Представлено нову модифікацію класичної криптосистеми McEliece на основі коригуючих кодів системи залишкових класів. Використання СЗК з розширеною системою модулів забезпечує ефективну корекцію помилок і тим самим підвищує складність до атак.

1. Classic McEliece. URL: https://classic.mceliece.org/impl.html (дата звернення: 30.04.2025).
2. Singh, Harshdeep. Code based cryptography: Classic mceliece. arXiv preprint arXiv:1907.12754, 2019.
3. Xiao, H., Garg, H. K., Hu, J., & Xiao, G. New error control algorithms for residue number system codes. *Etri Journal*, 2016, *38*(2), pp. 326-336.

Транспортна інформаційно-комунікаційна мережа як об'єкт кіберзагроз

УДК 004.056.5:004.08

Родіон Хворостяний

Державний університет інформаційно-комунікаційних технологій,
rodionhvorostyanoy@gmail.com

У сучасних умовах гібридної війни та відкритих військових дій кіберзагроз та пов'язані з ними кібератаки стають невід'ємною складовою збройного протистояння. Зі зростанням напруження в інформаційному та кіберпросторі фіксується значне зростання кількості кібератак, які спрямовані як на критичну інфраструктуру, так і на інформаційні системи державного та приватного секторів. Одним з елементів таких інформаційних систем є транспортні інформаційно-комунікаційні мережі регіонального та глобального рівня передачі даних.

Транспортна інформаційно-комунікаційна мережа - це мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу. Під терміном транспортної інформаційно-комунікаційної мережі (ТрІКМ) приймемо сукупність інформаційних систем, корпоративний мереж та каналів передачі інформації, а також способів комунікації та управління інформаційними потоками, призначеними для передачі інформації між великими регіонами в межах однієї держави, чи в межах міждержавного обміну даними на рівні глобальних світових регіонів [1].

Типова побудова регіональної ТрІКМ подана на Рис 1. Її складовими є верхній рівень магістральної транспортної мережі глобальної передачі даних, місцева транспортна мережа забезпечення даними окремих корпоративних мереж та рівень транспортної мережі доступу [1].

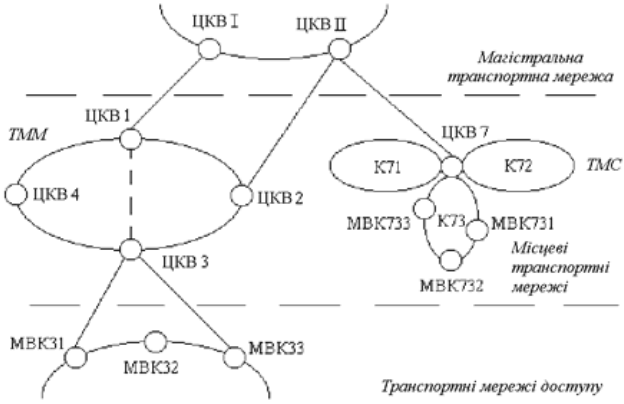

Рис.1 Структура регіональної (місцевої) транспортної мережі.

Її складовими є цифрові комутаційні вузли (ЦКВ), мультиплексори виділення каналів передачі даних (МВК), концентратори потоків передачі даних (К) та окремі корпоративні мережі передачі даних (ТММ, ТМС).

Класично в ТрІКМ виділяють чотири рівні [1]:

1. Рівень мережі – відповідає за взаємодію вузлів ІКС.

2. Рівень операційних систем – відповідає за обслуговування програмного забезпечення, яке реалізує вищі рівні, та його взаємодію з обладнанням мережі.

3. Рівень систем управління базами даних (СУБД) - відповідає за збереження ня та обробку даних.

4. Рівень прикладного програмного забезпечення – включає прикладні компоненти та інтерфейс взаємодії з користувачем.

Необхідно відмітити, що ТрІКМ обробляють різноманітні види трафіку. До яких можна віднести: трафік реального часу, потоковий трафік, еластичний трафік, сигнальний трафік. Тобто виникає потреба в захисті кожного з вказаних видів трафіку від цільових кібератак [1,2].

Відповідно до НД ТЗІ 2.5-005-99 [9] ТрІКС являє собою організаційно - технічну систему, яка поєднує операційну систему (ОС), фізичне середовище, персонал та оброблювану інформацію [3]. Кожна з цих складових безпосередньо впливатиме на загальний рівень захищеності, мати набір характеристик, вимог щодо налаштування та організації функціонування системи її кіберзахисту.

