сигналу. Збірник наукових праць "Спеціальні телекомунікаційні системи та захист інформації". К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2023. Вип. № 2 (38) С. 48-60.
[4]. Науково-дослідна робота. Розробка методів щодо виявлення цифрових детермінованих сигналів в неперервному середовищі з випадковими процесами. К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2023.
[5]. Про державну таємницю: Закон України від 21 січ.1994 р. № 3855-XII.
[6]. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII.
[7]. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 лип. 1994 р. № 80/94-ВР.
[8]. Про затвердження Концепції технічного захисту інформації в Україні: Постанова Кабінету Міністрів України від 8 жовт. 1997 р. N 1126.
[9]. Батаєв О.П., Ковтун І.В., Корольова Н.А. Теорія електричного зв'язку: навч. посіб. Харків, 2010. 650 с.

JUSTIFICATION OF THE PROBABILITY OF DETERMINING THE PRESENCE OF SIGNALS IN THE ENVIRONMENT OF THEIR PROPAGATION

The substantiation of the impossibility of determining the presence of signals in the media of their distribution was carried out. A discrete-continuous channel was used as a model of the information distribution channel. Information was produced from a discrete source, where each of the information symbols was matched by discontinuous implementations that propagated through a continuous medium with interference. Reception of signals is carried out by means that can be effective. From the point of view of securing information from uncontrolled dissemination and ensuring its security in the distribution environment, as a rule, two factors are used: attenuation of the wave (signal) amplitude during its propagation in the physical environment; the distorting effect of interference that takes place in the medium of signal propagation and destroys its shape. However, the use of these factors, which could ensure complete, almost absolute security of information, is a difficult issue, if not impossible. After all, signals propagating in space, in accordance with the laws of physics, do so in the form of electromagnetic or other waves, or streams of elementary (charged) particles. They can spread over fairly long distances, and theoretically almost to infinity, the effectiveness of their interception is completely determined by the effectiveness of the means of reception. To solve this issue, which is widely used in information security management, there is a risk-oriented approach that does not require absolute security, but allows the possibility of not fulfilling the security requirement with a certain acceptable risk [2]. This risk, as a rule, is determined by the permissible losses that the owner of the assets can incur, and at the same time the effectiveness of production processes will not be disturbed.
Keywords: information security, cyber security, information and communication systems, information protection systems, information signal, discrete channel.

Іванченко Сергій Олександрович, доктор технічних наук, професор, професор Спеціальної кафедри № 1 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".

Serhiy Ivanchenko, doctor of technical sciences, professor, professor of the Special Department No. 1 of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute".
E-mail: soivanch@ukr.net.
Orcid ID: 0000-0003-1850-9596.

Некоз Василь Сергійович, викладач Спеціальної кафедри № 3 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського".

Vasyl Nekoz, teacher of the Special Department No. 3 of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute".
E-mail: nvs20141987@gmail.com.
Orcid ID: 0000-0001-5091-0529.

DOI: 10.18372/2410-7840.26.18837
УДК 004.056

ДОСЛІДЖЕННЯ СТІЙКОСТІ ДО АТАК ВІДТВОРЕННЯ ПРОТОКОЛІВ ДИСТАНЦІЙНОГО КЕРУВАННЯ З ВИКОРИСТАННЯМ РАДІОКАНАЛУ 433 МГЦ

Ольга Михайлова, Артем Стефанків

У цій статті виявляються критичні вразливості протоколу EV1527, які широко використовуються в системах дистанційного керування, зокрема в домашніх автоматизаційних системах. Зосереджуючись на детальному аналізі структури протоколу та потенційних слабких місць, дане дослідження оцінює ризики атак повторного відтворення, які можуть здійснюватися шляхом перехоплення та повторної трансляції радіосигналів. Результати роботи демонструють значну вразливість цього протоколу до таких атак через відсутність криптографічного захисту переданих даних. У рамках цієї роботи було проведено експериментальні випробування з використанням програмно-керованого трансивера HackRF One, що дозволило відт-

ворити атаку в контрольованих лабораторних умовах. Експерименти підтвердили теоретичні припущення щодо можливості реалізації таких атак, підкреслюючи необхідність розробки більш захищених комунікаційних протоколів. Застосування HackRF One продемонструвало, як легко зловмисники можуть перехоплювати та повторно транслювати сигнали, отримуючи несанкціонований доступ до систем дистанційного керування. У даній статті акцентується увага на важливості переходу від застарілих технологій до сучасних рішень, які включають динамічні коди та криптографію для підвищення рівня безпеки. Використання динамічних кодів, таких як технологія рухомого коду HCS301, значно ускладнює можливість атак повторного відтворення, оскільки кожна передача коду є унікальною. Це означає, що навіть у разі перехоплення сигналу зловмисник не зможе його повторити для отримання доступу. Автори рекомендують впровадження криптографічних методів, таких як технологія рухомого коду HCS301, що значно ускладнює можливість повторних атак. Запровадження таких технологій підвищує рівень безпеки та робить системи дистанційного керування більш стійкими до зловмисних дій. Крім того, наголошується на необхідності постійного оновлення та вдосконалення безпекових протоколів для захисту критичної інфраструктури. З огляду на ці результати, дана робота вказує на нагальну потребу в оновленні та вдосконаленні систем дистанційного керування, включаючи розробку нових, більш стійких до атак протоколів, особливо в контексті забезпечення безпеки об'єктів критичної інфраструктури. Інтеграція сучасних криптографічних методів є ключовим кроком для захисту від зловмисних атак та забезпечення надійної роботи систем дистанційного керування.

***Ключові слова**: радіоканал, перехоплення, атака повторного відтворення, фізична безпека, PT2262, HackRF One, NanoVNA, EV1527.*

ВСТУП

Системи дистанційного керування є важливою частиною сучасних охоронних рішень, забезпечуючи зручність та ефективність управління фізичними периметрами – від шлагбаумів та автоматичних воріт до систем сигналізації. Однак радіозв'язок, який часто є основою цих систем, може стати вразливим, відкриваючи двері для потенційних атак. Особлива увага в цьому контексті приділяється вразливості протоколів дистанційного керування, зокрема EV1527, який можна використовувати для здійснення атак з відтворенням сигналу [1-3].

У цій роботі ми зосереджуємося на аналізі цих вразливостей, використовуючи як теоретичні, так і практичні методи для демонстрації можливих атак у лабораторних умовах. Важливість таких досліджень полягає у зростаючій залежності від бездротових технологій у системах безпеки, що робить їх потенційною мішенню для зловмисників і відображає необхідність розробки більш надійних протоколів безпеки.

Мотивацією для цього дослідження стали численні випадки повторних атак, які підкреслюють вразливість існуючих систем. Наша мета полягає не лише у виявленні та демонстрації вразливостей, а й у розробці рекомендацій щодо покращення безпеки використання систем дистанційного керування. Для цього ми провели детальний аналіз документації протоколів EV1527 і PT2262 і вивчили принципи їх роботи, структуру повідомлень і модуляцію даних. Також був проведений порівняльний аналіз обладнання, здатного здійснювати такі атаки, включаючи програмно керований трансивер HackRF One і векторний мережевий аналізатор NanoVNA V2.2 [6-8].

Важливо відзначити, що розвиток технології дистанційного керування має глибоке коріння в історії. Від перших хостів і бездротових систем, розроблених наприкінці 19-го століття для задоволення потреб управління автономними транспортними засобами, включаючи торпеди, до сучасних бездротових пристроїв, які є невід'ємною частиною нашого повсякденного життя. Наприклад, наприкінці 1930-х років Philco вперше розробила бездротовий пульт дистанційного керування для споживчих електронних пристроїв, відомий як Mystery Control, який використовував низькочастотну радіопередачу. Це був значний прорив у технології дистанційного керування. Іншим хорошим прикладом може бути набір сучасних переносних [19] пристроїв, підключених через Bluetooth, які також використовуються як частина налаштування Smart-home і можуть виконувати функцію дистанційного керування.

Також значним кроком у розвитку технології дистанційного керування стало створення першого телевізійного пульта дистанційного керування компанією Zenith Radio Corporation у 1950 році. Спочатку він підключався до телевізора за допомогою дроту, але в 1955 році з'явився бездротовий пульт "Flashmatic". був розроблений, який керував телевізором за допомогою спрямованих спалахів світла [17-18].

