УДК 004.8
DOI: 10.31673/2409-7292.2025.015925

Партика О.О., Стефанків А.В., Наконечний Т.І.

ОСНОВНІ ЗАГРОЗИ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ РАДІОКАНАЛОМ ТА МЕТОДИ ЇЇ ЗАХИСТУ

У зв’язку зі стрімким розвитком і поширенням систем дистанційного керування, які використовують радіоканал для передачі команд, актуалізується питання забезпечення надійного захисту переданих даних. Такі системи активно застосовуються у багатьох галузях, зокрема, в автоматизованих системах управління доступом, домашній автоматизації, промисловості, медицині та у концепції інтернету речей. Популярність радіоканальних систем пояснюється низькою вартістю впровадження, простотою налаштування, відсутністю потреби у прокладанні кабельних ліній, що істотно спрощує їх експлуатацію та знижує початкові витрати на встановлення обладнання. Однак використання відкритого радіоканалу створює серйозні ризики інформаційній безпеці через доступність ефіру для перехоплення та втручання сторонніх осіб. Найбільш актуальними є загрози конфіденційності інформації (прослуховування і перехоплення переданих команд), загрози автентичності (атаки повторного відтворення, що дозволяють імітувати команди легітимних передавачів) та загрози цілісності даних (умисне або випадкове спотворення повідомлень у каналі передачі). Реалізація захисту ускладнюється обмеженими технічними характеристиками пристроїв дистанційного керування, що мають малі обчислювальні ресурси та енергетичні обмеження. У роботі проведено аналіз зазначених загроз та запропоновано комплекс ефективних методів захисту інформації. Рекомендується використання гібридних криптографічних схем, які поєднують симетричні та асиметричні криптоалгоритми з формуванням унікальних сесійних ключів для забезпечення конфіденційності передачі даних. Для захисту автентичності пропонується застосування часових міток і одноразових псевдовипадкових ідентифікаторів, що суттєво знижує ймовірність успішної реалізації атак повторного відтворення. Для забезпечення цілісності інформації рекомендовано застосовувати завадостійке кодування, зокрема, код Ріда-Соломона, який дозволяє не тільки виявляти, але й ефективно коригувати помилки, що виникають внаслідок зовнішніх впливів або навмисних втручань у роботу радіоканалу.

Ключові слова: дистанційне керування, радіоканал, шифрування, автентифікація, повторне відтворення, завадостійке кодування.

Вступ

Використання систем дистанційного керування з передачею команд через радіоканал з кожним роком набуває дедалі більшої популярності. Такий ріст можна пояснити зручністю розробки комплексів з використанням згаданих систем, простотою їхнього встановлення, налаштування та експлуатації. Окремим фактором зростання їхньої популярності є менші грошові витрати на встановлення у зв’язку з відсутністю необхідності проведення робіт з монтажу кабельних систем. На даний момент, такі системи керування використовуються для активації або дезактивації контрольованих пристроїв перешкод в складі автоматизованих систем управління доступом як заміна громіздким та менш гнучким проводовим системам, в системах домашньої автоматизації та інтернету речей.

Проте, використання систем дистанційного керування з бездротовою передачею команд призводить до виникнення певних загроз інформаційної безпеки. Основною вразливістю, яка породжує дані загрози, є загальна доступність ефірного простору для приймача, передавача та зловмисника. Площа роботи радіоканалу визначається двома основними параметрами системи: чутливістю приймача та вихідною потужністю передавача. Таким чином, зловмиснику буде достатньо просто втрутитися в роботу радіоканалу.

Формулювання проблеми

Однією з основних загроз безпеці комунікації між передавачем та приймачем системи дистанційного керування є атака повторного відтворення. Виконання такої атаки не вимагає від зловмисника суттєвого рівня знань та кваліфікації, а також використання дороговартісних технічних засобів. Оскільки для виконання атаки не потрібно виконувати довготривалу обробку або криптоаналіз перехопленого повідомлення, то така атака може бути виконана в польових умовах, наприклад, приховуванням трансивера в рюкзаці та управління ним за допомогою смартфону. В разі повного розкриття такої системи зловмисник отримує доступ до значної кількості закладених функцій, наприклад, керування всіма під’єднаними механізмами.

