. Зосереджена на цілісності в комерційних системах (банківська справа, бухгалтерія). Вводить поняття транзакцій та поділу обов'язків (Separation of Duties). Вона строго математично описує, які програми (транзакції) можуть переводити систему з одного несуперечливого стану в інший.

Моделі RBAC (Role-Based Access Control)[10]. Формалізують доступ на основі ролей. Права призначаються ролям (множинам), а користувачі включаються до цих ролей. Математично це описується через операції над множинами та відношеннями.

У чому полягає практичний сенс цих моделей? Розробники сертифікованих систем (наприклад, для військових або банківських потреб) використовують ці математичні апарати на етапі проектування. Вони формулюють теорему: «Якщо початковий стан системи є безпечним, і всі операції в системі підпорядковуються правилам обраної математичної моделі, то система завжди залишатиметься в безпечному стані», а потім математично доводять її для своєї архітектури.

Розглянемо структуру пропонованої математичної моделі. Будемо вважати, що інформаційна система складається з двох об'єктів: об'єкта захисту та системи безпеки. Припускаємо, що зловмисники можуть реалізувати весь спектр вразливостей, тобто вони мають доступ до всіх видів атак на конфіденційність, цілісність та доступність об'єкта захисту.

Система безпеки спрямована на забезпечення захисту від будь-якого типу атак. Слід зазначити, що система безпеки не є абсолютно надійною. Вона може перебувати в неробочому стані, причому це може статися внаслідок двох подій, вплив яких необхідно враховувати.

По-перше, це *приховані відмови*, під час яких система втрачає здатність забезпечувати належний захист від атак. Це такий стан системи безпеки, який неможливо виявити без проведення тестування або заходів профілактики.

По-друге, це *помилкові відмови*, під час яких система безпеки генерує захисне рішення без такої необхідності. Помилкові відмови, як правило, призводять до припинення роботи інформаційної системи. Звернемо увагу, що приховані та помилкові відмови не можуть відбуватися одночасно. Таким чином, використання певного класу атак можливе лише тоді, коли атака реалізується в період непрацездатності відповідної підсистеми системи безпеки. Ця подія є порушенням роботи інформаційної системи.

Оскільки в такій складній технічній системі, якою є система безпеки, неможливо відразу виявити відмови окремих підсистем, то для виявлення несправностей застосовуються різні тестові та діагностичні процедури. Ці процедури покликані контролювати стан підсистем у задані моменти часу. Для виконання тестових та діагностичних процедур потрібен певний час, тобто їх неможливо виконати миттєво.

Припускаємо, що існує кілька типів атак. Атаки різних типів є статистично незалежними. Після відбиття атаки або після відновлення нормального стану після помилкового спрацьовування системи безпеки випадковий процес, що відповідає процесу функціонування, повертається до початкового стану з тими самими ймовірнісними характеристиками, що й у початковий момент часу, а це означає, що процес генерації атак на систему та їх відбиття можна описати за допомогою альтернативного процесу відновлення. Також припустимо, що одночасний вплив двох і більше атак малоймовірний, тобто такі події є практично неможливими. Слід зазначити, що хоча ці обмеження й є, загалом кажучи, досить строгими, але зазначені припущення, як правило, виконуються.

Спочатку опишемо математичну модель прихованих відмов.

Нехай захищена інформаційна система складається з n елементів: $S = \{s_1, s_2, s_3, \dots, s_m\}$. Для кожного елемента s_i введемо інтенсивність прихованої відмови: λ_i. Прихована відмова характеризується тим, що вона виникає в момент t_0, однак виявляється лише через певний час T_d.

Час виявлення можна описати як:

$$T_d = T_{виникнення} - T_{виявлення}, \quad (1)$$

де $T_{виникнення}$ - момент виникнення відмови, $T_{виявлення}$ - момент її виявлення.

