DOI: 10.20998/2079-0023.2024.01.11
УДК 004.9+519.85

В. О. ШАРОВ, аспірант кафедри інформаційних систем та технологій Національного технічного університету «Харківський політехнічний інститут», Харків, Україна; ORCID: https://orcid.org/ 0000-0003-3152-0650; e-mail: wyctpiy@gmail.com

О. М. НІКУЛІНА, д-р техн. наук, професор, завідувачка кафедри інформаційних систем та технологій Національного технічного університету «Харківський політехнічний інститут», Харків, Україна; ORCID: https://orcid.org/0000-0003-2938-4215; e-mail: elniknik02@gmail.com

ДВОРІВНЕВА КОНЦЕПЦІЯ ДЛЯ МОДЕЛЮВАННЯ ЄДИНОЇ ЗАВАДОСТІЙКОЇ ПЕРЕДАЧІ ЦИФРОВИХ ДАНИХ

У статті формалізується, створюється та надається для розглядання концепція єдиного безпечного завадостійкого каналу передачі цифрових даних. У сучасній теорії та практиці з кібербезпеки існує набір рекомендацій по зниженню ризиків для організацій NIST Cybersecurity Framework. Для того, щоб дані високого рівня були безпечними, висуваються вимоги для CIA-тріади, а саме до конфіденційності, цілісності та доступності інформації. Тому, у подальшому доцільність роботи та її результат напряму будуть залежати від задоволення виконання CIA-умов. Як відомо, дані високого рівня: як e-mail, візуальні дані у GUI різних додатків, тощо, передаються по каналам зв'язку низького рівня: як кабелі, бездротові канали радіозв'язку та інші. На кожному з рівнів для безпечної передачі інформації існують специфічні шкідники. На високих рівнях основною загрозою для інформації є людина та людський фактор. Чим нижче стає рівень передачі інформації, тим більше починає впливати природа, натуральні перепони і випадкові короткі явища. Для того, щоб користувач міг без загрози для конфіденційності, цілісності та доступності інформації користуватись різноманітними приладами, необхідно активно і безперебійно розробляти, вдосконалювати та покращувати вже існуючі способи захисту, відновлення, передачі та зберігання даних. Кожний аспект у цій боротьбі за безпеку є як і перевагою так і недоліком: надлишкова безпечність не доцільна для масового трафіку, складність не завжди надає відповідну захищеність і так далі. Тому важливим фактором постає оптимальність і доцільність методів, що використовуються для передачі даних. З цих причин, у роботі пропонується відносно простий, але не менш ефективний від того підхід для збереження CIA-вимог.

Ключові слова: завадостійкість, завадостійкі коди, безпека даних, канали передачі даних, VPN, CIA, NIST, OWASP.

Вступ. Розвиток моделей і методів забезпечення безпеки цифрової інформації є надзвичайно важливим напрямком інформаційних технологій, пов'язаним із захистом особистих даних, фінансової інформації, інтелектуальної власності та загальною безпекою держав і організацій. Відсутність належної безпеки для інформації може спричинити великі ризики від втрати інформації і негативні наслідки від її використання супротивниками [1–3].

Важливим є забезпечення безперервного удосконалення засобів безпеки цифрової інформації, адже це забезпечує захист особистих даних, фінансів, інтелектуальної власності, підтримання операційної та національної безпеки.

Захист особистих даних забезпечує конфіденційність та приватність інформації. Конфіденційність полягає у забезпечення того, що особисті дані користувачів (медичні записи, фінансові дані, адреси) залишаються конфіденційними і не потрапляють до рук зловмисників. Право на приватність надає користувачам можливість контролювати доступ до їхніх особистих даних та їх використання.

Захист фінансів забезпечує захист від крадіжок та шахрайства. Захист від крадіжок протидіє хакерам, які можуть отримати доступ до банківських рахунків, кредитних карток, криптовалютних гаманців, що може призвести до фінансових втрат для окремих осіб та організацій. Безпека даних допомагає запобігти фінансовим шахрайствам, які можуть бути вчинені через викрадену інформацію.