Структура роботи включає огляд літератури, методологію, результати аналізу, порівняльне дослідження та обговорення результатів. Ми спо-

діваємося, що ця робота не лише висвітлить поточні проблеми безпеки дистанційного керування, але й сприятиме розробці безпечніших рішень у цій галузі.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Поточні дослідження в галузі безпеки дистанційного керування та протоколів доступу без ключа наголошують на використанні динамічних кодів, особливо зосереджуючись на протоколі HCS301. Цей протокол використовується в системах безключового доступу для транспортних засобів, включаючи автомобільні сигналізації та системи запуску автомобіля. Однією з ключових особливостей HCS301 є використання запатентованого блокового шифру KeeLoq на основі нелінійного регістру зсуву зі зворотним зв'язком, що забезпечує високий рівень безпеки.

Одне з важливих досліджень, проведених Тобіасом ван Капеллевеном з Університету Радбауд Неймеген, присвячене порівняльному аналізу безпеки систем автомобільної сигналізації на основі протоколу EV1527. У своїй роботі ван Капеллевен підкреслює вразливість EV1527 до повторних атак, що ставить під сумнів його надійність у контексті безпеки.

Крім того, інші джерела, такі як статті на вебсайті Yaoertai, детально описують механізми та особливості технології рухомого коду HCS301. У цих статтях міститься інформація про роботу HCS301, його переваги та застосування в різних сферах, включаючи автомобільні та домашні системи безпеки. Особливу увагу приділено тому, як технологія HCS301 захищає від різних типів атак, включаючи захист від атак повторного відтворення.

Цей аналіз поточних досліджень і публікацій підкреслює важливість розуміння різноманітних протоколів безпеки та вразливостей, які існують у сучасних системах дистанційного керування та безключового доступу. Вони надають цінну інформацію, яку можна використати для підвищення безпеки цих систем [8].

ПОСТАНОВКА ЦІЛЕЙ

Основною метою цього дослідження є поглиблений аналіз протоколу EV1527, включаючи його дизайн, принципи роботи та потенційні вразливості.

Дослідження передбачає ретельний аналіз конструкторської документації модулів, які використовують цей протокол, а також аналіз основних характеристик антен і особливостей роботи з апаратним і програмним забезпеченням.

Основними завданнями дослідження є:

1. Аналіз дизайну протоколу EV1527: Вивчення технічної структури та основних компонентів протоколу, а також розуміння його функціональності та механізмів передачі даних;

2. Виявлення вразливостей: виявлення потенційних слабких місць у протоколі EV1527, включаючи його сприйнятливість до атак повторного відтворення та інших загроз;

3. Порівняльний аналіз обладнання: Оцінка та порівняння різних типів обладнання, яке можна використовувати для здійснення атак на системи з використанням протоколу EV1527;

4. Практична перевірка: проведення експериментів і випробувань в лабораторних умовах для перевірки теоретичних висновків і виявлення реальних вразливостей системи;

5. Оцінка доцільності використання протоколу: На основі отриманих даних і аналізу зробити висновок про практичність і безпеку використання протоколу EV1527 в системах дистанційного керування.

Результати цього дослідження нададуть цінну інформацію про надійність і безпеку протоколу EV1527, що має вирішальне значення для його застосування в системах безпеки та дистанційного керування. Очікується, що це дослідження допоможе розробникам та інженерам у виборі найбільш безпечних та ефективних рішень для їхніх систем.

ОСНОВНА ЧАСТИНА

Аналіз документації протоколу EV1527

EV1527 – це мікросхема кодера повідомлень, яка використовує однойменний протокол і розроблена компанією Silvan Chip Electronics Tech. Co. Ltd (КНР) [2]. Цей протокол і однойменна мікросхема і його клони використовуються в системах дистанційного керування механізмами, системах автоматики, панелях управління системами «розумний будинок», саморобних пристроях і т. д. Таке широке використання пояснюється відносною дешевизною мікросхеми, наявність механізму запобігання зіткнень, простота виконання приймача і передавача. Існують готові рішення на основі цього стандарту, які можна легко інтегрувати в існуючу структуру, включаючи пристрої контролю доступу, такі як шлагбауми, автоматичні ворота, автоматичні ролети тощо.

Мікросхема EV1527 виготовляється в корпусах DIP-8 і TSOP-8 і має чотири входи даних, один вхід синхронізації, входи живлення та один вихід коду, який можна передавати по радіо. Основні частоти для зв'язку – 433 МГц для країн

Європи і 315 МГц для США і Канади. В наявній документації наведена типова схема ввімкнення мікросхеми з радіопередавачем [2] (рис.1).

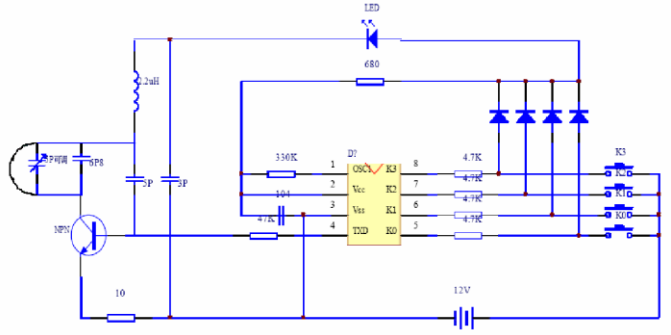


Рис. 1. Типова схема підключення мікросхеми кодера EV1527

Протокол, який використовує цей чіп, більш стійкий до атак перевиконання та зіткнень. Протокол передбачає один тип повідомлення з фіксованою структурою. Повідомлення складається з преамбули та основної частини (рис. 2).

Output data frame:

Preambl e	C0 ~ C19 (1 million codes)	D0	D1	D2	D3

Рис. 2. Будова повідомлення протоколу EV1527

Преамбула має довжину в 32 біти та використовується для синхронізації передавача та приймача. Будова преамбули наступна: один період домінантного стану та 31 період рецесивного стану на виході мікросхеми [2] (рис. 3).

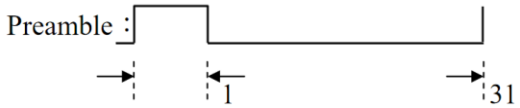


Рис. 3. Будова преамбули повідомлення

Основна частина повідомлення складається з коду ключа та чотирьох бітів даних. Основна частина повідомлення кодується за допомогою послідовностей «3-1» (три періоди в домінантному стані та один період в рецесивному стані на виході мікросхеми) для передачі логічної одиниці та оберненої послідовності «1-3» для передачі логічного нуля [2] (рис. 4). Аналогічне кодування використовується в мікросхемі PT2262 [3].

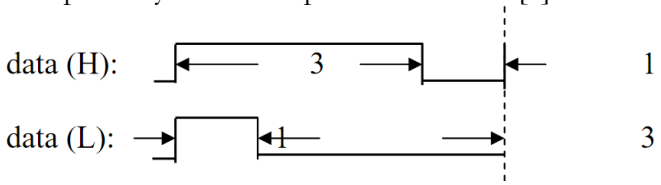


Рис. 4. Кодування на виході мікросхеми

Код ключа задається двадцятьма бітами, що дозволяє існування 1048576 унікальних ключів та значно ускладнює виконання атаки перебору, оскільки потрібно перебрати не тільки вказану вище кількість кодів ключів, але й 16 кодів кнопок, які використовуються в атакованій системі. Загальна кількість комбінацій для повного перебору складає 16777216 повідомлень.

Однак, даний протокол використовує статичний код та не використовує криптографічні засоби для підвищення рівня безпеки. Повідомлення не змінюється після кожного генерування, а тому можливе виконання атаки повторного відтворення [1].

Порівняльний аналіз протоколів EV1527 і PT2262

У цьому розділі представлено порівняльний аналіз двох популярних протоколів дистанційного керування: EV1527 і PT2262. Обидва протоколи часто використовуються в системах дистанційного керування, але вони мають деякі ключові відмінності. EV1527 – мікросхема, розроблена Silvan Chip Electronics Tech. Co. Ltd (КНР), яка використовує фіксований формат повідомлень і не має криптографічного захисту. Протокол забезпечує один тип повідомлення з фіксованою структурою, включаючи 32-розрядну преамбулу та основну частину з кодом ключа та чотирма бітами даних. EV1527 використовує механізм запобігання зіткненням і простий у застосуванні.