Чим більше T_d, тим довше система перебуває у стані прихованої несправності. Якщо припустити, що інтенсивність відмов λ є постійною, ймовірність того, що відмова не відбудеться протягом часу t, визначається так:

$$P_0(t) = e^{-\lambda t} \quad (2)$$

Тоді ймовірність виникнення відмови за проміжок часу t:

$$P_{\text{винекненя}}(t) = 1 - e^{-\lambda t} \quad (3)$$

Для декількох незалежних компонентів системи:

$$P_{\text{винекненя}}(t) = 1 - \prod_{i=1}^{n} e^{-\lambda_i t} = 1 - e^{-\sum_{i=1}^{n} \lambda_i t} \quad (4)$$

Для захищеної інформаційної системи особливо важливою є ймовірність того, що відмова вже виникла, але ще не виявлена. Нехай: λ — інтенсивність виникнення відмов; μ — інтенсивність виявлення відмов. Тоді середній час до виявлення:

$$T_d = \frac{1}{\mu} \quad (5)$$

Ймовірність перебування системи у стані прихованої відмови можна оцінити як:

$$P_{\text{прих}} = \frac{\lambda}{\lambda+\mu} \quad (6)$$

З формули видно, що зі збільшенням інтенсивності відмов λ ймовірність прихованого стану зростає, а зі збільшенням швидкості виявлення μ — зменшується.

Оцінімо вплив прихованої відмови на безпеку. Нехай D — втрати від експлуатації системи в стані прихованої відмови. Тоді очікувані втрати:

$$R_{\text{прих}} = P_{\text{прих}} * D \quad (7)$$

Якщо врахувати час, протягом якого відмова залишається невиявленою, можна застосовувати:

$$R_{\text{прих}} = \lambda * T_d * D \quad (8)$$

Отже, зниження ризику прихованих відмов досягається двома основними способами:

$\lambda \to min$ – тобто зниженням частоти виникнення відмов;

$T_d \to min$ – тобто скороченням часу їх виявлення.

Для захищеної інформаційної системи підсумкову модель прихованих відмов можна представити наступним чином:

$$M_{\text{прих}} = \langle \lambda, \mu, T_d, P_{\text{прих}}, D, P_{\text{прих}} \rangle, \quad (9)$$

де основними показниками є інтенсивність виникнення прихованих відмов, швидкість їх виявлення, середній час тривалості прихованого стану, ймовірність невиявленої відмови та пов'язаний з нею ризиків.

Таким чином, математична модель показує, що безпека системи залежить не тільки від здатності запобігати відмовам, але й від здатності своєчасно виявляти вже виниклі приховані порушення. Саме тому для захищених інформаційних систем важливим є постійний моніторинг, контроль цілісності, ведення журналу подій, резервування та автоматичне виявлення аномалій.

Розглянемо математичну модель хибних відмов захищеної інформаційної системи.

Хибна відмова — це ситуація, за якої захищена інформаційна система або її засіб контролю формує повідомлення про відмову, порушення чи загрозу, хоча фактичної відмови чи

порушення немає. Такі події можуть виникати через помилки датчиків, програмні помилки, некоректні налаштування, перешкоди в каналах зв'язку або недосконаліть алгоритмів виявлення.

Нехай, як і у попередньому випадку, захищена інформаційна система складається з безлічі контрольованих елементів:

$$S = \{s_1, s_2, s_3, \dots, s_m\}$$

Для кожного елемента встановимо:

λ_i −інтенсивність виникнення реальних відмов;

α_i— ймовірність помилкового спрацьовування системи контролю;

β_i— ймовірність пропуску реальної відмови;

μ_i— інтенсивність відновлення працездатності.

Позначимо подію реальної відмови через *F*, а подію формування системою сигналу про відмову через *A*. Тоді можливі чотири стани (табл.1).