Огляд останніх досліджень і публікацій

Проблеми безпеки бездротової комунікації та безпеці інтернету речей в цілому є доволі добре вивченими, незважаючи на значну кількість протоколів та стандартів, які конкурують між собою та є взаємно несумісними. Зокрема, групою науковців з Університету Кардіффа було проведено аналіз вразливостей різних пристроїв класу інтернету речей, які використовують різні протоколи та радіочастотні діапазони, в переважній більшості – протоколи, які використовують діапазон ISM 2,4 ГГц [1].

Авторами статті було проведено попереднє дослідження вразливості до атак повторного відтворення на прикладі системи дистанційного керування, яка використовує протокол передачі даних PT2262 [2]. Одним з новітніх напрямків в галузі методів виявлення та запобігання атакам повторного відтворення є використання методів машинного навчання. Ці методи можуть застосовуватися як для виявлення повторень в засобах біометричної автентифікації, так і для систем інтернету речей [3]. Проте, використання методів машинного навчання для реальних систем дистанційного керування є недоцільним у зв'язку з обмеженнями обчислювальних потужностей.

Мета дослідження

Метою дослідження є огляд та аналіз методів підвищення рівня безпеки комунікації віддалених систем, аналіз можливостей їхньої імплементації в межах протоколу дистанційного керування та визначення загального принципу роботи такого протоколу.

Завдання дослідження

Дослідити можливі методи захисту систем дистанційного керування та інформації, що передається в них, від можливих атак на основні властивості інформації.

Структура та складові елементи системи дистанційного керування

Система дистанційного керування – це система, побудована з метою віддаленої активації одного або декількох пристроїв (виконавчих механізмів). Відповідно, така система складається з передавача команд, приймача команд та виконавчих механізмів.

Передавач, в свою чергу, складається з інтерфейсу користувача, блоку обробки та формування повідомлень і блоку передачі даних (Рисунок 1).

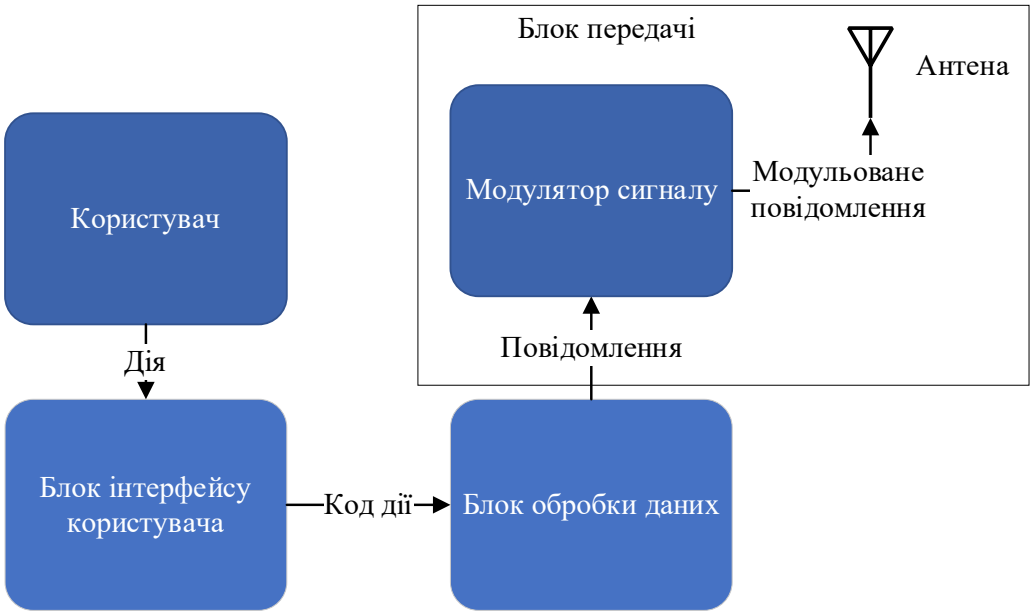

Рис. 1. Блок-схема передавача.

Блок інтерфейсу користувача забезпечує отримання команд від людини або іншого пристрою з метою їх передачі. Блок обробки та формування повідомлень виконує дії, необхідні для перетворення сигналу від блоку інтерфейсу в повідомлення стандартизованого

формату. Блок передачі даних виконує модуляцію даних та їхнє випромінювання в радіочастотний канал.