Захист інтелектуальної власності забезпечує захист комерційних таємниць і збереження конкурентних переваг. Комерційна таємниця даних повинна забезпечуватись, тому що багато компаній мають інтелектуальну власність (патенти, авторські права, комерційні таємниці), яка є критично важливою для їхнього успіху на ринку. Конкурентні переваги надаються шляхом захисту інформації про розробки, дослідження та стратегії компаній від конкурентів.

Підтримання операційної безпеки забезпечує безперервність бізнесу і протидіє репутаційним ризикам. Безперервність бізнесу може бути порушена тим, що витоки даних можуть призвести до зупинки роботи компаній, порушення логістичних ланцюгів та інших операційних проблем. Витік або компрометація даних може серйозно пошкодити репутацію компанії або організації та привести до репутаційних ризиків.

Підтримання національної безпеки протидіє кібертероризму і шпигунству. Держави та організації можуть бути атаковані хакерами з метою порушення роботи критичної інфраструктури, таких як енергетичні системи, транспорт, фінансові системи. Викрадення державних та військових секретів може поставити під загрозу національну безпеку та суверенітет країни.

При відсутності безпеки для інформації, будь-яка організація сприяє підвищенню ризиків, серед яких кіберзлочини, масові витоки інформації, фінансові збитки, порушення приватності, конкурентних переваг.

Кіберзлочини – витоки даних, зломи, шантаж та інші форми кіберзлочинності, які можуть спричинити фінансові втрати та шкоду репутації.

Масові витоки інформації, що можуть призвести до розголошення особистих даних мільйонів

користувачів, що може спричинити масштабні юридичні наслідки та втрату довіри.

Фінансові збитки – витрати на ліквідацію наслідків атак, штрафи за недотримання законодавства про захист даних (наприклад, GDPR в Європі), втрати від крадіжок і шахрайств.

Порушення приватності – неконтрольований доступ до особистих даних може призвести до порушення приватного життя користувачів, шантажу та інших форм зловживань.

Втрата конкурентних переваг – викрадення або компрометація інтелектуальної власності може призвести до втрати конкурентних переваг на ринку.

Отже, робота над безпекою цифрової інформації є критично важливою для захисту даних, забезпечення безперервності бізнесу, збереження конкурентних переваг та загальної безпеки суспільства [2, 3].

Мета та задачі дослідження. Мета даної статті полягає у аналізі способів підтримання безпеки передачі інформації, розробці моделі єдиної концепції безпечної та завадостійкої передачі даних для інформаційної технології оптимізації управління динамічними системами.

Для досягнення мети поставлені задачі дослідження:

1) проаналізувати перешкоди для безпечної передачі даних;

2) проаналізувати методи боротьби з перешкодами;

3) розробити модель захисту цифрової інформації від усіх типів перешкод.

Перешкоди безпечної передачі даних та методи захисту. Перепони для цілісної та конфіденційної передачі інформації можуть бути як штучними так і натуральними. Штучні перешкоди виникають переважно, коли зловмисники втручаються в процес передачі інформації. Натуральні перешкоди відбуваються коли сигнал, що передається, затухає при передачі, трапляються помилки при кодуванні, тощо.

Перешкоди для безпечної передачі цифрових даних можуть включати різні загрози, вразливості та технічні проблеми [3].

Загрози та вразливості створюються кіберзлочинцями, зловмисним програмним забезпеченням, перехопленням даних. Хакери використовують вразливості в програмному забезпеченні або мережах для несанкціонованого доступу до даних. Фішинг виконується шахрайськими методами для обману користувачів з метою отримання конфіденційної інформації, такої як паролі або фінансові дані.

Зловмисне програмне забезпечення – віруси, трояни, руткіти може викрадати або пошкоджувати дані. Шкідливе програмне забезпечення-вимагач (Ransomware) блокує доступ до даних і вимагає викуп за їх відновлення;

В інформаційних атаках типу «людина посередині» зловмисники перехоплюють і змінюють дані, що передаються між двома сторонами. Може бути підслуховування та нелегальне перехоплення комунікацій через незашифровані канали [1, 4].

Технічні проблеми та вразливості виникають через незашифровані з'єднання, слабкі або застарілі алгоритми шифрування, недостатню автентифікацію та авторизацію, вразливі програмні забезпечення та апаратні засоби.