Таблиця 1

Формування системою сигналу про відмову

Фактичний стан	**Сигнал системи**	**Результат**
Відмова відсутня	Сигнал відсутній	Нормальна робота
Відмова відсутня	Сигнал надходить	Хибна відмова
Існує відмова	Сигнал відсутній	Пропущена відмова
Існує відмова	Сигнал надходить	Вірно виявлена відмова

Якщо ймовірність виникнення реальної відмови за заданий проміжок часу дорівнює $P(F)$, а ймовірність помилкового спрацьовування за відсутності відмови дорівнює α, то ймовірність помилкової відмови:

$$P_{\text{хибн}} = P(\overline{F})\alpha\ ,$$

де

$$P\left(\overline{F}\right) = 1 - P(F)$$

Відповідно:

$$P_{\text{хибн}} = 1 - P(F)\alpha$$

Якщо інтенсивність реальних відмов є постійною і дорівнює λ, то:

$$P(F) = 1 - e^{-\lambda t}$$

Тоді:

$$P_{\text{хибн}} = e^{-\lambda t}\alpha$$

Якщо система працює протягом часу T, а інтенсивність хибних спрацьовувань дорівнює $\lambda_{\text{хибн}}$, очікувана кількість хибних відмов:

$$N_{\text{хибн}} = \lambda_{\text{хибн}} T$$

За наявності *n* незалежних елементів:

$$N_{\text{хибн}} = T \sum_{i=1}^{n} \lambda_{\text{хибн},i}$$

Це дає змогу оцінити навантаження на операторів та служби технічної підтримки.

Хибне спрацьовування може призвести до необґрунтованого відключення обладнання, блокування користувача, перемикання системи на резервний канал або запуску захисного механізму.

Нехай: $C_{\text{хибн}}$ — збитки від одного помилкового відмовлення; $N_{\text{хибн}}$ — очікувана кількість помилкових відмовлень. Тоді очікувані збитки:

$$R_{\text{хибн}} = C_{\text{хибн}} N_{\text{хибн}}$$

Або:

$$R_{\text{хибн}} = T\lambda_{\text{хибн}}C_{\text{хибнл}}$$

Для всієї системи:

$$R_{\text{хибн}} = T\sum_{i=1}^{n}\lambda_{\text{хибн},i}C_{\text{хибн},i}$$

Одним із важливих показників системи є коефіцієнт помилкових спрацювань:

$$K_{\text{пом}} = \frac{N_{\text{хибн}}}{N_{\text{хибн}}+N_{\text{іст}}},$$

де $N_{\text{хибн}}$ — кількість помилкових сигналів, а $N_{\text{іст}}$ — кількість істинних сигналів про відмови. Чим менше $K_{\text{пом}}$, тим вища точність системи контролю. Отже, математичну модель помилкових відмов захищеної інформаційної системи можна представити так:

$$M_{\text{хибн}} = \langle \lambda, \alpha, T, N_{\text{хибн}}\text{C}_{\text{хибн}}R_{\text{хибн}} \rangle,$$

де λ характеризує реальні відмови, α — ймовірність помилкового спрацювань, T — час функціонування системи, $N_{\text{хибн}}$ — очікувана кількість помилкових відмов, $\text{C}_{\text{хибн}}$ — збиток від однієї помилкової відмови, а $R_{\text{хибн}}$ — сумарний очікуваний ризик.

Головне завдання моделі полягає у мінімізації кількості помилкових спрацювань при збереженні високої ймовірності виявлення реальних відмов: $R_{\text{хибн}}\rightarrow$min, $P_{\text{виявл}}\rightarrow$max. Тобто система має одночасно мінімізувати помилкові тривоги та максимально точно виявляти реальні порушення.

Як було визначено вище, інформаційна система складається з двох об'єктів: об'єкта захисту та системи безпеки.

Якщо мова йде саме про математичну модель об'єкта захисту в захищеній інформаційній системі, її зручно сформулювати так, щоб вона описувала, що саме захищається, від яких загроз і якими властивостями повинна володіти система захисту.

Основними властивостями інформації, які необхідно забезпечити, є: C_f= конфіденційність, I_n= цілісність, A_v=доступність.