З іншого боку, PT2262 може мати різні конфігурації повідомлень від 6 до 12 біт коду клавіші та від 0 до 6 біт коду кнопки. Протокол забезпечує послідовність синхронізації в кінці повідомлення, що є зміною в порівнянні з EV1527. PT2262 не має вбудованих механізмів пом'якшення колізій і використовує статичну адресацію.

Однією з ключових відмінностей є те, що якщо передавач втрачено, системи на основі PT2262 вимагають змінити код на приймачі та інших передавачах, щоб скасувати доступ втраченого передавача. Цього недоліку немає в системі на базі EV1527, де можна скасувати доступ, видаливши запис про втрачений передавач з пам'яті приймача.

Загалом, хоча обидва протоколи не мають криптографічної безпеки та вразливі до атак із повторенням, EV1527 виявився більш гнучким у використанні та адаптації до потреб різних користувачів. Це робить його більш привабливим вибором для сучасних систем дистанційного керування, незважаючи на наявні вразливості.

Принцип повторної атаки

Повторна атака – це форма кібератаки, коли зловмисник перехоплює зв'язок між двома законними сторонами та повторно надсилає перехоплені дані. Цей метод використовується для отри-

мання неавторизованого доступу до системи або ініціювання небажаних дій від імені законного користувача. На відміну від атаки «людина посередині», де зловмисник активно втручається в спілкування, атака повтору є пасивною.

Сценарій атаки можна описати наступним чином (рис. 5):

1. Зловмисник, якого ми назвемо Єва, прослуховує діапазон радіочастот, в якому працюють приймач і передавач сигналу, і записує сигнал;

2. Аліса посилає сигнал Бобу, щоб активувати певний механізм, наприклад відкрити автоматичні ворота;

3. Боб приймає та декодує сигнал, і, якщо він збігається із збереженим кодом, діє;

4. Єва відтворює перехоплений сигнал, і система, вразлива до атаки відтворення, сприймає це як сигнал від Аліси та виконує дію у відповідь.

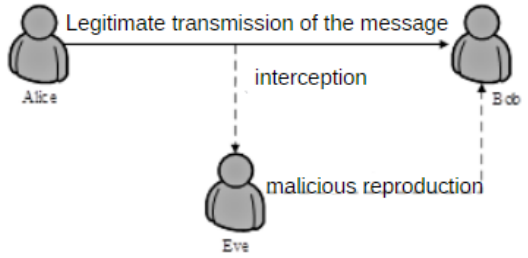


Рис. 5. Схема атаки повторного відтворення

При цьому зловмисник повинен мати можливості для пасивного перехоплення та відтворення. Важливість впровадження більш потужних механізмів безпеки в цих системах стає очевидною для зменшення ризиків несанкціонованого доступу або контролю.

Для захисту від повторних атак системи дистанційного керування повинні включати додаткові рівні безпеки, такі як криптографічне кодування або використання динамічних кодів, які змінюються з кожною передачею. Наприклад, використання технологій, подібних до HCS301 Rolling Code, про який йшлося раніше, може значно підвищити безпеку систем дистанційного керування.

Повторна атака є особливо небезпечною, оскільки вона не вимагає від зловмисника глибоких технічних знань або складного обладнання. Легкість реалізації таких атак робить їх загрозою для широкого кола бездротових систем, від систем домашньої автоматизації до більш складних систем контролю доступу.

Розуміння цих ризиків і вразливостей має вирішальне значення для розробників безпеки та виробників обладнання. Це дослідження підкреслює необхідність постійного оновлення знань про кібербезпеку та розробки більш стійких і надійних рішень для запобігання подібним атакам у майбутньому.

Порівняльний аналіз основних характеристик антен для перехоплення сигналу

Проведення порівняльного аналізу основних характеристик антен дозволяє визначити придатність кожної з наявних антен для перехоплення та відтворення сигналу та виявити їх недоліки та/або дефекти.

Існуючий приймач і передавачі використовують діапазон LPD433 (433,050 МГц – 434,79 МГц), який знаходиться в межах 70 см радіоаматорського діапазону (430 МГц - 440 МГц).

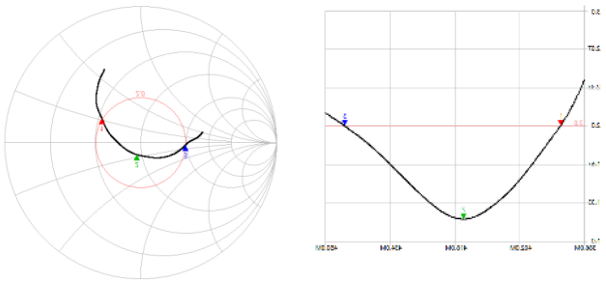
Діапазон LPD433 розділений на 69 каналів з кроком 25 кГц, цей діапазон використовується для малопотужних передавачів малої дальності. До передавачів малого радіусу дії належать системи дистанційного керування, системи домашньої автоматизації, системи безключового доступу в автомобілі, портативні рації малої потужності тощо. В Україні використання цього діапазону регламентується ДСТУ ETSI EN 300 220-1:2018 та ДСТУ ETSI EN 300 220-2:2017, який є гармонізацією стандарту ETSI EN 300 220-1 V3.2.1 [4] та ETSI EN 300 220-2 V3 .1.1 [5]. Межі діапазону визначаються рекомендаційним документом авторства CEPT/ERC Rec 70-03 [6]. У США цей діапазон не використовується для неліцензійного мовлення, тому Федеральна комісія зі зв'язку (FCC) виділила діапазон 315 МГц для короткочасної роботи пристроїв ближнього радіусу дії з обмеженням на напруженість вихідного електричного поля 300 мкВ/м. з тривалістю передачі до 3 хвилин [8].

Основною вимогою до антен є відповідність їх робочого діапазону частот заданій смузі з мінімальним значенням КСХ.

Для порівняльного аналізу використовували портативний аналізатор електричних кіл NanoVNA [9] та програмне забезпечення NanoVNA-Saver [10]. Порівняно чотири типи антен за параметрами коефіцієнта стоячої хвилі та робочого діапазону частот. Граничне значення КСХ для визначення діапазону робочих частот становить 2000. Антени вимірювали у вертикальній поляризації та усереднювали п’ять послідовних вимірювань.

Антена 1 Телескопічна антена з роз'ємом SMA, мінімальна довжина 17 см і максимальна довжина 102 см. Вимірювання проводилося в двох конфігураціях довжини антени – мінімальній і максимальній.

Нижче наведені результати вимірювання параметрів антени 1 на мінімальній довжині (рис. 6, табл. 1) і максимальній довжині (рис. 7, табл. 2).



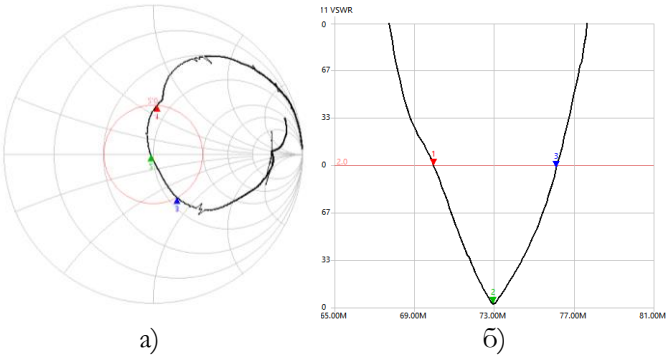
а) б)

Рис. 6. Параметри антени 1 при мінімальній довжині: а) діаграма Сміта, б) графік частотної залежності

Таблиця 1

Значення параметрів антени 1 при мінімальній довжині в мітках 1-3

	Мітка 1	Мітка 2	Мітка 3
Частота	391,966 МГц	415,851 МГц	445,286 МГц
КСХ за напругою	2,000	1,191	2,000
Втрати повернення	-9,543 дБ	-21,213 дБ	-9,545 дБ
Імпеданс	26,6 - j10,8 Ом	46,9 + j7,85 Ом	99,8 + j3,25 Ом



а) б)

Рис. 7. Параметри антени 1 на максимальній довжині: а) діаграма Сміта, б) графік залежності КСХ від частоти