Аналіз та оцінка сучасного стану кібербезпеки України, дослідження механізмів захисту національної безпеки від кібератак та аналіз сучасного її стану показує, що як глобальні так і регіональні ТрІКМ можуть стати об’єктом кіберзагроз різного характеру [4,5]. Виходячи з призначення, типової топології побудови та складових елементів в якості кіберзагроз для ТрІКМ визначимо наступні, що подані в Табл. 1 [4,5].

Таблиця 1.

Типи кіберзагроз транспортної інформаційно-комунікаційної мережі

Тип кіберзагрози	Мета атаки, тип	Об'єкт атаки	Тип трафіку
Порушення доступності	Оприманння доступу до ТрІКМ. DDoS - атака	Сервери, локальні мережі	Трафік реального часу
Порушення конфіденційності	Перехопленння конфіденційних даних. Скіфінг, фішинг	Бази даних, інформаційні сховища, файли	Потоковий трафік
Блокування систем захисту	Виведення з ладу або знищення обладнання захисту. Поширення шкідливого ПЗ	Засоби управління кіберзахистом, міжмережеві екрани, маршрутизатори	Мережевий трафік (ICMP). Прикладний трафік (SMPT, SIP, H323)
Використанння вразливостей	Застосування експойлерів. SQL-ін'єкції, кібершпигунство	Веб-додатки, хмарні сервіси	Прикладний трафік (HTTP, SQL) Мережевий трафік (IP) Транспортний трафік (TCR)

Вирішення задання забезпечення кібернетичної безпеки ТрІКМ не можливо без наявності та використання відповідних моделей кіберзахисту. В свою чергу процес розробки такої моделі повинен врахувати види кіберзагроз, типи кібератак та об'єкти, що під них можуть потрапити. Базовим матеріалом, який може бути використаний для розробки такої моделі є інформація, що подана в Табл.1.

Таким чином, в роботі визначено термін транспортної інформаційно-комунікаційної мережі, як об'єкти впливу кіберзагроз, подані їх основні види, типи кібератак, що використовуються для їх реалізації, об'єкти впливу кібератак та види трафіку потоків даних через які реалізуються подані кіберзагрози.

1. http://vnstele.com/system-komut/lecz-ok/102-44-lecz-ok.html
2. https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf

3. НД ТЗІ 2.5-005 -99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

4. Mynenko, S., Kochnieva, V., & Babych, Y. (2024). Оцінка рівня кібербезпеки України в умовах війни. *Європейський науковий журнал Економічних та Фінансових інновацій*, *2*(14), 487-500. https://doi.org/10.32750/2024-0243

5. Толкачов М. Ю Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, №4 (2024), С. 85-99. DOI: 10.31673/2409-7292.2024.040009

Аналіз механізму впливу імпульсної нефлуктаційної завади на цілісність дискретного сигналу, що передається інформаційно-комунікаційною мережею

УДК 004.056.5:004.08

Євген Бондаренко
Державний університет інформаційно-комунікаційних технологій,
bondarenko.alfa.inet@gmail.com

У сучасних умовах гібридних війни та відкритого військового протистояння надзвичайно важливим є збереження цілісності корисної інформації в умовах впливу різноманітних завад та збурень по всьому спектру каналів інформації.

Особливо важливе це відносно радіоканалів передачі корисних даних в умовах впливу різноманітних завада різного характеру [1].

Відомо, що в сучасних радіоканалах поряд із шумовими завадами (релєєвське завмирання, адитивний білий гауссівський шум) часто присутні й нефлуктуаційні завади від різних джерел. Це можуть бути як природні причини формування різних радіо шумів, так і похибки радіоапаратури та порушенням технології радіозв'язку. Необхідно прийняти до уваги, що поява нефлуктаційних завад в радіопросторі передачі дискретних сигналів може обумовлюватися не тільки природніми причинами але і через навмисні дії протиборчої сторони, яка прагнуть створити певні перешкоди для роботи радіоканалу передачі цифрових даних [2].

Встановлено, що основними та найбільш небезпечними для порушення цілісності дискретних сигналів нефлуктаційними завадами є гармонічна завада, фазоманіпульована завада, ретрансльована завада, скануюча завада, хаотична імпульсна завада, мультиплікативна завада. Але, тільки при навмисно створеному прицільному впливі, саме імпульсна завада може нанести найбільшого порушення цілісності дискретному сигналу [2,4].

Вплив імпульсної завади проявляється в зростанні імовірності символьної помилки. Інтесивність впливу імпульсної завади загалом визначається спектром та енергією шуму, який оцінюється в загальних залежностях розрахунку символьної помилки співвідношенням сигнал/загальний шум в каналі передачі інформації.

Відповідно встановленим результатам проведених досліджень, мінімальна ймовірність помилки на символ дискретного сигналу з деяким типом модуляції *M* визначається залежністю [1,2]: