https://doi.org/10.31891/2219-9365-2026-87-28
УДК 004.042

ТІТОВА Віра
Хмельницький національний університет
https://orcid.org/0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
КЛЬОЦ Юрій
Хмельницький національний університет
https://orcid.org/0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
ЧАБАН Олександр
Хмельницький національний університет
https://orcid.org/0009-0001-4710-3336
e-mail: chabanolek@khmnu.edu.ua
КУПЧИК Наталія
Хмельницький національний університет
https://orcid.org/0009-0004-2743-7162
e-mail: nataliiakupchyk@gmail.com

МУЛЬТИГРАФОВА МОДЕЛЬ ІНФОРМАЦІЙНИХ ПОТОКІВ ДЛЯ АНАЛІЗУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

У статті розглянуто підхід до формалізованого опису процесів передавання інформації в інформаційних системах на основі моделі елементарних інформаційних потоків. Проведено огляд існуючих рішень у сфері застосування моделей інформаційних потоків для задач інформаційної безпеки та показано обмеження наявних підходів, пов'язані з недостатньою формалізацією каналів передавання інформації. Запропоновано мультиграфову модель елементарних інформаційних потоків, яка враховує гетерогенність каналів взаємодії та дає змогу описувати гетерогенні комп'ютерні системи за допомогою скінченної множини елементів. На прикладі процесу передавання електронної пошти продемонстровано практичне застосування розробленої моделі. Показано, що запропонований підхід може слугувати формальною основою для подальшого аналізу загроз інформаційній безпеці, побудови моделей загроз і формування політики розмежування доступу.

Ключові слова: інформаційний потік, елементарний інформаційний потік, захист інформації, модель загроз, розмежування доступу, теорія графів, гетерогенна інформаційна система, канал передавання інформації.

TITOVA Vira, KLOTS Yurii, CHABAN Oleksandr, KUPCHYK Nataliia
Khmelnitskyi National University

MULTIGRAPH MODEL OF INFORMATION FLOWS FOR INFORMATION SECURITY ANALYSIS IN COMPUTER SYSTEMS

The paper considers an approach to the formalized description of information transfer processes in information systems based on a model of elementary information flows. The relevance of the study is determined by the growing complexity of modern information systems, the increasing number of communication channels, and the need to improve formal methods for security analysis. In existing approaches, information flows are often treated only as auxiliary elements of architectural descriptions, while communication channels are not sufficiently formalized as independent security objects.

The study reviews existing solutions related to the application of information flow models in cybersecurity, threat modeling, and access control policy formation. It is shown that although information flow theory is applied to a wide range of systems, including cyber-physical systems, telemedicine platforms, SCADA systems, cloud services, IoT infrastructures, and general-purpose software systems, many existing approaches remain limited in their ability to represent heterogeneous communication channels and their role in threat realization.

To address this issue, the paper proposes a multigraph model of elementary information flows in an information system. In the proposed model, an elementary information flow consists of three components: two vertices representing information carriers and one interaction channel connecting them. Using graph theory notation, sets of users, software components, storage devices, and communication channels are defined. The communication channels are classified according to the environment and mode of interaction, including local and remote channels, as well as electromagnetic and virtual environments. This makes it possible to construct a finite set of elementary information flows for describing heterogeneous computer systems.

The practical applicability of the proposed model is demonstrated through the example of e-mail transmission and reception. The communication process is decomposed into a sequence of elementary information flows that together form a complete flow scheme. The example shows that any information transfer process in the system can be reduced to a finite set of elementary flows, while the completeness and precision of the resulting scheme depend on the accuracy of the system element description.

The results indicate that the proposed approach provides a formal basis for further security analysis by enabling communication channels to be treated as independent objects of protection. The model can be used for threat modeling, structured system description, and access control policy development. In addition, its application reduces the level of subjectivity in system analysis by replacing intuitive threat identification with a formalized description of information flows. Future research may focus on using the proposed model as a basis for classifying threats to confidentiality, integrity, and availability of information.

Keywords: information flow, elementary information flow, information security, threat model, access control, graph theory, heterogeneous information system, communication channel.