Таблиця 2

Значення параметрів антени 1 при максимальній довжині в мітках 1-3

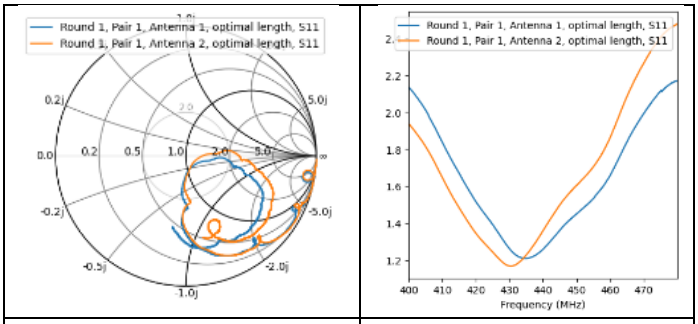
	Мітка 1	Мітка 2	Мітка 3
Частота	69,9772 МГц	72,9504 МГц	76,1219 МГц
КСХ за напругою	1,996	1,021	1,977
Втрати повернення	-9,566 дБ	-39,615 дБ	-9,676 дБ
Імпеданс	42,2 - j31,5 Ом	49 + j0,136 Ом	57,1 + j36,5 Ом

Отримані результати свідчать про придатність антени 1 при мінімальній довжині для роботи з цільовим сигналом.

Антена 2. Телескопічна антена з роз'ємом SMA, мінімальна довжина 11,5 см і максимальна довжина 47,5 см. Доступно чотири екземпляри цієї антени. Для кожного із зразків вимірювання проводились у конфігурації довжини, що відповідає чверті довжини хвилі цільового діапазону (17,5 см). За допомогою методу попарного порівняння відібрано зразок з найкращими характеристиками (рис. 10-12). Критеріями порівняння були обрані мінімальне значення коефіцієнта стоячої хвилі за напругою, частота, на якій було досягнуто мінімальне значення КСХ, і вхідний опір антени на частоті з мінімальним КСХ. Порівняння проходило у два раунди, у перших двох парах зразків (№ 1 і № 2 і № 3 і № 4 відповідно), порівнювали у другому раунді, а зразки з кращими характеристиками від попереднього раундів порівнювали.

Графи побудовані за допомогою бібліотеки sci-kit-of для мови програмування Python [7]. Ця бібліотека підтримує створення та імпорт файлів збереження Touchstone, які використовуються в більшості аналізаторів схем у програмі Nano-VNA-Saver.

Раунд 1. Порівнюється пара екземплярів №1 і №2. Показані результати порівняння (рис. 8).



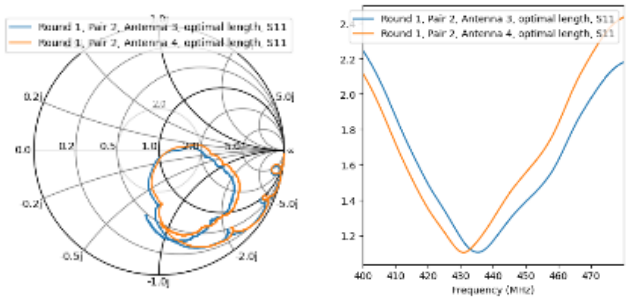
а) б)

Рис. 8. Параметри зразків № 1 і № 2 антени 2 при оптимальній довжині: а) діаграма Сміта, б) графік залежності КСХ від частоти

На рис. 8 видно, що значення хвильового опору для обох зразків на лінії КСХ 1,0 досить близькі. Проте в зразку № 2 спостерігається додатковий резонанс на частоті 882 МГц, нехарактерний для зразка № 1. Також рис. 8 демонструє перевагу зразка № 1 над зразком № 2 в діапазоні 430-440 МГц. Мінімальне значення КСХ екземпляра №2 знаходиться на початку діапазону і досягає значення 1,357 в кінці цього діапазону. Зразок № 1 демонструє дещо більше значення КСХ 1,208 на частоті 435,058 МГц.

З проведеного аналізу даних можна зробити висновок, що екземпляр 2 демонструє найкращі показники в цьому діапазоні.

Показано порівняння пари 2 (зразки №3 і №4) (рис. 9).



а) б)

Рис. 9. Параметри екземплярів 3 і 4 антени 2 при оптимальній довжині: а) діаграма Сміта, б) графік залежності КСХ від частоти

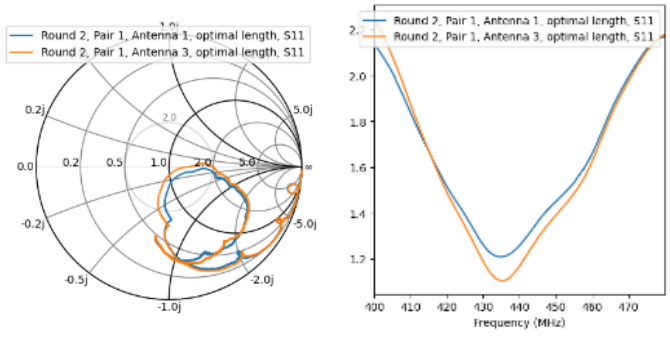
Нижче (рис. 10) можна спостерігати, що значення реактивної складової опори для обох екземплярів на лінії КСХ 1.0 досить близькі. Але примірник 2 демонструє додатковий резонанс на частоті 882 МГц, що не характерно для примірника 1.

Далі (рис. 11) показано перевагу екземпляра 1 над екземпляром 2 у діапазоні 430-440 МГц. Мінімальне значення КСХ екземпляра 2 знаходиться на початку діапазону і досягає значення 1,357 наприкінці діапазону. Екземпляр 1 демонструє трохи вищий КСХ 1,208 на 435,058 МГц.

З аналізу даних можна зробити висновок, що зразок 2 демонструє найкращі показники в цьому діапазоні.

Порівняння пари 2 (Примірники №3 і №4) показано на рис. 12 і 13.

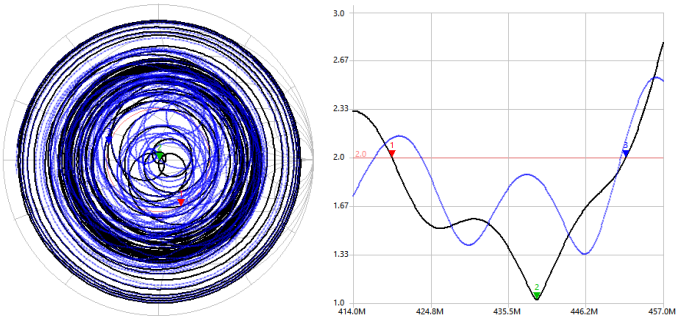
Враховуючи наведену вище схожість між частотами мінімального значення КСХ і відповідними значеннями, наведеними на рисунку 15, можна зробити висновок, що серед наявних найкращу продуктивність демонструє зразок №3 і він придатний для роботи з цільовим сигналом.



а) б)

Рис. 10. Параметри екземплярів 1 і 3 антени 2 при оптимальній довжині: а) діаграма Сміта; б) графік залежності КСХ від частоти

Антена 3. Чотирьох діапазонна автомобільна антена з роз'ємом PL-259 є частиною автомобільної радіостанції QYT KT-7900D, яка призначена для роботи в діапазонах 136-174 МГц, 220-270 МГц, 350-390 МГц і 400-4. Антена оснащена магнітною підставкою з вхідним роз'ємом SO-239 і кабелем SYWV 50-3 довжиною 7 метрів з роз'ємом PL-259. Нижче наведені результати вимірювання параметрів антени 3 в діапазоні частот сигналу (рис. 13, табл. 3). Синім кольором позначено вимірювання параметрів при підключенні антени через магнітну підставку, що входить в комплект, а чорним - при підключенні антени кабелем RG-58U70 довжиною 5 метрів через перехідник SMA-SO-239 до антени.



а) б)

Рис. 11. Параметри антени 3: а) діаграма Сміта; б) графік залежності КСХ від частоти

З рисунка 11 видно, що магнітна підставка погіршує роботу антени. Під час використання магнітної підставки в заявленому виробником діапазоні 440 МГц пік КСХ відсутній.