Приймач складається з блоків прийому даних, обробки повідомлень та взаємодії з виконавчими механізмами (рис. 2).

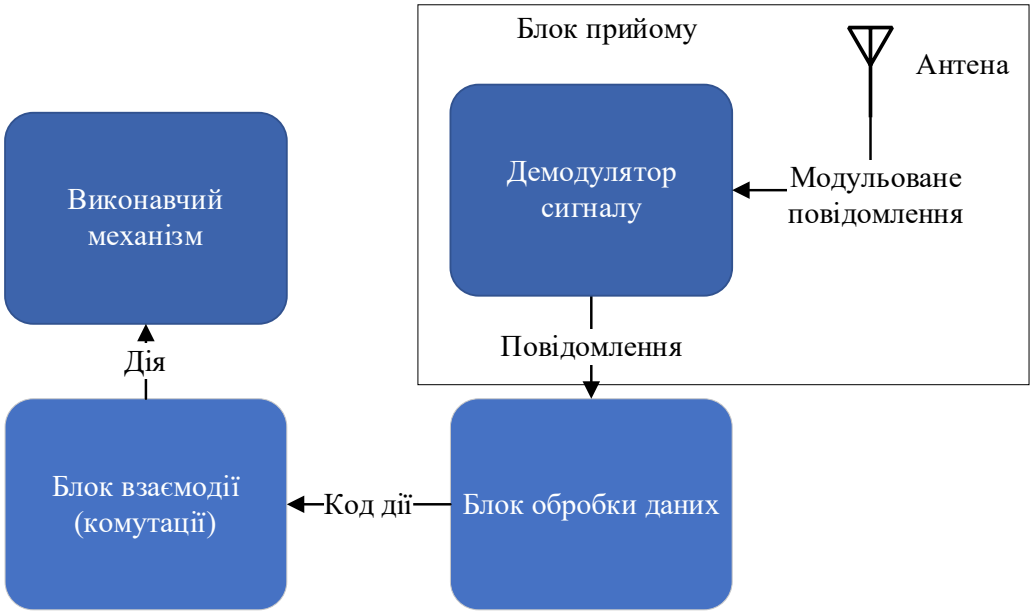

Рис. 2. Блок-схема приймача.

Блок прийому даних виконує демодуляцію вхідного сигналу та передає його блоку обробки. Блок обробки повідомлень виконує перетворення отриманих даних в набір вхідних даних та приймає рішення про активацію того чи іншого виконавчого механізму. Блок взаємодії з виконавчими механізмами виконує комутацію сигналів керування та/або живлення виконавчих механізмів відповідно до отриманих команд.

В якості виконавчих механізмів можуть виступати пристрої освітлення (лампи різних видів, світлодіодні набори), електромеханічні пристрої (реле, соленоїди, дверні електромагніти), контрольовані пристрої перешкод (турнікети, шлагбауми, ворота, двері тощо).

Загрози інформації при її передачі відкритими каналами

Для забезпечення захисту інформації при її передачі відкритими каналами, зокрема радіоканалом, необхідно розуміти вразливості, які можуть бути реалізовані з метою порушення властивостей цієї інформації. Можна виокремити наступні загрози інформації, які виникають у описаних умовах:

- Загрози конфіденційності:
  - Загрози прослуховування – захоплення зловмисником повідомлень комунікації з метою їхнього аналізу та отримання даних;
  - Загрози маніпуляції даними – зміна даних в процесі їхньої передачі каналом зв’язку з метою виконання дії від імені легітимного передавача.
- Загрози автентичності:
  - Загрози повторного відтворення – захоплення зловмисником повідомлень комунікації та їх ретрансляція через певний проміжок часу з метою імітації передавача;
- Загрози цілісності:
  - Загрози пошкодження даних – внесення зловмисником або навколишнім середовищем змін в зміст повідомлень, що призведе до неправильної роботи приймача та виконавчого механізму
- Загрози доступності:

© Партика О.О., Стефанків А.В., Наконечний Т.І. (2025). Основні загрози інформації при передачі радіоканалом та методи її захисту. Сучасний захист інформації, 1(61), 113–120. https://doi.org/10.31673/2409-7292.2025.015925.

- Загрози глушіння сигналу – внесення зловмисником шумових завад, які перевищують рівень корисного сигналу, внаслідок чого приймач втрачає здатність прийому цього сигналу; ця загроза може бути реалізована сумісно з загрозою повторного відтворення.