Отже, стан захищеності об'єкта можна представити у вигляді вектору:

$$\text{Z}= (C_f, I_n, A_v).$$

Кожному інформаційному ресурсу i_j можна зіставити рівень важливості:

$$W_j \in [0,1],$$

а для кожної загрози t_i— ймовірність її реалізації P_i та величину потенційних збитків D_i. Тоді ризик реалізації окремої загрози визначається за формулою: $R_i = P_i D_i$. Загальний ризик для об'єкта захисту:

$$R_{\text{зах}} = \sum_{i=1}^{k} P_i D_i$$

Після застосування засобів захисту ймовірність успішної реалізації загрози зменшується. Якщо E_i— ефективність застосовуваного засобу захисту, то залишковий ризик можна представити як:

$$R_{\text{залиш}} = \sum_{i=1}^{k} P_i(1 - E_i)D_i \text{ , де } 0 \le E_i \le 1$$

При цьому завдання системи захисту полягає у мінімізації залишкового ризику: $R_{\text{залиш}} \rightarrow min$

Одночасно мають виконуватися такі вимоги:

$$C_f \ge C_{min}\ I_n \ge I_{min}\ \ A_v \ge A_{min},$$

де C_{min}, I_{min} та A_{min} — мінімально допустимі рівні конфіденційності, цілісності та доступності.

Отже, математичну модель об'єкта захисту захищеної інформаційної системи можна представити у загальному вигляді:

$$O=\langle I, S, R, T, V, C_f, I_n, A_v, R_{\text{залиш}}\rangle \quad (10)$$

Математична модель (10) дозволяє формалізувати склад об'єкта захисту, інформаційні ресурси, суб'єктів доступу, загрози та вразливості, а також кількісно оцінити рівень захищеності та залишковий ризик. Практичне значення моделі полягає в тому, щоб визначити, які ресурси потребують захисту в першу чергу, які загрози є найнебезпечнішими та наскільки ефективно обрані засоби захисту знижують ризик.

Результати дослідження

За результатами проведених досліджень створено математичну модель функціональної стійкості захищеної інформаційної системи з урахуванням контрольних профілактичних заходів. Надані рекомендації щодо побудови функціонально стійкої інформаційної системи, яка буде проектуватися та експлуатуватися з високим ступенем стабільності.

Висновки та перспективи подальших досліджень

У даній роботі вдалося отримати оцінки показників надійності систем захисту інформації. Запропоновані оцінки досить просто обчислюються та враховують велику кількість різних параметрів процесу функціонування інформаційної системи.

Практичне значення моделі полягає в тому, щоб визначити, які ресурси потребують захисту в першу чергу, які загрози є найнебезпечнішими та наскільки ефективно обрані засоби захисту знижують ризик.

Внесок авторів

Вячеслав ЗІНЧЕНКО – аналіз сучасних підходів і математичних моделей захисту інформаційних систем, розробка математичних моделей прихованих та хибних відмов, визначення основних показників надійності та ризику, проведення математичних розрахунків і аналіз результатів, підготовка та редагування рукопису; Сергій ПРОКОПОВ – формулювання мети та постановка задачі дослідження, розроблення математичної моделі функціональної стійкості захищеної інформаційної системи, формалізація моделі об'єкта захисту, аналіз отриманих результатів, формулювання висновків.

Декларація про штучний інтелект

Автори підтверджують, що технології штучного інтелекту використовувалися виключно як об'єкт дослідження та інструмент експериментального аналізу, без застосування генеративних моделей для створення тексту рукопису.

Конфлікт інтересів

Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Список використаної літератури

1. Tolupa S., Laptiev S. The methodology for evaluating the functional stability of the protection system of special networks. Science-based technologies. 2022. Vol. 55, no. 3. P. 178–183. URL: https://doi.org/10.18372/2310-5461.55.16900 (date of access: 16.08.2026).