У незашифрованих з'єднаннях передача даних виконується через незахищені канали, такі як HTTP замість HTTPS, що робить їх вразливими до перехоплення.

Використання слабких або застарілих алгоритмів шифрування (наприклад, MD5 або SHA-1) може призвести до легкого зламу даних.

Слабкі або відсутні механізми автентифікації та авторизації можуть дозволити зловмисникам отримати доступ до системи.

Вразливі програмні забезпечення та апаратні засоби такі як баги та експлойти в програмному забезпеченні або апаратних засобах можуть бути використані для отримання доступу до даних.

Організаційні та людські фактори також впливають не безпеку передачі даних. Відсутність освіти та навчання користувачів, недостатня обізнаність про безпеку даних може призвести до помилок, таких як використання слабких паролів або відкриття фішингових електронних листів. Порушення політик та процедур безпеки, таких як незахищене зберігання даних або обмін конфіденційною інформацією через незахищені канали, а також інсайдерські загрози, ненавмисні або зловмисні дії працівників або інших інсайдерів, які мають доступ до конфіденційної інформації зменшують безпеку передачі даних [3].

Природні та техногенні фактори також впливають на безпеку передачі даних. Перебої в електропостачанні можуть призвести до втрати даних або пошкодження обладнання. Природні катастрофи – пожежі, повені, землетруси можуть пошкодити фізичну інфраструктуру, в якій зберігаються або передаються дані. відмова апаратного забезпечення. Вихід з ладу серверів, мережевого обладнання або інших критичних компонентів може призвести до втрати або порушення передачі даних. Природні перешкоди у каналах передачі даних викликають затухання сигналів, магнітні перешкоди, перекручування бітів, дроблення сигналу, фазовий зсув.

Проти подібних загроз існують наступні методи захисту: шифрування даних, регулярне оновлення програмного забезпечення, двофакторна аутентифікація, навчання та освіта користувачів, використання VPN і завадостійких кодів.

Шифрування даних використовує сучасні методи шифрування для захисту даних під час передачі та зберігання:

- регулярне оновлення програмного забезпечення – встановлення останніх патчів та оновлень для усунення вразливостей;
- двофакторна аутентифікація – використання додаткових методів аутентифікації для підвищення безпеки доступу;
- навчання та освіта користувачів – постійне навчання працівників щодо кращих практик безпеки;

- використання VPN – створення захищених тунелів для передачі даних через незахищені мережі;
- використання завадостійких кодів – кодування даних завадостійкими комбінаціями, які за рахунок введення надлишковості можуть ігнорувати певні помилки, які трапляються у фізичних каналах зв'язку.

Всі ці заходи допомагають знизити ризики та забезпечити безпечну передачу цифрових даних [1, 4].

Постановка задачі. У роботі розглядається саме процес передачі інформації, тому основними перепонами для нього будуть саме перешкоди штучні, створені людиною на високому апаратному рівні, а також натуральні природні явища в каналах передачі даних. Для них шифрування даних і використання VPN – для високого рівня, а також завадостійкі коди – для фізичного рівня являються одними з найбільш ефективних методів, тому їх дослідження та інтеграція у одну систему може значно спростити і покращити умови для безпечної передачі даних. З цієї причини розробка єдиної моделі, яка поєднувала б безпекові протоколи та підходи у один алгоритм є актуальним.

Верхній рівень концепції. Оскільки перепони для збереження конфіденційності, цілісності та доступності інформації можуть виникати на різних рівнях, необхідно обрати методи боротьби, які будуть захищати інформацію на кожному етапі її передачі. Для зручності, як орієнтир можно використовувати стандартну модель OSI. Одним з обраних методів боротьби з перешкодами – використання VPN.

VPN (Virtual Private Network) забезпечує захищений і приватний доступ до Інтернету, створюючи шифрований тунель між користувачем та віддаленим сервером. Основні принципи роботи VPN:

- шифрування трафіку – VPN використовує протоколи шифрування (наприклад, OpenVPN, IKEv2, IPSec) для захисту даних, що передаються між користувачем та VPN-сервером, це запобігає перехопленню даних третіми сторонами;
- маршрутизація трафіку через VPN-сервер, коли користувач підключається до VPN, його трафік перенаправляється через VPN-сервер, цей сервер виступає як посередник між користувачем та Інтернетом, приховуючи реальну IP-адресу користувача;
- приховування IP-адреси – VPN змінює IP-адресу користувача на адресу VPN-сервера, що забезпечує анонімність та допомагає обійти географічні обмеження доступу до контенту;
- аутентифікація – VPN використовують різні методи аутентифікації для перевірки користувачів, наприклад, логін-пароль, двофакторна аутентифікація, цифрові сертифікати.