Загрози доступності знаходяться поза межами дослідження, оскільки вимагають розробки завадостійких апаратних рішень для передачі даних.

Вимоги до захищеного протоколу дистанційного керування

Захищений протокол дистанційного керування повинен забезпечувати надійну та захищену передачу команд від передавача до приймача з достатньою швидкодією. Необхідно забезпечити належний захист від описаних в попередньому пункті загроз конфіденційності та доступності. При цьому, з метою підвищення рівня безпеки, конфігурація приймача повинна відбуватися при кожному встановленні нової сесії роботи, тобто необхідно реалізувати метод віддаленої конфігурації приймача. Протокол повинен володіти засобами контролю цілісності повідомлень та виправлення помилок при передачі та отриманні.

Також необхідно враховувати специфічні обмеження систем дистанційного керування. Одним з них є суттєве обмеження доступних обчислювальних потужностей та обсягів постійної та оперативної пам'яті, викликане необхідністю обмеження енергоспоживання та габаритів. Також важливим є дотримання строгої моделі передачі даних в одному напрямку, викликане особливостями модулів прийому та передачі даних. Найпростіші системи дистанційного керування передбачають використання симплексного зв'язку. Дуплексний зв'язок може використовуватися для передачі статусу віддаленого механізму, проте реалізація дуплексного зв'язку потребує ускладнення апаратної складової системи та є невиправданим з точки зору необхідних функцій.

Засоби забезпечення конфіденційності інформації при її передачі відкритими каналами

Найбільш ефективними засобами захисту конфіденційності інформації є криптографічні перетворення. Проте, накладені обмеження суттєво впливають на вибір криптографічних алгоритмів, які можуть бути використані при розробці захищеного протоколу дистанційного керування. Зокрема, використання асиметричного шифрування для передачі даних є недоцільним у зв'язку з недостатньою швидкодією цих алгоритмів, викликаною використанням складного математичного апарату для шифрування та розшифрування. Також, використання протоколів асиметричного шифрування без криптографічного доповнення повідомлень, наприклад, за стандартом OAEP [4, 5], є небезпечним, оскільки в такому випадку не забезпечується семантична стійкість шифротексту [5]. Використання асиметричної криптографії з доповненням для віддаленого налаштування приймача є цілком виправданим з точки зору оптимізації швидкодії, оскільки цей етап необхідно виконувати лише один раз при встановленні сесії, при цьому основні дані будуть зашифровані за допомогою симетричного алгоритму.

Використання методів взаємного встановлення таємного значення, таких як варіації протоколу Діффі-Геллмана (в тому числі, з використанням математичного апарату еліптичних кривих), є неможливим у зв'язку з встановленим обмеженням напрямку передачі даних, тому передавач повинен в односторонньому порядку виконувати встановлення спільного сесійного ключа шифрування даних.

Огляд алгоритмів симетричного шифрування

Симетричні криптографічні алгоритми є основними засобами криптографічного захисту інформації завдяки своїй надійності та значній швидкодії в порівнянні з асиметричними алгоритмами, надійність яких заснована на теоретичній стійкості односторонніх математичних функцій (наприклад, дискретного логарифмування – алгоритм Ель-Гамаля [6] або факторизації великих чисел – RSA [7]) та які характеризуються значно меншими швидкостями обробки даних і більшою довжиною ключів. При цьому, довжина ключа шифрування даних повинна бути достатньою для забезпечення захисту повідомлень від

© Партика О.О., Стефанків А.В., Наконечний Т.І. (2025). Основні загрози інформації при передачі радіоканалом та методи її захисту. Сучасний захист інформації, 1(61), 113–120.
https://doi.org/10.31673/2409-7292.2025.015925.

криптоаналізу, але достатньо малою для підтримки максимального рівня швидкодії системи. Найбільш поширеними симетричними алгоритмами шифрування є AES [8], DES [9], Blowfish [10], Twofish [11] та IDEA [12].

Алгоритм DES на даний момент вважається небезпечним, оскільки було успішно розроблено апаратні засоби для його криптоаналізу. Потрійне шифрування даних 3DES дещо збільшує час криптоаналізу, проте основний алгоритм вважається застарілим та небезпечним. Алгоритм використовує ключі довжиною 64 біти (з яких ефективними є лише 56 бітів) та мережу Фейстеля. Алгоритм був національним стандартом в США до 1999 року, коли його було замінено шифром 3DES, а згодом, національним стандартом став шифр Rijndael, більш відомий як AES.