Стаття надійшла до редакції / Received 02.07.2026
Прийнята до друку / Accepted 12.08.2026
Опубліковано / Published 10.09.2026

© ТІТОВА Віра, КЛЬОЦ Юрій, ЧАБАН Олександр, КУПЧИК Наталія

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Інформація сьогодні – це важливий ресурс, втрата якого загрожує небезпечними наслідками [1]. Документообіг – це рух документів в організації з моменту їх створення або отримання до завершення виконання або відправлення; будь-яку схему документообігу можна подати як сукупність інформаційних потоків [1].

Інформаційний потік – це сукупність повідомлень, що циркулюють у межах системи, а також між системою та зовнішнім середовищем, необхідних для контролю та управління діяльністю [1]. Необхідність застосування моделі інформаційних потоків неодноразово підкреслювалася в різних дослідженнях. Однак, як і в багатьох інших випадках, що стосуються забезпечення інформаційної безпеки, ця тема залишається відкритою через відсутність типізації. У даній статті пропонується власна версія застосування моделі інформаційних потоків для забезпечення інформаційної безпеки.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

У наукових працях, присвячених інформаційній безпеці, неодноразово наголошується на доцільності використання моделі інформаційних потоків під час побудови моделі загроз, політик розмежування доступу та засобів контролю взаємодії між компонентами системи. Такий підхід дає змогу розглядати систему не лише як сукупність окремих елементів, а і як середовище циркуляції інформації, де саме потоки даних часто стають об'єктом атак або каналом реалізації загроз.

Теорія інформаційних потоків застосовується до широкого спектра сучасних систем, зокрема кіберфізичних систем, телемедичних платформ, SCADA-систем, хмарних сервісів, IoT-інфраструктур та програмних систем загального призначення. Для кожного з цих класів систем характерною є наявність великої кількості взаємопов'язаних компонентів і каналів передавання даних, що підвищує значущість контролю інформаційних потоків як окремого напряму забезпечення безпеки.

У дослідженнях [2,3], присвячених кіберфізичним системам, інформаційний потік розглядається як один із базових елементів архітектури безпеки, оскільки саме порушення умов допустимого передавання інформації може призводити до втрати конфіденційності, цілісності або доступності даних. Водночас у частині робіт основну увагу зосереджено переважно на фізичних процесах або структурних компонентах системи, тоді як інформаційні потоки згадуються лише як допоміжний елемент моделі.

Подібна ситуація простежується і в роботах, присвячених телемедичним та розподіленим системам. Частина дослідників пропонує використовувати для аналізу безпеки методології DFD у поєднанні зі STRIDE або іншими підходами до класифікації загроз [3,4]. Це дає можливість відобразити взаємодію між клієнтами, серверами, базами даних і зовнішніми сервісами. Однак навіть у таких роботах інформаційний потік не завжди розглядається як самостійний об'єкт захисту, а радше як частина загальної схеми обміну даними.

Особливе значення аналіз інформаційних потоків має для SCADA- та IoT-систем, оскільки саме в них кількість каналів передавання інформації є найбільшою, а порушення режиму захищеності в таких каналах може призводити до суттєвих економічних втрат або навіть критичних наслідків для інфраструктури. У низці досліджень загрози, пов'язані з каналами зв'язку, вже враховуються в межах моделі, однак сам канал або потік передавання інформації часто не отримує достатньо повного формального опису [5-7]. Через це модель втрачає частину аналітичної цінності, оскільки не охоплює всі можливі способи несанкціонованого впливу на процес обміну даними.

У більшості прикладних рішень для опису взаємодії між компонентами системи використовується методологія DFD, яка є зручною для візуалізації процесів, зовнішніх сутностей, сховищ даних і потоків обміну. Разом із тим цей підхід має певні обмеження. Зокрема, DFD здебільшого використовується як інструмент структурного опису системи, але не забезпечує достатньої деталізації характеристик самих каналів передавання інформації, їхніх властивостей і умов безпечного функціонування. Це ускладнює застосування DFD як єдиної основи для побудови повноцінної моделі загроз.