2. Barabash O., Sobchuk V., Sobchuk A., Musienko A., Laptiev O.. Algorithms for synthesis of functionally stable wireless sensor network // Advanced Information Systems. 2025. V. 9, № 1. Pp. 70–79. DOI: https://doi.org/10.20998/2522-9052.2025.1.08

3. Barabash O., Sobchuk V., Musienko A., Laptiev O., Bohomia V., Kopytko S.. System analysis and method of ensuring functional sustainability of the information system of a critical infrastructure object// System Analysis and Artificial Intelligence / Zgurovsky M., Pankratova N. (ed.). Cham:

Springer, 2023. (Studies in Computational Intelligence; v. 1107). DOI:https://doi.org/10.1007/978-3-031-37450-0_11

4. Maksymuk, O., Sobchuk, V., Salanda, I., Sachuk, Yu.: A system of indicators and criteria for evaluation of the level of functional stability of information heterogenic networks. Math. Model. Comput. 7(2), 285–292 (2020).

5. Arun Kumar B. R., Shreyas A. Cyber Security Tools for Vulnerability Assessment: A Survey and Analysis. Information Systems Engineering and Management. Cham, 2024. P. 485–498. URL: https://doi.org/10.1007/978-3-031-69201-7_36 (date of access: 16.08.2026).

6. Bell D. E., La Padula L. J. Secure Computer System: Unified Exposition and Multics Interpretation. Fort Belvoir, VA : Defense Technical Information Center, 1976. URL: https://doi.org/10.21236/ada023588 (date of access: 18.08.2026).

7. Bosselaers A., Preneel B. Integrity concepts. Integrity Primitives for Secure Information Systems. Berlin, Heidelberg, 1995. P. 9–22. URL: https://doi.org/10.1007/3-540-60640-8_2 (date of access: 18.08.2026).

8. Harrison M. A., Ruzzo W. L., Ullman J. D. Protection in operating systems. Communications of the ACM. 1976. Vol. 19, no. 8. P. 461–471. URL: https://doi.org/10.1145/360303.360333 (date of access: 18.08.2026).

9. Clark D. D., Wilson D. R. A Comparison of Commercial and Military Computer Security Policies. 1987 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 27–29 April 1987. 1987. URL: https://doi.org/10.1109/sp.1987.10001 (date of access: 18.08.2026).

10. Abdallah A. E., Khayat E. J. A Formal Model for Parameterized Role-Based Access Control. Formal Aspects in Security and Trust. New York. P. 233–246. URL: https://doi.org/10.1007/0-387-24098-5_17 (date of access: 18.08.2026).

V. Zinchenko. S. Prokopov

MATHEMATICAL MODEL OF A SECURE INFORMATION SYSTEM

A modern information system is a complex of technical facilities, software, data, and users designed to ensure the efficient collection, storage, processing, transmission, and protection of information using modern digital technologies. In contemporary information systems, particular attention is paid to information security. The primary function of a secure information system is to ensure the confidentiality, integrity, and availability of information. This enables the secure storage, processing, and transmission of data while reducing the risks of cyberattacks and other threats. In the context of the rapid development of digital technologies, global digitalization of the economy, and widespread use of the Internet, secure information systems (SISs) have ceased to be merely tools for internal control and have become a key element of organizational resilience, trust, and competitiveness. The modern approach to SISs requires moving beyond traditional cybersecurity methods toward a comprehensive, adaptive, and predictive model of information protection.

This article is devoted to the development of a mathematical model of a secure information system consisting of a protected object and security systems, taking into account the current state of the system. In order to disrupt system operation and gain unauthorized access to protected data, attackers employ various types of attacks. Since the system functioning process is stochastic in nature, a stochastic process is used as the mathematical model. Analysis of the proposed model makes it possible to obtain the following estimates: the probability that no failure will occur during the recovery cycle of the process, as well as the mean time to failure of the information system. The model also makes it possible to take into account the effects of false and hidden failures.

Keywords: information system, mathematical model, hidden failures, false failures, security system.

Надійшла до редакції: 19.08.2026
Прийнята до друку: 09.09.2026
Опубліковано: 30.10.2026
© 2026 Зінченко В. В., Прокопов С. В.
Цей матеріал ліцензовано за умовами CC BY 4.0.https://creativecommons.org/licenses/by/4.0/