Найбільшу швидкодію серед представлених алгоритмів демонструють алгоритми сімейства Blowfish/Twofish. Алгоритми цього сімейства засновані на 16-раундовій мережі Фейстеля та пропонують поєднання продуктивності та безпеки. Проте, використання алгоритму Blowfish можна вважати небезпечним через недостатню довжину ключа у 64 біти. Ключі такої довжини є вразливими до атак «днів народження». Алгоритм Blowfish використовується для шифрування сховища ключів в криптографічній системі GnuPG [13].

Одним з найбільш відомих алгоритмів шифрування є AES. Цей алгоритм використовує SP-мережу з 4 функцій – ShiftRows, MixColumns, AddKey та SubBytes. Можливе використання ключів шифрування довжиною 128, 192 та 256 бітів. Надвисокий рівень захисту від криптоаналізу досягається навіть при використанні ключа довжиною 128 біт. Алгоритм підтримує безліч режимів роботи, зокрема ECB, CBC, CFB, OFB, GCM, EAX, XTS, CTR тощо. Перелік режимів роботи включає як просте шифрування, так і AEAD (автентифіковане шифрування з додатковими даними), що зменшує часові затрати на додаткову генерацію коду автентифікації повідомлення та значно збільшує захищеність даних. Цей алгоритм використовується державними органами США для шифрування інформації при зберіганні, а також такими програмними засобам, як dm-crypt [14], BitLocker [15] та VeraCrypt [16].

Альтернативою алгоритмам Blowfish, Twofish та AES є алгоритм IDEA, який використовує ключ шифрування довжиною 128 біт та блоки довжиною 64 біти. Алгоритм побудовано на основі схеми Лей-Массі, яка є модифікацією мережі Фейстеля. Використання коротких блоків даних може зменшити ефективність алгоритму в порівнянні з AES, який використовує блоки даних довжиною, відповідній довжині ключа шифрування. Даний алгоритм був захищений патентним правом, у зв’язку з чим не здобув значного розповсюдження. Зокрема, його було використано в програмному пакеті PGP.

Засоби захисту від атак повторного відтворення

Найбільш ефективними засобами захисту від атак повторного відтворення є алгоритми взаємної ідентифікації при передачі повідомлень, одноразові паролі або ідентифікатори, сесійні ключі шифрування та часові мітки. Проте, обмеження системи передачі даних симплексним зв’язком накладає значні обмеження на перелік можливих засобів. В системах дистанційного керування можливе використання двох основних методів захисту від атак даного класу: одноразові ідентифікатори та часові мітки. Для захисту цих міток від модифікації зловмисником необхідно виконувати їхнє шифрування при передачі.

Принцип роботи автентифікації за одноразовими ідентифікаторами полягає у використанні генераторів псевдовипадкових числових послідовностей (далі – ГПЧП) та криптографічних засобів перетворення даних (геш-функції, функції формування ключа) для перетворення чергового елемента числової послідовності в послідовність з високим рівнем ентропії. Отримана послідовність передається разом з повідомленням, сторона приймача генерує аналогічну послідовність та виконує перевірку збігу. У разі збігу повідомлення вважається достовірним. Надійність цього методу захисту залежить від надійності ГПЧП та його вразливості до атак [17, 18].

© Партика О.О., Стефанків А.В., Наконечний Т.І. (2025). Основні загрози інформації при передачі радіоканалом та методи її захисту. Сучасний захист інформації, 1(61), 113–120.
https://doi.org/10.31673/2409-7292.2025.015925.

При використанні методу часових міток до кожного повідомлення протоколу додається ідентифікатор, виведений за допомогою геш-функції або функції формування ключа зі значення часу формування повідомлення. При цьому, значення часу формування повідомлення повинно мати достатню кількість розрядів для безпомилкового визначення факту атаки. Кількість розрядів та межі дії мітки визначаються швидкодією процесора передавача та ступенем оптимізації програмної реалізації протоколу. З цього можна зробити висновок, що використання часових міток для малопотужних вбудованих рішень на мікроконтролерах є неоптимальним у зв'язку з необхідністю встановлення відносно великого часу дії мітки (одиниці секунд), що знижує стійкість до атак повторного відтворення автоматизованими засобами.