Окремі дослідження пропонують альтернативні підходи, зокрема використання марковських моделей або мереж Петрі [8]. Такі методи є корисними для опису станів системи, сценаріїв атак або процесів передавання даних, однак вони не завжди придатні для виокремлення інформаційного потоку як окремого об'єкта аналізу в задачах інформаційної безпеки. У результаті вони краще працюють для моделювання динаміки подій або сценаріїв розвитку атаки, ніж для формування універсальної моделі загроз на основі потоків інформації.

Важливо також розмежовувати поняття мережевого з'єднання та інформаційного потоку. Мережевий канал є лише окремим випадком реалізації інформаційного потоку, тоді як сам інформаційний потік охоплює

ширший спектр способів передавання, оброблення та обміну інформацією в системі. Змішування цих понять ускладнює побудову коректної моделі загроз і призводить до неповного опису потенційних векторів впливу на інформацію.

Отже, аналіз існуючих рішень свідчить, що підхід на основі інформаційних потоків вже використовується в різних прикладних сферах і визнається перспективним для задач інформаційної безпеки. Водночас наявні методи або недостатньо формалізують самі потоки, або зосереджуються переважно на компонентах системи, а не на зв'язках між ними. Це дає підстави вважати доцільним подальше розроблення моделей, у яких інформаційні потоки розглядаються як повноцінний об'єкт аналізу при побудові моделі загроз та обґрунтуванні заходів захисту.

Побудова моделі інформаційних потоків

Будь-яку схему обміну інформацією можна подати як сукупність елементарних інформаційних потоків. Елементарний інформаційний потік включає три елементи: дві вершини та канал взаємодії.

Це поняття можна продемонструвати, застосувавши теорію графів. Введемо такі позначення: *IC* – множина носіїв інформації (множина вершин графа), *CC* – множина каналів взаємодії (множина ребер графа). Поставивши у відповідність будь-які два елементи з *IC* та один елемент з *CC*, отримаємо елементарний інформаційний потік у вигляді неорієнтованого графа з двома вершинами (рис. 1).

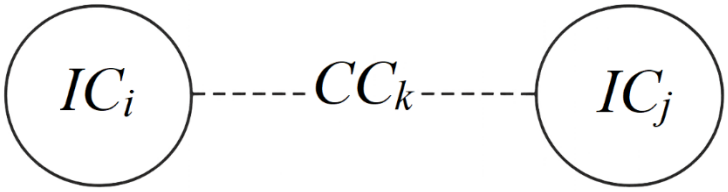

Рис. 1. Елементарний інформаційний потік

Нотація інформаційних потоків ґрунтується на нотації теорії графів. Зазначений вище інформаційний потік описується трійкою:

$$g = \{IC_i, CC_k, IC_j\}, \tag{1}$$

де IC_i, IC_j – можливий носій інформації; CC_z – можливий канал передавання інформації.

Множину носіїв інформації було поділено на три підмножини, і вона набула такого вигляду:

$$IC = \{IC_1, IC_2, IC_3\}, \tag{2}$$

де IC_1 – множина користувачів, IC_2 – множина програмного забезпечення, IC_3 – множина пристроїв зберігання інформації.

Оскільки межі дослідження обмежені взаємодією в кіберпросторі, вважається, що користувач здійснює взаємодію з програмним забезпеченням (ПЗ) засобами операційної системи. А канали взаємодії між користувачем і ПЗ є каналами взаємодії між операційною системою та ПЗ. Щоб конкретизувати множину каналів передавання інформації, слід звернутися до моделі OSI.

Дослідивши всі рівні взаємодії та використовувані протоколи, їх можна поділити на певні групи. Перша класифікація випливає з визначення самих рівнів – канали зв'язку можна поділити на локальні та віддалені. Друга класифікація випливає з особливостей роботи протоколів і пристроїв на різних рівнях – канали можна поділити на такі, що працюють у віртуальному та електромагнітному середовищі. Тоді множина каналів взаємодії набуде такого вигляду:

$$CC = \{CC_1, CC_2, CC_3, CC_4\}, \tag{3}$$

де CC_1 – множина каналів взаємодії в електромагнітному середовищі (поле передавання даних), CC_2 – множина каналів взаємодії у віртуальному середовищі (віртуальний адресний простір), CC_3 – множина каналів віддаленої взаємодії в електромагнітному середовищі, CC_4 – множина каналів віддаленої взаємодії у віртуальному середовищі.