Ефективність VPN можна оцінювати за кількома ключовими показниками.

Швидкість підключення може бути виміряна як різниця між швидкістю інтернет-з'єднання без VPN та зі включеним VPN.

$$\triangle V = (\frac{V - V_{\text{VPN}}}{V}) \times 100 , \quad (1)$$

де $\triangle V$ – зниження швидкості (%);

V – швидкість без VPN;

V_{VPN} – швидкість з VPN.

Затримка вимірюється як час (у мілісекундах), який потрібен для передачі даних від користувача до сервера і у зворотному напрямку:

$$D = \frac{t_f - t_b}{2} , \quad (2)$$

де D – затримка;

t_f – це час передачі даних до сервера;

t_b – це час повернення даних.

Надійність підключення вимірюється як кількість успішних підключень до VPN-сервера без розривів

$$R = \left(\frac{C_s}{C_o} \right) , \quad (3)$$

де R – надійність (%);

C_s – кількість успішних підключень;

C_o – кількість спроб підключень.

Час підключення вимірюється як середній час, необхідний для встановлення VPN-з'єднання.

$$T_{ca} = \frac{t_c}{C_o} , \quad (4)$$

де T_{ca} – середній час підключення;

t_c – загальний час підключення.

Ефективність шифрування – як рівень шифрування даних (наприклад, AES-256), який визначає складність зламування шифру.

Ефективність шифрування не має прямої формули, але можна враховувати довжину ключа та методи шифрування, що використовуються.

Тестування швидкості: використання інструментів на кшталт Speedtest для вимірювання швидкості Інтернету з VPN та без нього.

Моніторинг затримки – використання команд, таких як ping, для перевірки затримки між клієнтом та VPN-сервером.

Перевірка надійності тривалості та стабільності з'єднання протягом певного часу, фіксування випадків розриву.

Оцінка рівня шифрування технічної документації VPN-провайдера щодо використовуваних протоколів та методів шифрування.

Забезпечення ефективної роботи VPN є важливим для гарантування безпеки та приватності користувачів, а також для підтримання високої продуктивності та надійності з'єднань.

Після того як код шифрується та створюється VPN тунель, виникають вже суто фізичні перешкоди, які заважають швидкій, достовірній та безпечній передачі інформації. Для мінімізації наслідків ефективно використовуються завадостійкі коди.

Нижній рівень концепції. Щоб код можна було назвати завадостійким, він має надавати можливість для виявлення або виправлення різних помилок, що

можуть генеруватись при передачі даних з причини різноманітних завад. Можливість коду виявляти ці помилки отримується за допомоги введення надмірності в початкову інформаційну кодову комбінацію. Ті самі додаткові надмірні символи створюються за предписаними правилами і називаються перевірочними або контрольними. Збільшення числа надмірних символів у кодовій комбінації збільшує детективну і виправляючу властивості коду, але знижає швидкість передачі інформації [5–7].

Видів надлишковості може бути два: абсолютна та відносна. Абсолютну надлишковість можна визначити за допомогою кількості додаткових вводимих розрядів

$$k = n - m, \qquad (5)$$

де k – абсолютна надлишковість або кількість перевірочних елементів;

n – загальна кількість елементів у кодовій комбінації, довжина кодової комбінації;

m – загальна кількість інформаційних елементів у кодовій комбінації.

Нехай на вхід кодуючого пристрою надійшла деяка послідовність m інформаційних двійковий розрядів. На виході їй буде відповідати послідовність з n двійкових символів, де $n > m$. Усього може бути 2^m різних послідовностей з 2^n, які є дозволеними кодовими комбінаціями. Інші $2^n - 2^m$ з можливих вихідних послідовностей для передачі не використовуються, тому вони будуть називаються забороненими [7–10].