Засоби забезпечення цілісності інформації при передачі відкритими каналами

Головним чинником викликати пошкодження даних в процесі їх передачі радіоканалом є перевищення рівня «сигнал-шум», яке може бути викликане недостатньою потужністю передавача, недостатньою чутливістю приймача, перевантаженням приймача сторонніми сигналами в межах діапазону, перевантаженням приймача сторонніми сигналами на гармоніках, випромінювання зловмисником сигналів випадкової частоти або комбінацією перелічених факторів.

Найбільш ефективним методом виправлення помилок при передачі даних є застосування завадостійких кодів [19, с. 182]. Одним з найбільш універсальних завадостійких кодів є код Ріда-Соломона [19, с. 285], який знайшов безліч застосувань в сфері інформаційних технологій як при передачі даних (системи супутникового зв'язку, DVB, ATSC тощо), так і при їхньому зберіганні на носіях (жорсткі диски, RAID-масиви, оптичні диски, матричні коди тощо). Код Ріда-Соломона відноситься до сімейства систематичних циклічних кодів та є частковим випадком недвійкових кодів Боуза-Чоудхурі-Хоквінгема (БЧХ-кодів) [19, с. 262]. Недвійковість коду означає, що він працює не з бітами окремо, а з елементами поля Галуа, заданого генераторним поліномом (многочленом). Елементи поля Галуа можуть бути подані у вигляді бітових послідовностей, що дозволяє транслювати їх в символи різних систем кодування та навпаки.

Наприклад, розглянемо код RS(255,223) [20]. Параметри цього коду такі: $n = 255, k = 223, r = 32$. Цей код здатен виправляти до $t = 16$ помилок $(t = r/2)$ в повідомленні з довжиною корисної частини $k = 223$ символи. Код RS(255,223) оперує в полі $GF(2^8)$, елементи якого синтезуються примітивним многочленом восьмого ступеня $x^8 + x^4 + x^3 + x^2 + 1$. Твірним поліномом даного коду є послідовність $g(x) = (x + \alpha)(x + \alpha^2)(x + \alpha^3) \dots (x + \alpha^{31})(x + \alpha^{32})$. Коефіцієнти отримаємо шляхом розкриття поліному.

Кодування повідомлення виконується за систематичною схемою: шляхом ділення поліному повідомлення на твірний поліном зі зсувом r та заміною нульових символів, отриманих в результаті зсуву, на остачу від цього ділення. Також кодування можна представити у вигляді регістру зсуву з лінійним зворотним зв'язком (Рисунок 3). В процесі проходження даних через схему кодувальника при нижньому положенні вихідного перемикача вихід не змінюється, а вхідні дані додатково проходять через елементи регістру зсуву. Після входження останнього символу даних комірки регістру містять сформовану надлишкову частину.

Процес декодування складається з визначення синдрому помилки, побудови поліному помилки, його розв'язання та виправлення помилок [21]. Процес визначення синдрому помилки полягає в діленні поліному отриманого коду на поліном перевірки, і у разі виникнення ненульової остачі робиться висновок про наявність помилок в коді. Побудова поліному помилки може виконуватися за допомогою спеціалізованого алгоритму Берлекемпа-Мессі або за допомогою універсального алгоритму Евкліда. Пошук коренів поліному помилки виконується за допомогою процедури пошуку Цяня (Chien Search) [22]. Визначення позиції і характеру помилки проводиться за алгоритмом Форні [23], заснованим на формальному

диференціюванні. Отримана в результаті роботи алгоритму Форні маска помилки додається до пошкодженої кодової послідовності за правилами додавання елементів поля, після чого надлишкова частина відкидається. В результаті, отримуємо початкове повідомлення.