Також необхідно ввести додаткові обмеження:

- ✓ елементи множини IC_1 не можуть безпосередньо взаємодіяти з іншими елементами цієї самої множини;
- ✓ елементи множини IC_3 не можуть безпосередньо взаємодіяти з іншими елементами цієї самої множини;
- ✓ елементи множини IC_1 не можуть безпосередньо взаємодіяти з елементами множини IC_3 і

навпаки;

✓ віддалені канали доступні лише під час взаємодії елементів множини IC_2 з елементами цієї самої множини.

З урахуванням усього викладеного множина всіх елементарних потоків матиме такий вигляд:

$$G = \{g_i \mid g \in G\},\ i = \overline{1,8}, \tag{4}$$

де $g_1 = \{IC_1, CC_1, IC_2\}$, $g_2 = \{IC_1, CC_2, IC_2\}$, $g_3 = \{IC_2, CC_1, IC_2\}$, $g_4 = \{IC_2, CC_2, IC_2\}$, $g_5 = \{IC_2, CC_3, IC_2\}$, $g_6 = \{IC_2, CC_4, IC_2\}$, $g_7 = \{IC_2, CC_1, IC_3\}$, $g_8 = \{IC_2, CC_2, IC_3\}$

Результатом об'єднання всіх зазначених вище графів буде неорієнтований мультиплікативний граф (рис. 2), який і становитиме модель елементарних інформаційних потоків під час здійснення доступу до електронних інформаційних ресурсів.

Ця модель дає змогу побудувати схему інформаційних потоків в інформаційній системі, використовуючи скінченну множину елементарних інформаційних потоків *G*.

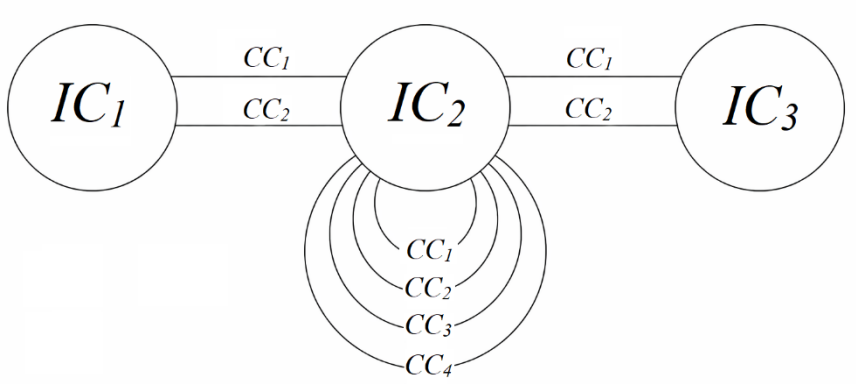

Рис.2. Модель елементарних інформаційних потоків у вигляді неорієнтованого мультиплікативного графа

Продемонструємо застосування моделі елементарних інформаційних потоків на прикладі процесу передавання/отримання електронної пошти. Листування здійснюється між двома користувачами з їхніх мобільних пристроїв, які підключені до мережі Інтернет бездротовим з'єднанням (загальну схему описуваного процесу наведено на рис. 3).