Завадостійких кодів зараз існує досить багато. На рис. 1 приводиться неповна ієрархія завадостійких кодів [9–11].

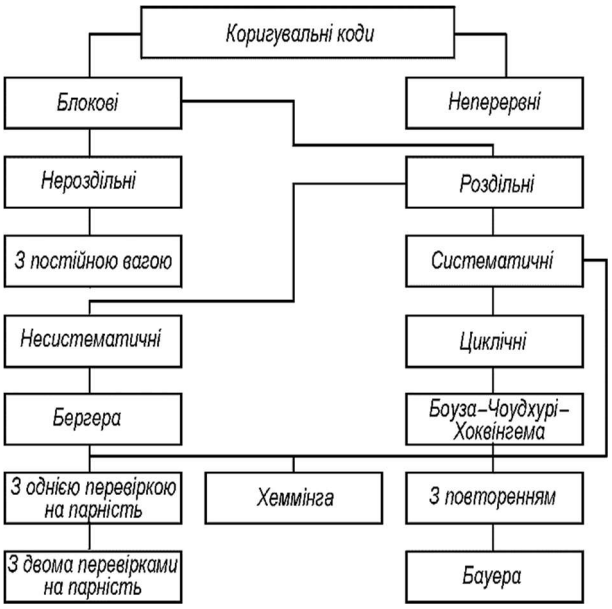

Рис. 1. Види завадостійких кодів

У роботах, що стосувались безпосередньо завадостійких кодів, було прийнято рішення розглядати і працювати з кодами Хеммінга з багатьох причин, у тому числі, тому що вони являються оптимальними для виконання поставлених у роботі завдань [5–7].

Оскільки просто використання кодів Хеммінга може бути недостатньо, було запропоновано використовувати каскадні коди.

Каскадний код, у нашому випадку, буде використовувати паралельний, блоковий, систематичний код Хеммінга, який здатен виправляти помилки, що виникають при передачі цифрової інформації каналом зв'язку з шумами – як першу ступінь, а у якості другого ступеня буде простий та надійний код (біт) перевірки кодової комбінації на парність.

Тобто, каскадні коди складаються з двох або більше, менших за розміром і простіших кодів. Головна ідея каскадного коду, у тому числі у нашій моделі, полягає у тому, що початкове інформаційне повідомлення повідомлення кодується кодером 1, потім це повідомлення з додатковими бітами першого завадостійкого коду кодується поверх кодером 2. При декодуванні процес зазначений процес виконується у зворотному порядку.

Поширену схему каскадних кодів можна побачити на рис. 2 [12].

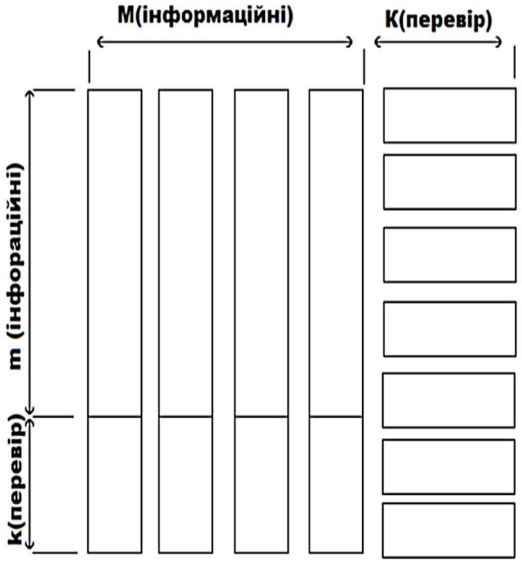

Рис. 2. Загальна схема каскадного коду

Поширена схема-алгоритм для кодування та декодування каскадним кодом наведена на рис. 3 [13, 14].

Об'єднання двох рівнів концепції. Для того, щоб була можливість оцінити та візуалізувати поєднання двох рівнів безпеки, запропоновано використовувати модель OSI.

На рис. 4 VPN протоколи SSL, IPSec, PPTP, L2TP поєднуються у єдиному контурі безпеки з завадостійкими кодами.