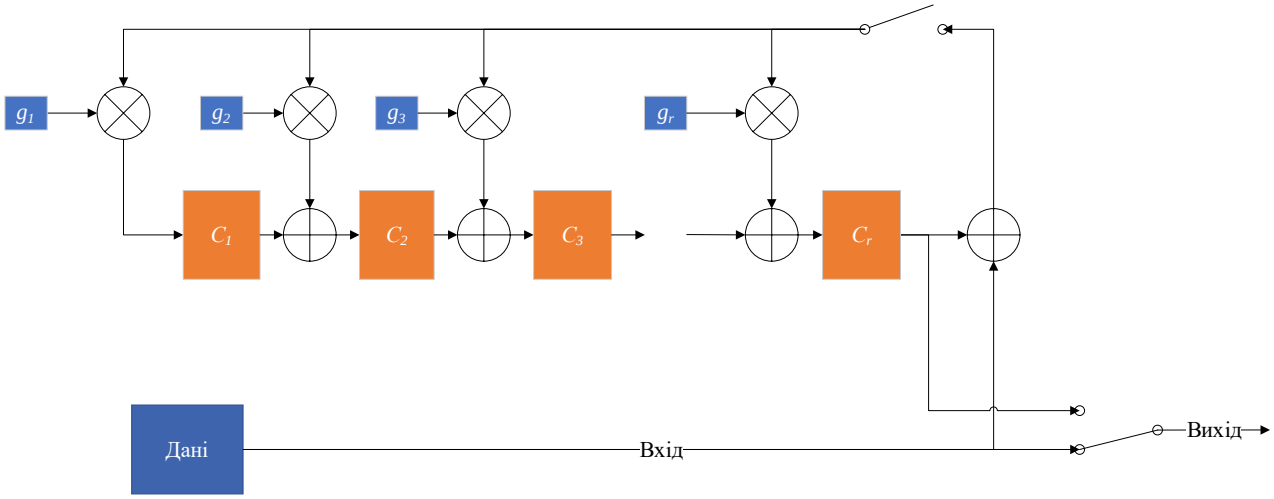

Рис. 3. Схема кодувальника коду Ріда-Соломона на основі регістру зсуву з лінійним зворотним зв'язком.

Застосування завадостійкого коду Ріда-Соломона дозволяє не тільки виявляти, але й виправляти помилки при передачі даних, тим самим, значно збільшуючи стійкість повідомлень до загроз пошкодження даних. Кодування може виконуватися для кожного пакету при передачі кожного фрагменту повідомлення (за умови використання модулів передачі даних з обмеженням довжини пакетів), для певних блоків повідомлення та для всього повідомлення.

Висновки

Використання радіоканалу для передачі даних має значні переваги з точки зору складності системи передачі. Водночас, у зв'язку з його відкритістю та загальністю він є вразливим до певного переліку атак, які можуть бути здійснені переважною більшістю зловмисників. При розробці пристроїв, які використовують радіоканал для комунікації, необхідно приділити увагу питанням конфіденційності даних та забезпечення доступності систем. Іншим джерелом загроз є навколишнє середовище, поточний стан якого може завадити безперебійній роботі такої системи, зокрема, призвести до порушення цілісності даних в процесі передачі. В даній роботі виокремлено основні загрози інформації при її передачі методи забезпечення конфіденційності, автентичності, цілісності даних та доступності компонентів системи. Дослідження методів забезпечення доступності знаходиться поза межами цього дослідження і є предметом для подальших досліджень.

Також в ході дослідження було проаналізовано методи захисту від атак повторного відтворення, доступні криптографічні алгоритми шифрування даних, які можна використати для забезпечення конфіденційності даних та їхньої автентичності та принципи роботи завадостійкого коду Ріда-Соломона, який є одним з варіантів підвищення завадостійкості процесу комунікації.

Перелік посилань

1. Investigating Radio Frequency Vulnerabilities in the Internet of Things (IoT) / E. Anthi et al. IoT. 2024. Vol. 5, no. 2. P. 356—380. URL: https://doi.org/10.3390/iot5020018 (date of access: 08.11.2024).
2. Resistance to Replay Attacks of Remote Control Protocols using the 433 MHz Radio Channel / A. Stefankiv et al. Cybersecurity Providing in Information and Telecommunication Systems 2024. 2024. Vol. 3654, no. 1. P. 98–110.
3. Pichamuthu R., Sathishkumar A., Khadirkumar N. An Enhanced Deep Learning Approach for Preventing Replay Attacks in Wireless Sensor Network. Solid State Technology. 2020. Vol. 63, no. 4. P. 8010—8023.