Таблиця 3

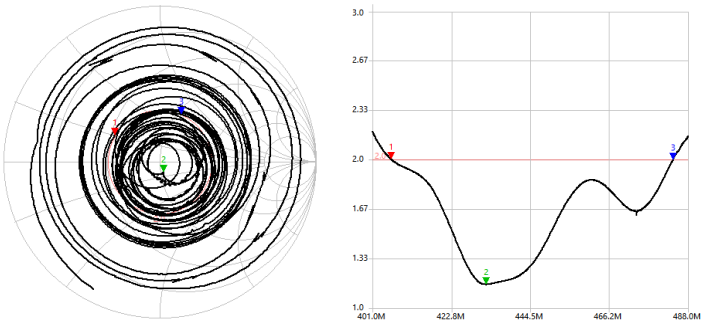
Значення параметрів антени 3 без підставки в мітках 1-3

	Мітка 1	Мітка 2	Мітка 3
Частота	419,373 МГц	439,469 МГц	451,821 МГц
КСХ за напругою	1,998	1,022	1,999
Втрати повернення	-9,552 дБ	-39,356 дБ	-9,551 дБ
Імпеданс	54,9 - j36,7 Ом	51,0 - j0,308 Ом	25,5 + j5,74 Ом

Результати показують, що ця антена може обробляти цільовий сигнал, але її продуктивність буде менш оптимальною, ніж у антени 2.

Антена 4. Антена "Ground plane" з роз'ємом BNC і комплектним кабелем BNC-SMA типу RG-174 довжиною 3 метри, заявлений виробником діапазон 65-375 МГц. Антена складається з друкованої плати, на якій закріплені роз'єми BNC для виходу і входу центрального елемента і отвори для чотирьох заземлюючих елементів, виконаних

у вигляді телескопічних антен довжиною від 20 до 95 см. Експериментально цю антену вдалося налаштувати на цільову дальність (довжина центрального елемента – 47,5 см, довжина заземлюючих елементів – 51,5 см). Антена була встановлена на саморобній щоглі на висоті приблизно 175 см від рівня підлоги. Нижче наведені вимірювання цієї антени в наведеній вище оптимальній конфігурації (рис. 12, табл. 4).



а) б)

Рис. 12. Параметри антени 4 при оптимальній довжині: а) діаграма Сміта;
б) графік залежності КСХ від частоти

Таблиця 4

Значення параметрів антени 4 при оптимальній довжині в мітках 1-3

	Мітка 1	Мітка 2	Мітка 3
Частота	406,237 МГц	432,313 МГц	483,779 МГц
КСХ за напругою	2,000	1,157	1,996
Втрати повернення	-9,545 дБ	-22,766 дБ	-9,566 дБ
Імпеданс	26,4 + j10,3 Ом	51,8 - j7,2 Ом	53,6 + j36,3 Ом

З отриманих даних можна зробити висновок, що дана антена придатна для роботи з цільовим сигналом у такій конфігурації, але стабільність параметрів не може бути досягнута через роботу антени поза заявленими виробником характеристиками та розрахунковими значеннями довжина елементів (для діапазону 430-440 МГц довжина центрального елемента повинна бути приблизно 16,5 см, а довжина заземлюючих елементів – 18,3 см) [8]. Отже, для роботи з цільовим сигналом в лабораторних умовах найкращі показники демонструє зразок № 3 антени № 2. Для визначення стабільності показників у часі була проведена серія послідовних вимірювань протягом 16 годин. Вимірювання проводили з інтервалом 2 – 2,5 години.

Результати вимірювань знаходяться в одному діапазоні і не виходять за встановлений діапазон, обмежений значенням КСХ 2000.

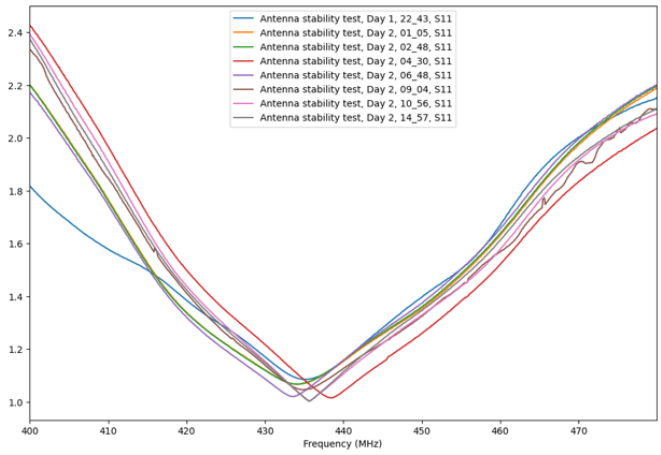


Рис. 13. Тестування стабільності продуктивності в часі

Процес виконання демонстрації повторної атаки

У цьому розділі ми зосередимося на детальному вивченні та практичному застосуванні методів перехоплення та відтворення сигналу в системах бездротового зв'язку. Наша мета – дослідити та продемонструвати, як зловмисник може використовувати спеціалізоване обладнання та програмне забезпечення для перехоплення та імітації сигналів для незаконного доступу або контролю систем.

Цей процес, відомий як атака повтору, є ключовим елементом у вивченні безпеки бездротового зв'язку та розробці ефективних заходів протидії [1-6].

Обладнання:

- передавачі сигналу;
- приймач сигналу з приводом;
- трансивер з програмним управлінням HackRF One;
- кабель USB 2.0 A – USB 2.0 Micro-B;
- антена та з'єднувальні кабелі з перехідниками;
- комп'ютер під керуванням Kali Linux;
- аналізатор радіочастотного спектру gqrx [6];
- пакет програм Universal Radio Hacker для зворотного проектування бездротових протоколів [12].

Опис обладнання:

1. Передавачі сигналів: передавач А – мініатюрний передавач управління з двома кнопками з позначками A і B і світлодіодом, чорний з сріблястими вставками, живиться від елемента 23A; трансмітер B - мініатюрний керуючий трансмітер з чотирма кнопками, позначеними A, B, C, D і світлодіодом, сріблястого кольору з захисною кришкою, живиться від елемента 23A;

2. Приймач сигналу з приводом - розроблений JoyDeal, компактний приймач і декодер ко-

манд стандартів EV1527 і PT2262 з пам'яттю на 15 кнопок і стандартною гвинтовою антеною. Напруга живлення коливається від 3,6 до 24 вольт; в якості виконавчого механізму використовується світлодіод з обмежувальним резистором;

3. Програмно-керований трансивер HackRF One – портативний трансивер з програмним керуванням HackRF One у версії PortaPack H1 з можливістю автономної роботи. Трансивер має роз'єми для підключення антени, вбудований вихід генератора і вхід синхронізації, а також роз'єм живлення/даних USB Micro-B і роз'єм TRS 3,5 мм для підключення навушників і виведення демодульованого аудіосигналу;

4. Кабель USB 2.0 A – USB 2.0 Micro-B – кабель для передачі даних із роз'ємами USB 2.0 A та USB 2.0 Micro-B, довжиною 1 метр;

5. Антена та з'єднувальні кабелі з перехідниками – робочою антеною обрано екземпляр 3 антени 2; процес порівняльного аналізу описано в пункті 7. Адаптери та з'єднувальні кабелі не використовуються;

6. Комп'ютер під керуванням Kali Linux – ноутбук Asus Vivo book 15 X509FJ із встановленою спеціальною операційною системою Kali Linux 2024.1. Опис процедури підготовки комп'ютера до атаки наведено нижче.

Послідовність атаки:

• зловмисник починає перехоплювати сигнал за допомогою Universal Radio Hacker і чекає, поки законний користувач (жертва) надішле сигнал;

• законний користувач надсилає сигнал;

• приймач виконує вказану дію;

• зловмисник, використовуючи Universal Radio Hacker, посилає сигнал, що імітує законного користувача системи (жертву);

• одержувач виконує вказану дію, оскільки не може відрізнити зловмисника від законного користувача.