Висновки. Об'єднання двох рівнів боротьби з перешкодами для конфіденційної, достовірної та доступної передачі інформації надає переваги у плануванні та керуванні різними системами, адже в умовах динамічних завад дозволяє оцінити та швидко імплементувати вже готові методи, які на практиці довели свою надійність і є доступними для кожного, адже всі базові протоколи-фреймворки з кібербезпеки є відкритими для використання і впровадження, а

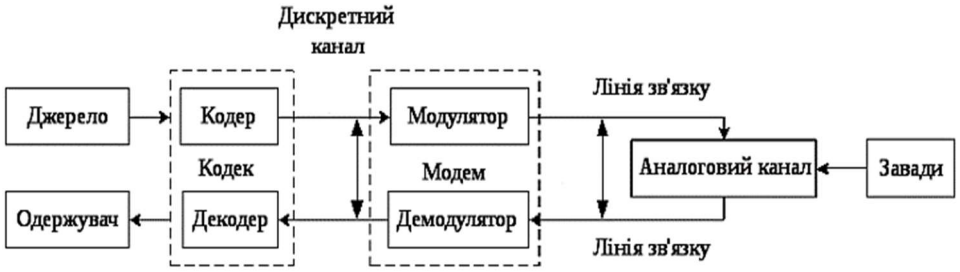

Рис. 3. Загальна схема кодування та декодування

завадостійкі коди є досить легкими, логічними й доступними для реалізації у широкому спектрі систем управління. Подальше дослідження, уточнення та покращення ідеї є актуальним.

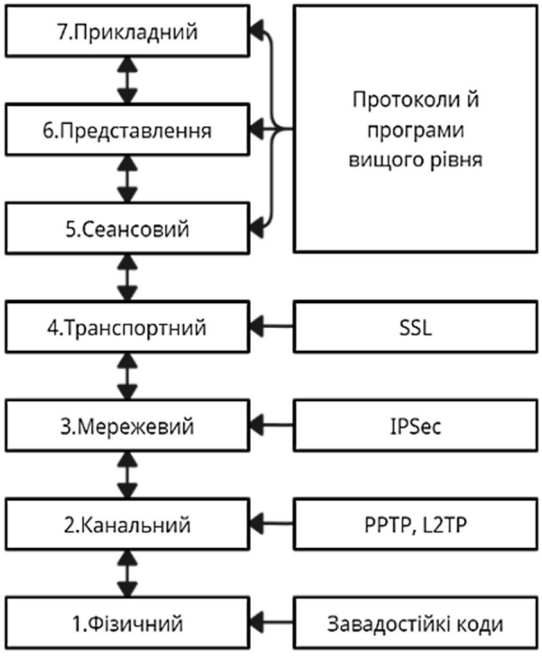

Рис. 4. Ключові елементи концепції на моделі OSI

Список використаної літератури

1. Nieles M., Dempsey K., Pillitteri V. Y. *An Introduction to Information Security. National Institute of Standards and Technology Special Publication 800-12 Revision 1, June 2017*. 101 p. URL: https://nsarchive.gwu.edu/document/22632-document-07-michael-nieles-kelley-dempsey-and (дата звернення: 25.04.2024).
2. Stallings W., Brown L. *Computer Security : Principles and Practice*. New Jork: Prentice Hall, 2008. 817 p.
3. Pfleeger C. P., Pfleeger S. L. *Security in Computing*. New Jersey: Prentice Hall, 2003. 746 p.
4. Tiller J. S. *The Ethical Hack: A Framework for Business Value Penetration Testing*. Auerbach Publications, 2005. 352 p.
5. Шаров В. О., Нікуліна О. М., Северин В. П. Моделювання та аналіз кодерів завадостійких каскадних кодів для динамічних систем. *Вісник Національного технічного університету «Харківський політехнічний інститут»: сб. наук. пр. Темат. вип.: Системний аналіз, управління та інформаційні технології*. Харків: НТУ «ХПІ», 2023, № 1 (9). С. 64–69.
6. Шаров В. О., Нікуліна О. М., Северин В. П. Розробка моделі завадостійкої передачі даних для інформаційної технології оптимізації управління динамічними системами. *Вісник Національного технічного університету «Харківський політехнічний інститут» »: сб. наук. пр. Темат. вип.: Системний аналіз, управління та інформаційні технології*. Харків : НТУ «ХПІ», 2022, № 2 (8). С. 57–62.
7. Шаров В. О., Нікуліна О. М., Лошкарьова С. Є. Розробка гнучкої моделі завадостійкої передачі даних для управління динамічними системами. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: Тези доповідей XXXI міжнародної науково-практичної конференції MicroCAD-2023*. Харків: НТУ «ХПІ», 2023. С. 1048
8. Захарченко Н. В., Горохов С. М., Кочетков А. В. *Інформаційні параметри позиційних кодів*. Одеса: ОНАС, 2018. 212 с.
9. Eklund J.-E., Arvidsson R. A multiple sampling, single A/D conversion technique for I/Q demodulation in CMOS. *IEEE Journal of Solid-State Circuits.* 1996. Vol. 31, is. 12. P. 1987–1994.
10. Blahut R. E. *Theory and Practice of Error Control Codes*. Addison-Wesley Publishing Company, 1983. 500 p.
11. Лосев Ю. І., Шматков С. І. Основи теорії передачі інформації. Харків: ХНУ ім. В. Н. Каразіна, 2013. 290 с.
12. Yue Tang, Tian Mao, Bing Jiang, Design and Experiment of Multi-resolution Composite Digital Array Antenna. *Journal of Radars*. 2016, 5 (3). P. 265.
13. Банкет В. Л., Іващенко П. В., Іщенко М. О. Завадостійке кодування в телекомунікаційних системах. Одеса: ОНАЗ ім. О. С. Попова, 2011. 100 с.
14. Жураковськй Ю. П., Полторак В. П. Теорія інформації та кодування. Київ: Вища шк., 2001. 255 с.
15. Кожевников В. Л., Кожевников В. Л. Теорія інформації та кодування. Дніпропетровськ: НГУ, 2011. 108 с.

References (transliterated)

1. Nieles M., Dempsey K., Pillitteri V. Y. *An Introduction to Information Security. National Institute of Standards and Technology Special Publication 800-12 Revision 1, June 2017*. 101 p. Available at: https://nsarchive.gwu.edu/document/22632-document-07-michael-nieles-kelley-dempsey-and (accessed 25.04.2024).
2. Stallings W., Brown L. *Computer Security : Principles and Practice*. New Jork, Prentice Hall, 2008. 817 p.
3. Pfleeger C. P., Pfleeger S. L. *Security in Computing*. New Jersey, Prentice Hall, 2003. 746 p.
4. Tiller J. S. *The Ethical Hack: A Framework for Business Value Penetration Testing*. Auerbach Publications, 2005. 352 p.
5. Sharov V. O., Nikulina O. M., Severyn V. P. Modelyuvannya ta analiz koderiv zavadostiikyh kodiv dlya dynamychnykh system [Modeling and analysis of coders of secure cascade codes for dynamic systems]. *Vestnik Nats. tekhn. un-ta "KhPI": sb. nauch. tr. Temat. vyp.: Sistemnyy analiz, upravlenie i informatsionnye tekhnologii* [Bulletin of the National Technical University "KhPI": a collection of scientific papers. Thematic issue: System analysis, management and information technology]. Kharkiv, NTU "KhPI", Publ., 2023, no.1 (9), pp. 64–69. (In Ukr.).
6. Sharov V. O., Nikulina O. M., Severyn V. P. Rozrobka modeli zavadostiykoji peredachi danyh dlja informatsiynoji tekhnologiji optymizatsii upravlinnja dynamichnymy sistemamy [Development of a data transfer model for information technology optimization of dynamic systems control]. *Vestnik Nats. tekhn. un-ta "KhPI": sb.*