4. RFC 8017. PKCS #1: RSA Cryptography Specifications Version 2.2. Replaces RFC 3447 ; effective from 2016-11-01. Official edition. Fremont, CA : IETF, 2016. 78 p. URL: https://datatracker.ietf.org/doc/html/rfc8017.

5. Pointcheval D. How to encrypt properly with RSA. RSA Laboratories CryptoBytes. 2002. Vol. 5, no. 1. P. 9—19.

6. Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory. 1985. Vol. 31, no. 4. P. 469—472. URL: https://doi.org/10.1109/tit.1985.1057074 (date of access: 08.11.2024).

7. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978. Vol. 21, no. 2. P. 120—126. URL: https://doi.org/10.1145/359340.359342 (date of access: 08.11.2024).

8. FIPS 197. Advanced Encryption Standard (AES). Replaces FIPS 197 (11/26/2001) ; effective from 2023-05-09. Official edition. Gaithersburg, MA : NIST, 2023. 46 p. URL: https://doi.org/10.6028/NIST.FIPS.197-upd1.

9. FIPS 46-3. Data Encryption Standard (DES). Replaces FIPS 46-2 ; effective from 1999-10-25. Official edition. Gathiersburg, MA : NIST, 1999. 27 p.

10. Schneier B. The Blowfish Encryption Algorithm. Dr. Dobb's Journal. 1994. Vol. 19, no. 4. P. 38—40.

11. Twofish: A 128-Bit Block Cipher / B. Schneier et al. Schneier on Security. URL: https://www.schneier.com/wp-content/uploads/2016/02/paper-twofish-paper.pdf (date of access: 08.11.2024).

12. Massey J. L., Lai X. A Proposal for a New Block Encryption Standard. Advances in Cryptology — EUROCRYPT '90. Lecture Notes in Computer Science. 1991. Vol. 473, no. 1. P. 389—404.

13. GnuPG. GnuPG. Version 2.5.1. 2024. URL: https://gnupg.org/index.html (date of access: 08.11.2024).

14. dm-crypt — The Linux Kernel documentation. The Linux Kernel documentation — The Linux Kernel documentation. URL: https://docs.kernel.org/admin-guide/device-mapper/dm-crypt.html (date of access: 08.11.2024).

15. BitLocker overview. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/ (date of access: 08.11.2024).

16. IDRIX. VeraCrypt. Version 1.26.15. Paris: IDRIX, 2024. URL: https://veracrypt.fr (date of access: 08.11.2024).

17. Гарасимчук О. І., Максимович В. М. Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості. Ukrainian Information Security Research Journal. 2003. Т. 5, № 3(16). URL: https://doi.org/10.18372/2410-7840.5.4270 (дата звернення: 08.11.2024).

18. Хомік М., Гарасимчук О. АНАЛІЗ ЗАГРОЗ ДЛЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ І ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ТА ЗАХОДИ ЗАХИСТУ. Ukrainian Information Security Research Journal. 2023. Т. 25, № 4. С. 172—184. URL: https://doi.org/10.18372/2410-7840.25.18222 (дата звернення: 08.11.2024).

19. Івашко А. В. Теорія інформації та кодування в прикладах і задачах : навч. посібник / А. В. Івашко, В. А. Крилова ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2022. – 317 с.

20. Kuila B. Design and Implementation of RS (255, 223) Detecting Code in FPGA. International Journal of Computer Applications. 2015. Vol. 123, no. 9. P. 33-39. URL: https://discovery.researcher.life/download/article/ecde86c509123e8ba804da34f30903f0/full-text (date of access: 08.11.2024).

21. Czynszak S. Decoding algorithms of Reed-Solomon code: магістерська робота. Karlskrona, 2011. 125 p. URL: https://www.diva-portal.org/smash/get/diva2:833161/FULLTEXT01.pdf (date of access: 08.11.2024).

22. Chien R. Cyclic decoding procedures for Bose- Chaudhuri-Hocquenghem codes. *IEEE Transactions on Information Theory*. 1964. Vol. 10, no. 4. P. 357–363. URL: https://doi.org/10.1109/tit.1964.1053699 (date of access: 08.11.2024).

23. Forney G. On decoding BCH codes. *IEEE Transactions on Information Theory*. 1965. Vol. 11, no. 4. P. 549–557. URL: https://doi.org/10.1109/tit.1965.1053825 (date of access: 08.11.2024).

Надійшла 04.02.2025