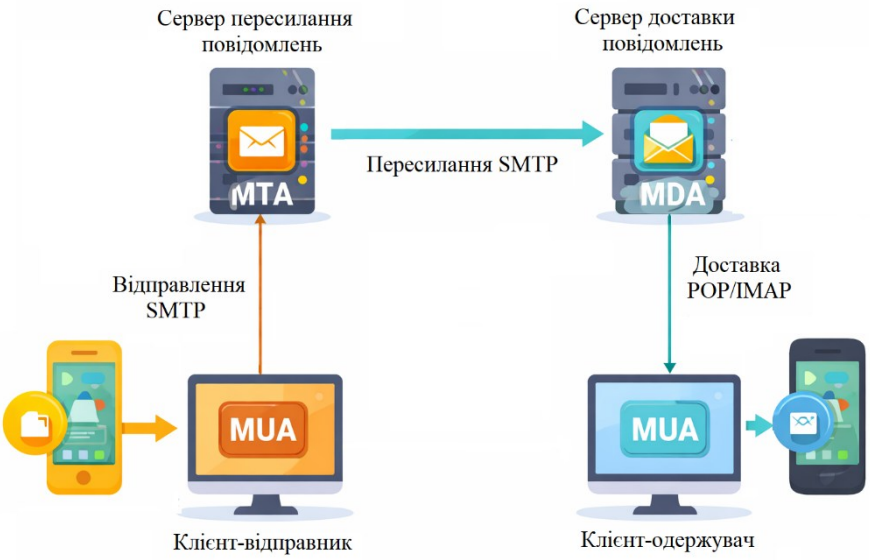

Рис. 3. Схема процесу передавання/отримання електронної пошти

Загальний опис процесу передавання/отримання електронної пошти:

– перший користувач надсилає листа на поштовий сервер свого провайдера;

– поштовий провайдер пересилає листа на сервер провайдера одержувача;
– сервер провайдера одержувача передає листа одержувачу.

Щоб скласти повний перелік інформаційних потоків, додамо ще кілька уточнень до опису процесу:

– лист має лише текстову складову й набирається користувачем;
– Mail Transfer Agent (MTA) не зберігає повідомлення в себе, а лише передає їх до Mail Delivery Agent (MDA);
– MDA (як і MTA) – це певний програмно-апаратний комплекс, що складається із програмного засобу пересилання повідомлень і сховища даних;
– у нашому випадку здійснюється взаємодія між мобільним поштовим клієнтом і серверним ПЗ, яке вже взаємодіє із серверним сховищем;
– взаємодія між поштовим клієнтом одержувача та MDA здійснюється за протоколом IMAP.

Із усього сказаного випливає такий перелік інформаційних потоків: відправник – Mail User Agent (MUA); MUA – MTA; MTA – MDA; MDA – серверне сховище; серверне сховище – MDA; MDA – MUA; MUA – одержувач.

Спираючись на перелік інформаційних потоків і враховуючи, що MDA і MTA – це різні пристрої, побудуємо повний перелік елементарних інформаційних потоків. Кожен потік розбивається на два елементарні, оскільки модель передбачає поділ каналу передавання даних на електромагнітний і віртуальний. Додатково введемо позначення всіх учасників процесу відповідно до моделі елементарних інформаційних потоків.

Множина користувачів: $IC_1 = \{IC_{1,1}, IC_{1,2}\}$, де $IC_{1,1}$ – відправник; $IC_{1,2}$ – одержувач.

Множина процесів: $IC_2 = \{IC_{2,1}, IC_{2,2}, IC_{2,3}, IC_{2,4}\}$, де $IC_{2,1}$ – MUA відправника; $IC_{2,2}$ – MTA; $IC_{2,3}$ – MDA; $IC_{2,4}$ – MUA одержувача.

Множина сховищ інформації IC_3 містить тільки один елемент – серверне сховище (база даних).

Підсумкова множина елементарних інформаційних потоків матиме такий вигляд:

$$IF_1 = \{IC_{1,1}, CC_1, IC_{2,1}\},\ IF_2 = \{IC_{1,1}, CC_2, IC_{2,1}\},\ IF_3 = \{IC_{2,1}, CC_3, IC_{2,2}\},$$
$$IF_4 = \{IC_{2,1}, CC_4, IC_{2,2}\},\ IF_5 = \{IC_{2,2}, CC_3, IC_{2,3}\},\ IF_6 = \{IC_{2,2}, CC_4, IC_{2,3}\},$$
$$IF_7 = \{IC_{2,3}, CC_1, IC_3\},\ IF_8 = \{IC_{2,3}, CC_2, IC_3\},\ IF_9 = \{IC_3, CC_1, IC_{2,3}\},$$
$$IF_{10} = \{IC_3, CC_2, IC_{2,3}\},\ IF_{11} = \{IC_{2,3}, CC_3, IC_{2,4}\},\ IF_{12} = \{IC_{2,3}, CC_4, IC_{2,4}\},$$
$$IF_{13} = \{IC_{2,4}, CC_1, IC_{1,2}\},\ IF_{14} = \{IC_{2,4}, CC_2, IC_{1,2}\}$$

Увесь процес передавання інформації можна описати за допомогою набору елементарних інформаційних потоків, які в сукупності й формують повну схему інформаційних потоків.

Слід також зазначити таке: можна помітити, що в розглянутому прикладі наявні чотирнадцять інформаційних потоків, тоді як у моделі елементарних інформаційних потоків їх лише вісім. Річ у тім, що модель за визначенням має абстрактний характер, а кожен її інформаційний потік може бути представлений нескінченною множиною прикладів із реального життя.

З урахуванням симетричності потоків і належності вершин до одних і тих самих множин можна однозначно зіставити всі елементи множини *IF* елементам множини *G*: $IF_1, IF_{13} \Rightarrow g_1$, $IF_2, IF_{14} \Rightarrow g_2$, $IF_3, IF_5, IF_6, IF_{11} \Rightarrow g_5$, $IF_4, IF_{12} \Rightarrow g_6$, $IF_7, IF_9 \Rightarrow g_7$, $IF_8, IF_{10} \Rightarrow g_8$.

Із цього випливає, що будь-який процес передавання інформації в системі можна звести до скінченної множини елементарних інформаційних потоків. Потужність цієї множини дорівнює восьми, тобто всі канали будь-якої системи передавання електронної інформації можна описати за допомогою скінченної множини елементів. Безперечно, такого опису недостатньо для більшості потреб, пов'язаних із використанням інформаційних систем, однак у контексті захисту інформації та визначення переліку типових загроз інформації такого опису більш ніж достатньо.

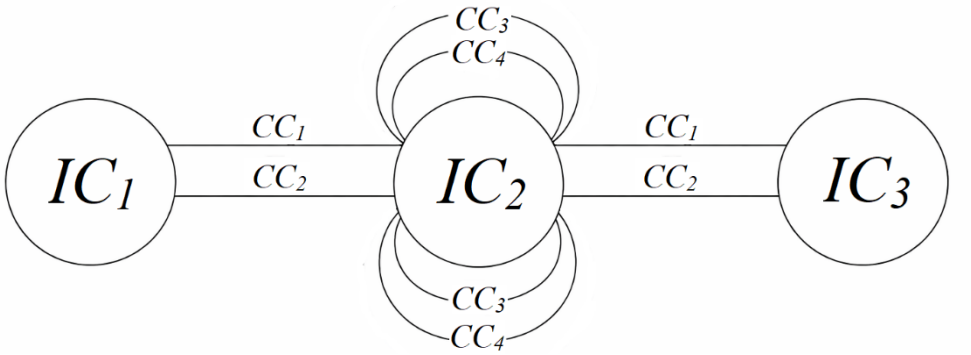

Рис. 4. Граф інформаційних потоків процесу передавання/отримання електронної пошти

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У даній статті запропоновано мультиграфову модель елементарних інформаційних потоків в інформаційній системі, що відрізняється врахуванням гетерогенності каналів взаємодії.

Розроблена модель елементарних інформаційних потоків дає змогу описати гетерогенну комп'ютерну систему за допомогою скінченної множини елементів. Схема елементарних інформаційних потоків включає всі можливі потоки, які можуть виникнути в системі. Запропонований підхід створює формальну основу для подальшого аналізу загроз інформаційній безпеці, оскільки дає змогу розглядати канали передавання інформації як окремі об'єкти захисту.

Практична цінність моделі полягає в можливості її використання для побудови моделей загроз, формування політики розмежування доступу та структурованого опису взаємодії між елементами системи. Крім того, застосування моделі дає змогу зменшити рівень суб'єктивності під час аналізу системи за рахунок переходу від інтуїтивного визначення загроз до формалізованого опису інформаційних потоків. Перспективою подальших досліджень є використання запропонованої моделі як основи для класифікації типових загроз конфіденційності, цілісності та доступності інформації.

Література

1. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ, 1999.