nauch. tr. Temat. vyp.: Sistemnyy analiz, upravlenie i informatsionnye tekhnologii [Bulletin of the National Technical University "KhPI": a collection of scientific papers. Thematic issue: System analysis, management and information technology]. Kharkiv, NTU "KhPI", Publ., 2022, no. 2 (8), pp. 57–62. (In Ukr.).
7. Sharov V. O., Nikulina O. M., Loshkaryova S.E. Rozrobka gnuchkoi modeli zavadostiikoi peredachi danyh dlya upravlinnya dynamychnymy systemamy [Development of a flexible model of data transmission for controlling dynamic systems]. *Information technologies: science, engineering, technology, education, health: Abstracts of the XXXI International Scientific and Practical Conference MicroCAD-2023*. Kharkiv, NTU "KhPI", Publ., 2023, p. 1048. (In Ukr.).
8. Zakharchenko N. V., Gorokhov S. M., Kochetkov A. V. *Informatsijni parametry pozitsijnyh kodiv* [Information parameters of positional codes]. Odesa, ONAS Publ., 2018. 212 p. (In Ukr.).
9. Eklund J.-E., Arvidsson R. A multiple sampling, single A/D conversion technique for I/Q demodulation in CMOS. *IEEE Journal of Solid-State Circuits*. 1996, vol. 31, is. 12, pp. 1987–1994.
10. Blahut R. E. *Theory and Practice of Error Control Codes*. Addison-Wesley Publishing Company, 1983. 500 p.
11. Losev Yu. I., Shmatkov S. I. *Osnovy teotiji peredachi informatsiji* [Fundamentals of the theory of information transfer]. Kharkiv, KhNU named V. N. Karazina Publ., 2013. 290 P. (In Ukr.).
12. Yue Tang, Tian Mao, Bing Jiang Design and Experiment of Multi-resolution Composite Digital Array Antenna. *Journal of Radars*, 2016, 5 (3). pp. 265.
13. Banket V. L., Ivashchenko P. V., Ishchenko M. O. *Zavadostijke koduvannja v telekomunatsijnyh systemah* [Interference-resistant coding in telecommunication systems]. Odesa, ONAZ named O. S. Popova Publ., 2011. 100 P. (In Ukr.).
14. Zhurakovsky Yu. P., Poltorak V. P. *Teorija informatsiji ta koduvannja* [Theory of information and coding]. Kyiv, Vyshcha shk. Publ., 2001. 255 p. (In Ukr.).
15. Kozhevnikov V. L., Kozhevnikov V. L. *Teorija informatsiji ta koduvannja* [Theory of information and coding]. Dnipropetrovsk: NGU Publ., 2011. 108 p. (In Ukr.).

Надійшла (received) 06.05.2024

UDC 004.9+519.85

V. O. SHAROV, Postgraduate of Department Information Systems and Technologies National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0003-3152-0650; e mail: wyctpiy@gmail.com
O. M. NIKULINA, Doctor of Technical Sciences, Associate Professor, Head of Department Information Systems and Technologies National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0003-2938-4215; e mail: elniknik02@gmail.com

TWO-LEVEL CONCEPT FOR SIMULATING UNIFORM INTERFERENCE-RESISTANT DIGITAL DATA TRANSMISSION

The article formalizes, creates and provides for consideration the concept of a single secure interference-resistant data transmission channel. In modern cybersecurity theory and practice, there is the NIST Cybersecurity Framework, which is a set of recommendations for reducing risks for organizations. In order for high-level data to be secure, there are requirements for the SIA triad, namely confidentiality, integrity and availability of information. Therefore, in the future, the expediency of the work and its result will directly depend on the satisfaction of the SIA conditions. As you know, high-level data: such as e-mail, visual data in the GUI of various applications, etc., are transmitted over low-level communication channels: such as cables, wireless radio communication channels, and others. At each of the levels for safe transmission of information, there are specific pests. At high levels, the main threat to information is man and the human factor. The lower the level of information transmission becomes, the more nature, natural obstacles and random short phenomena begin to influence. In order for the user to be able to use various devices without a threat to the confidentiality, integrity and availability of information, it is necessary to actively and continuously develop, improve and improve the existing methods of data protection, restoration, transmission and storage. Each aspect in this struggle for security is both an advantage and a disadvantage: excessive security is not appropriate for mass traffic, complexity does not always provide adequate security, and so on. Therefore, the optimality and expediency of the methods used becomes an important factor. For these reasons, the paper proposes a relatively simple, but no less effective approach to maintaining SIA requirements.

Keywords: noise immunity, immunity codes, data security, data channels, VPN, CIA, NIST, OWASP.

Повні імена авторів / Author's full names

Автор 1 / Author 1: Шаров Владислав Олегович / Sharov Vladyslav Olegovych
Автор 2 / Author 2: Нікуліна Олена Миколаївна / Nikulina Olena Mykolaivna