Виконання атаки:

1. Підготовка системи. Щоб підготувати систему до роботи з HackRF One, вам потрібно інсталювати пакети hackrf, hackrf-doc, hackrf-firmware, libhackrf-dev, libhackrf0 із власних репозиторіїв менеджера пакетів операційної системи;

2. Програмування приймача. Програмування приймача відбувається шляхом натискання кнопки програмування певну кількість разів для переходу в необхідний режим перемикання (миттєвий, перемикання, фіксація, таймер) і натискання потрібної кнопки на передавачі. Як зазначалося раніше, пам'ять приймача має 15 комірок. Були запрограмовані такі позиції: 1) Кнопка А передавача А в миттєвий режим; 2) Кнопка В передавача для перемикання режимів; 3) Кнопка А передавача В у режим таймера із затримкою 5 секунд;

3. Оцінка радіочастотного діапазону та перевірка прийому сигналу. Радіочастотний спектр оцінюється за допомогою gqrx [11].

Gqrx – це програма для аналізу радіочастотного спектру в реальному часі, яка поширюється під відкритою ліцензією GPL.[6]

Порядок виконання:

• підключіть антену до HackRF One і підключіть її до комп'ютера;

• перемкніть HackRF One у комп'ютерний режим;

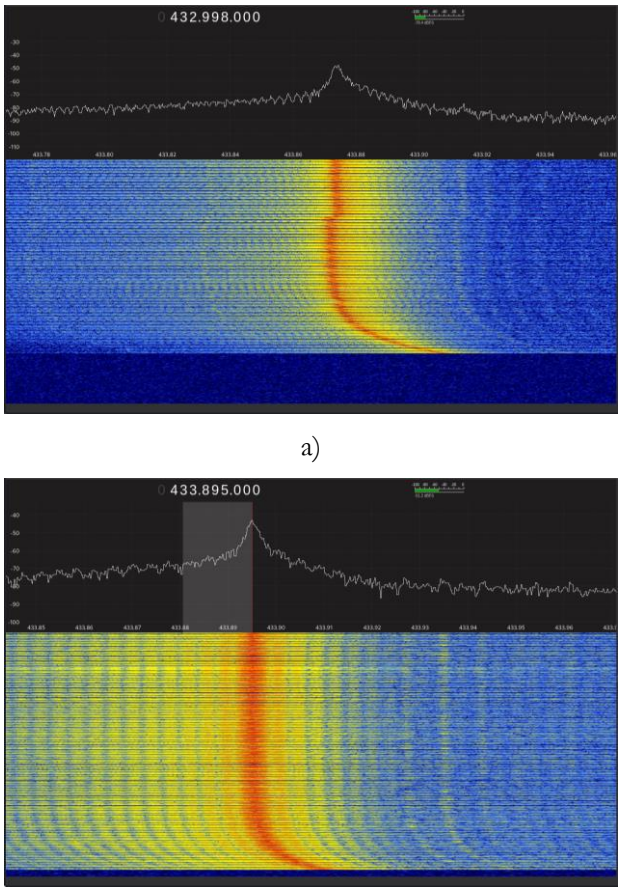
• запустіть gqrx на вашому комп'ютері;

• виберіть HackRF One зі списку пристроїв і встановіть підключення;

• встановіть частоту прийому 433,92 МГц;

• увімкнути моніторинг.

На екрані з'явиться водоспадний графік і лінійний графік сигналу. При натисканні кнопок на передавачі А спостерігаємо появу сигналу на графіках (рис. 14).

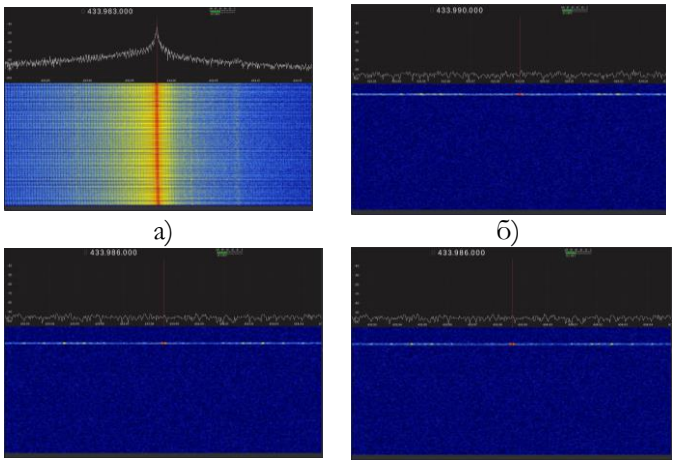


а)

б)

Рис. 14. Каскадні графіки сигналів кнопки передавача А: а) кнопка А; б) кнопка В

Ми виконаємо аналогічну процедуру для кнопок A, B, C і D передавача B (рис. 15).



а) б) в) г)

Рис. 15. Каскадні графіки сигналів кнопки передавача B: а) кнопка A; б) кнопка B; в) кнопка C; г) кнопка D

З отриманих даних можна зробити висновок, що підключення та конфігурація трансивера та комп'ютера правильні, і припустити, що передавач B частково працює або не має заявлених функцій. Сигнали від кнопок, які не передають сигнал (кнопки B, C, D передавача B), далі не розглядаються.

Перехоплення та аналіз сигналу

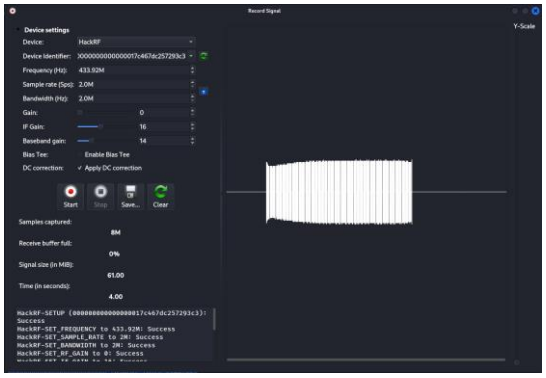
Для перехоплення та аналізу сигналу використовується програмний пакет Universal Radio Hacker [12]. Цей програмний пакет має можливості для запису сигналів, їх аналізу, зворотного проектування бездротових протоколів, відтворення записаних сигналів і створення нових сигналів на основі довільних даних. Цей програмний пакет написаний на Python і поширюється під безкоштовною ліцензією GPLv3. Встановлення виконується за допомогою менеджера пакетів pipx.

Порядок виконання:

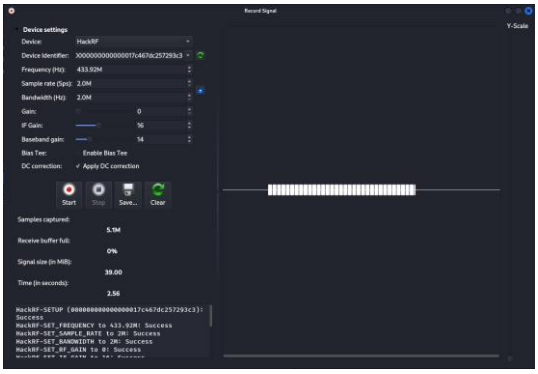
- підключіть антену до HackRF One і підключіть її до комп'ютера;
- перемкніть HackRF One у комп'ютерний режим;
- у меню Файл виберіть Записати сигнал;
- виберіть HackRF One зі списку доступних пристроїв;
- натисніть кнопку оновлення, яка розташована навпроти поля «Ідентифікатор пристрою», і дочекайтеся появи серійного номера в полі.;
- встановіть частоту перехоплення 433,92 МГц;
- натисніть кнопку «Пуск»;
- зачекайте на надходження сигналу;
- після запису сигналу натисніть кнопку «Стоп»;
- збережіть сигнал у файл за допомогою кнопки Зберегти;
- закрийте вікно запису, збережений сигнал автоматично відкриється в головному вікні програми.

Сигнали від передавачів A і B, розпізнані приймачем JoyDeal (кнопки A і B передавача A і кнопка A передавача B), були перехоплені (рис. 16) та інтерпретовані (рис. 17).

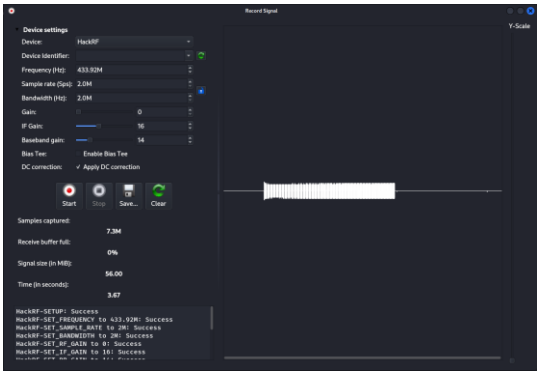
Сигнал був перехоплений із налаштованою смугою пропускання трансивера 2,0 МГц і частотою сканування 2 мільйони вибірок на секунду.