2. Моргуль Д. М., Нарєжній О. П., Гріненко Т. О. Модель порушника та модель загроз для веб-сервісу QRNG // Радіотехніка. 2025. № 221. https://doi.org/10.30837/rt.2025.2.221.04

3. Коротунов С. Ю., Табунщик Г. В., Вольфф К. Аналіз існуючих архітектур та методів моделювання кіберфізичних систем для розумних енергомереж // Електротехнічні та комп'ютерні системи. 2018. № 27(103). https://doi.org/10.15276/eltecs.27.103.2018.20

4. Невольніченко А. І., Чумаченко С. М., Михайлова А. В., Пиріков О. В., Мурасов Р. К. Моделювання загроз виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури з використанням методу системної динаміки // Таврійський науковий вісник. Серія: Технічні науки. 2022. № 3. С. 88–99. https://doi.org/10.32851/tnv-tech.2022.3.10

5. Журило О. Д., Ляшенко О. С. Архітектура та системи безпеки IoT на основі туманних обчислень // Сучасний стан наукових досліджень та технологій в промисловості. 2024. № 1(27). С. 54–66. https://doi.org/10.30837/ITSSI.2024.27.054

6. Шабала Є., Корнійчук Б. Методологія оцінювання безпеки IoT на промислових об'єктах // Управління розвитком складних систем. 2024. № 60. С. 146–155. https://doi.org/10.32347/2412-9933.2024.60.146-155

7. Завгородній В. В., Дроздова Є. А., Козел В. М. Аналіз проблем безпеки IoT пристроїв // Вісник Херсонського національного технічного університету. 2020. № 4(75)

8. Никифоров О. В., Путятін В. Г., Куценко С. А. Математичні моделі та методи для вирішення деяких питань інформаційної безпеки // Реєстрація, зберігання і обробка даних. 2023. Т. 25, № 2. С. 27–65. https://doi.org/10.35681/1560-9189.2023.25.2.300525

References

1. ND TZI 1.1-003-99. Terminolohiia v haluzi zakhystu informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu. Kyiv: Departament spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii SBU, 1999.

2. Morhul D. M., Nariezhnii O. P., Hrinenko T. O. Model porushnyka ta model zahroz dlia veb-servisu QRNG // Radiotekhnika. 2025. № 221. https://doi.org/10.30837/rt.2025.2.221.04

3. Korotunov S. Yu., Tabunshchyk H. V., Volff K. Analiz isnuiuchykh arkhitektur ta metodiv modeliuvannia kiberfizychnykh system dlia rozumnykh enerhomerezh // Elektrotekhnichni ta kompiuterni systemy. 2018. № 27(103). https://doi.org/10.15276/eltecs.27.103.2018.20

4. Nevolnichenko A. I., Chumachenko S. M., Mykhailova A. V., Pyrikov O. V., Murasov R. K. Modeliuvannia zahroz vynyknennia nadzvychainykh sytuatsii na obiektakh krytychnoi infrastruktury z vykorystanniam metodu systemnoi dynamiky // Tavriiskyi naukovyi visnyk.

Seriia: Tekhnichni nauky. 2022. № 3. S. 88–99. https://doi.org/10.32851/tnv-tech.2022.3.10

5. Zhurylo O. D., Liashenko O. S. Arkhitektura ta systemy bezpeky IoT na osnovi tumannykh obchyslen // Suchasnyi stan naukovykh doslidzhen ta tekhnolohii v promyslovosti. 2024. № 1(27). S. 54–66. https://doi.org/10.30837/ITSSI.2024.27.054

6. Shabala Ye., Korniichuk B. Metodolohiia otsiniuvannia bezpeky IoT na promyslovykh obiektakh // Upravlinnia rozvytkom skladnykh system. 2024. № 60. S. 146–155. https://doi.org/10.32347/2412-9933.2024.60.146-155

7. Zavhorodnii V. V., Drozdova Ye. A., Kozel V. M. Analiz problem bezpeky IoT prystroiv // Visnyk Khersonskoho natsionalnoho tekhnichnoho universytetu. 2020. № 4(75)

8. Nykyforov O. V., Putiatin V. H., Kutsenko S. A. Matematychni modeli ta metody dlia vyrishennia deiakykh pytan informatsiinoi bezpeky // Reiestratsiia, zberihannia i obrobka danykh. 2023. T. 25, № 2. S. 27–65. https://doi.org/10.35681/1560-9189.2023.25.2.300525