а)



б)

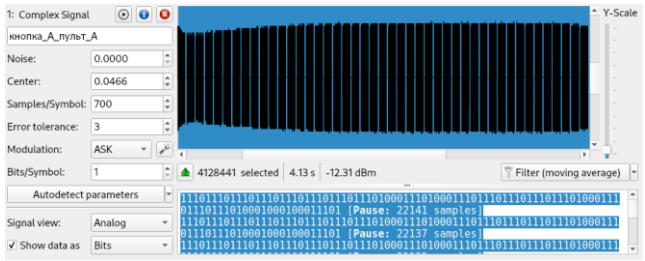


в)

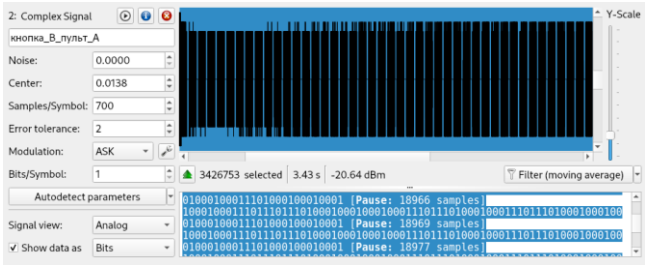
Рис. 16: Захоплення сигналу від передавачів: а) кнопка A передавача A; б) кнопка B передавача A; в) кнопка A передавача B

Перехоплені сигнали використовують маніпуляцію зі зсувом амплітуди та записуються з роздільною здатністю 700 вибірок на символ.

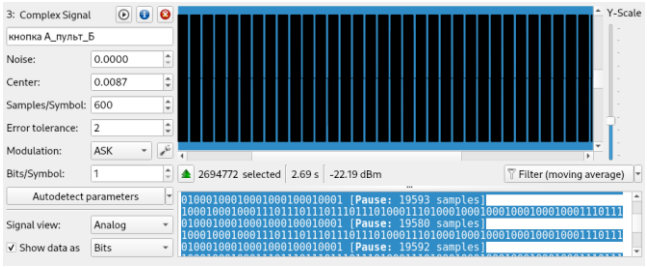
У стандартах PT2262 і EV1527 використовується однакове бітове кодування - «3-1» для кодування логічної одиниці і «1-3» для кодування логічного нуля. При роздільній здатності 700 зразків на символ це будуть послідовності «1110» і «1000» відповідно.



а)



б)



в)

Рис. 17. Інтерпретація сигналу передавача:
а) кнопка А передавача А; б) кнопка В передавача А;
в) кнопка А передавача В

При додаванні цих параметрів до шаблону аналізу Universal Radio Hacker (рис. 18) ми отримуємо такі повідомлення (рис. 19):

• кнопка А передавача А – 0xFF5F7 1 (1111-1111010111110111 0001) (рис. 19, повідомлення 1);

• кнопка В передавача А – 0x38860 8 (0011-1000100001100000 1000) (рис. 19, повідомлення 47);

• кнопка А передавача В – 0x1F40C 0 (0001-1111010000001100 0000)(рис.19, повідомлення 91).

Додаткова пам'ять зберігається на 24 бітах, що вказує на використання протоколу EV1527. Протокол складається з 20-бітної адреси передачі та 4-бітної пошти, що підтверджується документацією [2].

Відкриття сигналу

Щоб відкрити закритий сигнал, також використовується Universal Radio Hacker, процедура наведена нижче:

• підключіться до HackRF One і розпізнайте його на своєму комп'ютері;

• HackRF One в комп'ютерному режимі;

• відкрийте файл із корисним сигналом;

• вкладки тлумачення, натисніть кнопку відкриття;

• змінити вигляд продавця HackRF One і дізнатися інші зв'язки продавця (аналогічно пунктам 3-4 попередніх підготовок);

• повторити вибір кількості повторень передачі наполовину;

• натисніть кнопку «Пуск»;

• в результаті передачі сигналу отримано запрограмований на добу сигнал.

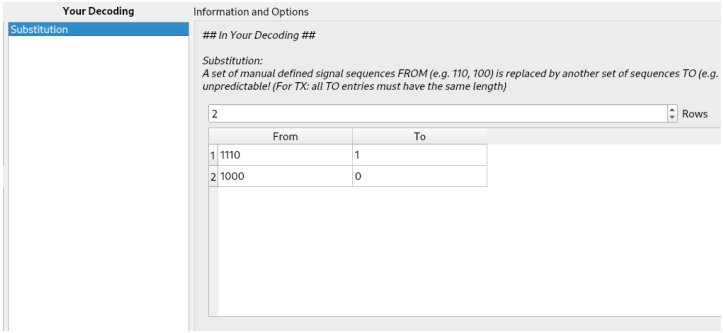


Рис. 18. Параметри кодування сигналу

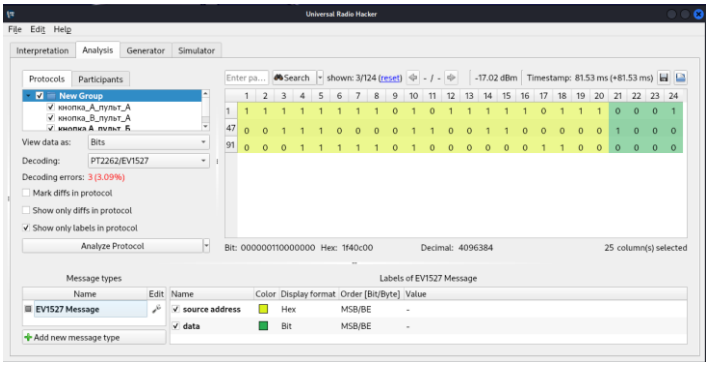


Рис. 19. Отримані повідомлення
(повторні повідомлення приховано)

ВИСНОВОК

У сучасному світі, коли цифрові технології проникають у всі сфери нашого життя, питання безпеки стає дуже актуальним. Системи віддаленого керування, які використовують статичні коди, відкриті для кількох потенційних загроз, серед яких атака повтору є однією з найпростіших і найефективніших. У цій публікації детально аналізується вразливість протоколу EV1527, який широко використовується в простих системах дистанційного керування, до такого типу атак. Лабораторне дослідження наочно демонструє, як можна здійснити атаку відтворення за допомогою спеціалізованого обладнання, тим самим підтверджуючи критичну вразливість протоколу.

Важливість цього дослідження неможливо переоцінити, оскільки воно висвітлює фундаментальні недоліки безпеки систем на основі статичного коду. Висновки, яких ми дійшли, є вагомим аргументом на користь переходу від використання застарілих технологій до більш сучасних та безпечних рішень. Системи, що використовують динамічні коди, такі як HCS301, забезпечують значно вищий рівень безпеки завдяки використанню методів криптографічного захисту даних, які ускладнюють або навіть унеможливлюють такі атаки.

Проте перехід до більш безпечних технологій має бути обдуманим і системним. Необхідно враховувати не тільки безпеку протоколів, але й специфіку їх застосування, зручність кінцевих користувачів і вартість впровадження. У деяких випадках більш прийнятним може бути використання протоколів загального призначення або спеціалізованих протоколів, які включають складні механізми безпеки. Особливо це стосується об'єктів критичної інфраструктури, які, безсумнівно, повинні бути добре захищені та стійкі з точки зору кібербезпеки [20].

Враховуючи проведені дослідження, можна зробити висновок, що безпека систем дистанційного керування є критичним аспектом, який потребує негайної уваги. Вибір обладнання та технологій має базуватися не лише на їх ефективності та простоті використання, а й на забезпеченні належного рівня безпеки. Використання динамічних кодів і криптографічних протоколів є ключовим кроком до підвищення безпеки дистанційно керованих систем від несанкціонованого доступу.

ЛІТЕРАТУРА

[1]. Banakh R., Piskozub A. (2018). Attackers' Wi-Fi devices metadata interception for their location identification. Proceedings of the 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS-SWS 2018, art. no. 8525538, pp. 112-116. DOI: 10. 1109/IDAACS-SWS.2018.8525538.

[2]. Building a poor man's quarter-wave 433MHz antenna: Antenna's construction. (n.d.). Element14. Available at: https: // community. element14.com / challenges-projects /project14 / rf /b/blog/posts/building-a-poor-man-s-quarter-wave-433mhz-antenna-antenna-s-construction.

[3]. DSTU ETSI EN 300 220-1:2018. (2018). Small range radio equipment operating in the frequency range from 25 MHz to 1000 MHz. Part 1. Technical characteristics and test methods. Kyiv.

[4]. DSTU ETSI EN 300 220-2:2017. (2019). Small range radio equipment operating in the frequency range from 25 MHz to 1000 MHz. Part 2. General technical requirements. Kyiv.

[5]. "GitHub - NanoVNA-Saver/nanovna-saver: A tool for reading, displaying and saving data from the NanoVNA." GitHub. Available at: https://github.com/NanoVNA-Saver/nanovna-saver.

[6]. "Gqrx SDR – Open-source software defined radio by Alexandru Csete OZ9AEC." Available at: https: //www.gqrx.dk/.

[7]. "GitHub - jopohl/urh: Universal Radio Hacker: Investigate Wireless Protocols Like a Boss." GitHub. Available at: https://github.com/jopohl/urh.

[8]. "History of Remote Control." Wikipedia. Retrieved from: https :// en.wikipedia.org/wiki/Remote_control#History.

[9]. NanoVNA | Very tiny handheld Vector Network Analyzer. (n.d.). Available at: https://nanovna.com/.

[10]. Open-Source RF Engineering. (n.d.). GitHub – scikit-rf/scikit-rf: RF and Microwave Engineering Scikit. GitHub. Available at: https://github.com/scikit-rf/scikit-rf.

[11]. Princeton Technology Corp. (n.d.). PT2262 remote control encoder. LCSC. Available at: https: // datasheet.lcsc.com / lcsc / 1809291408_PTC-Princeton-Tech-PT2262-S_C42793.pdf.

[12]. Rec 70-03. (1997). Relating to the use of short-range devices (SRD). Montreaux: CEPT, 93 p.

[13]. Silvan Chip Electronics Tech. Co. (n.d.). EV1527 OTP encoder. Sunrom Electronics. Available at: https://www.sunrom.com/download/EV1527.pdf.

[14]. Synoxo Inc. (2010). SYN470R Datasheet (300-450MHz ASK Receiver). Available at: https: // lcsc. com / productdetail / RF-Transceiver-ICs_Synoxo_SYN480R-FS24_Synoxo-SYN480R-FS24_C15561. html.

[15]. Synoxo Inc. (2020). SYN531R Datasheet (300MHz to 450MHz ASK Receiver). Available at: [https:// datasheet.lcsc.com / szlcsc / 1811141751_Synoxo-SYN531R_C77_C77785.pdf).

[16]. Van Capelleveen, T. (2020). Security analysis of aftermarket remote keyless entry systems for consumer vehicles. Nijmegen, 84 p.

[17]. "What is the history of the remote control?" HowStuffWorks. Retrieved from: https: // science. howstuffworks.com / innovation / everyday-innovations/remote-control-history.htm.

[18]. Yevseiev, S., Herasymov, S., Kuznietsov, O., Opirskyy, I., Volkov, A., Peleshok, Y., Sinitsyn, I., Milevskyi, S., Matovka, T., & Rizak, V. (2023). Method of assessment of frequency resolution for aircraft. Eastern-European Journal of Enterprise Technologies, 2(9 (122), pp. 34-45. https: // doi.org / 10.15587/ 1729-4061.2023.277898.

[19]. Ivan Opirskyy, Anatolii Shevchyk, Yurii Senyk, Olga Mykhaylova, Security research of bluetooth devices

based on smart watches, 2023, DOI: https://doi.org /10.18372/2225-5036.29.17548.
[20]. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et. al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: PC TECHNOLOGY CENTER, 196. doi: http: // doi.org/10. 15587/978-617-7319-57-2.

STUDY OF RESISTANCE TO ATTACKS OF REPRODUCING REMOTE CONTROL PROTOCOLS USING THE 433 MHz RADIO CHANNEL

This article identifies critical vulnerabilities in the EV1527 protocol that are widely used in remote control systems, particularly home automation systems. Focusing on a detailed analysis of the protocol structure and potential weaknesses, this study assesses the risks of replay attacks that can be carried out by intercepting and retransmitting radio signals. The results of the work demonstrate the significant vulnerability of this protocol to such attacks due to the lack of cryptographic protection of the transmitted data. As part of this work, experimental tests were conducted using the HackRF One software-controlled transceiver, which allowed to reproduction of the attack in controlled laboratory conditions. The experiments confirmed theoretical assumptions about the possibility of implementing such attacks, emphasizing the need to develop more secure communication protocols. HackRF One's application demonstrated how easily attackers can intercept and rebroadcast signals, gaining unauthorized access to remote control systems. This article highlights the importance of transitioning from legacy technologies to modern solutions that include dynamic codes and cryptography to increase security. The use of dynamic codes, such as the HCS301's moving code technology, greatly complicates the possibility of replay attacks because each code transmission is unique. This means that even if the signal is intercepted, an attacker will not be able to repeat it to gain access. The authors recommend the implementation of cryptographic methods, such as the HCS301 moving code technology, which greatly complicates the possibility of repeated attacks. The introduction of such technologies increases the level of security and makes remote control systems more resistant to malicious actions. In addition, the need for constant updating and improvement of security protocols to protect critical infrastructure is emphasized. Given these results, this work indicates an urgent need for updating and improving remote control systems, including the development of new, more attack-resistant protocols, especially in the context of ensuring the security of critical infrastructure facilities. The integration of modern cryptographic methods is a key step to protect against malicious attacks and ensure the reliable operation of remote-control systems.

Keywords: radio channel, interception, replay attack, physical security, PT2262, HackRF One, NanoVNA, EV1527.

Михайлова Ольга Олександрівна, доцент кафедри захисту інформації Національного університету «Львівська політехніка».

Olha Mykhaylova, associate professor of the Information Protection Department, Lviv Polytechnic National University.
E-mail: olha.o.mykhailova@lpnu.ua.
Orcid ID: 0000-0002-3086-3160.

Стефанків Артем Вікторович, студент кафедри захисту інформації Національного університету «Львівська політехніка».

Artem Stefankiv, student of the Information Protection Department, Lviv Polytechnic National University.
E-mail: artem.stefankiv.kb.2020@lpnu.ua.
Orcid ID: 0009-0006-8851-8358.

DOI: 10.18372/2410-7840.26.18838
УДК 004.056

СИМВОЛІКА БЕЗПЕКИ: ІНТЕГРАЦІЯ КРИПТОГРАФІЇ З КІБЕРБЕЗПЕКОЮ ДЛЯ ЗАХИСТУ ЦИФРОВИХ СИСТЕМ

Катерина Михайлишин, Іван Опірський

Кібербезпека виступає як комплекс процедур спрямованих на захист комп'ютерних систем, мереж та даних від несанкціонованого доступу. У теперішньому цифровому середовищі кібербезпека стала критично важливою для підприємницької діяльності, адміністрації та керівництва, а також для залучення приватних осіб, оскільки загрози від кібератак постійно зростають. Сучасний світ нерозривно пов'язаний з новітніми технологіями, які проникають в усі сфери нашого життя. Однак зростання залежності від цифрових технологій призводить до кіберзагроз, які можуть вплинути на безпеку та стабільність суспільства. Інтеграція криптографії з кібербезпекою є відповіддю на ці виклики. Стратегічний підхід до забезпечення безпеки інформаційної технології представляє інтеграція криптографії, що базується як забезпечення від несанкціонованого доступу і для забезпечення автентифікації та недоступності даних або систем. Злиття криптографії з кібербезпекою дозволяє створити комплексний підхід охорони цифрових систем враховуючи сучасні ризики й проблеми. Зростання кількості та складності загроз вимагає постійного вдосконалення методів, які в подальшому дозволять адаптуватися до сучасних і майбутніх атак, забезпечуючи ефективний захист цифрових систем та актуальність проблеми у сучасному цифровому світі. Дослідження в даній області стає