УКРАЇНА

(19) UA (11) 112400 (13) C2

(51) МПК (2016.01)
H04L 9/00
H04L 9/20 (2006.01)
H04L 9/34 (2006.01)
H04L 27/34 (2006.01)
H04W 12/08 (2009.01)

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки: **a 2015 11988**

(22) Дата подання заявки: **03.12.2015**

(24) Дата, з якої є чинними права на винахід: **25.08.2016**

(41) Публікація відомостей про заявку: **10.03.2016, Бюл.№ 5**

(46) Публікація відомостей про видачу патенту: **25.08.2016, Бюл.№ 16**

(72) Винахідник(и):
Ганшин Дмитро Геннадійович (UA),
Цопа Олександр Іванович (UA)

(73) Власник(и):
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ,
пр. Леніна, 14, м. Харків, 61166 (UA)

(56) Перелік документів, взятих до уваги експертизою:
US 2005055546 A1, 10.03.2005
US 20150229350 A1, 13.08.2015
RU 2439796 C2, 10.01.2012
US 6973141 B1, 06.12.2005
US 8289946 B2, 16.10.2012
US 4924516 A, 08.05.1990
WO 2005043791 A2, 12.05.2005
RU 2419204 C2, 20.05.2011
RU 2532722 C2, 10.11.2014
Трещев И.А. О подходе к скремблированию цифрового аудиопотока для защиты телефонных переговоров в условиях отсутствия шумов/И.А.Трещев// Мир науки. Научный интернет-журнал.-2014.- Вып.3. [Інтернет-публікація], URL: http://mir-nauki.com

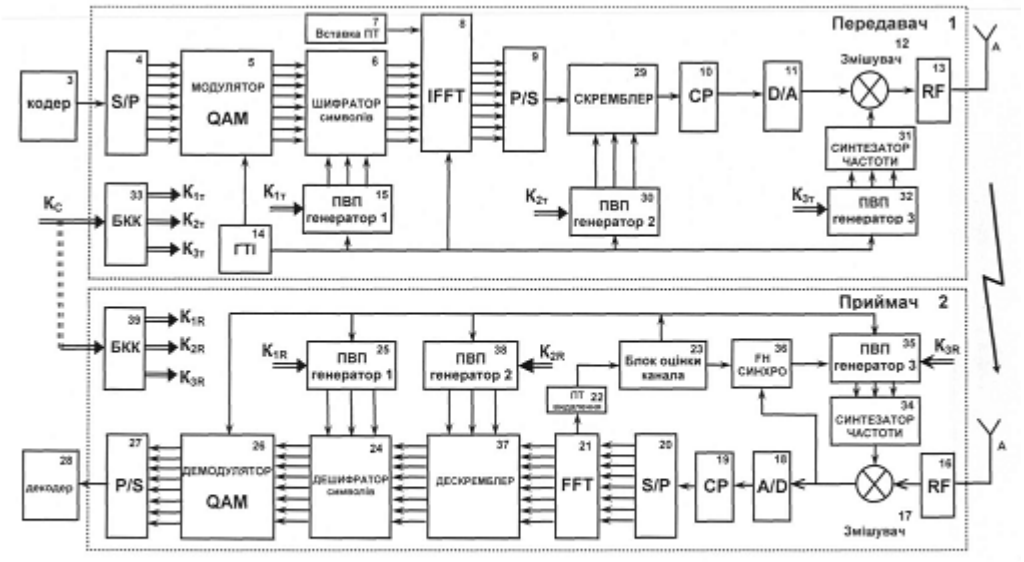
UA 112400 C2

(54) СПОСІБ ЗАХИСТУ ІНФОРМАЦІЇ НА ФІЗИЧНОМУ РІВНІ СИСТЕМИ ЗВ'ЯЗКУ З БАГАТОЧАСТОТНИМИ СИГНАЛАМИ ТА ПРИСТРІЙ ДЛЯ ЙОГО ЗДІЙСНЕННЯ

(57) Реферат:

Винахід належить до бездротових систем зв'язку з використанням багаточастотних сигналів (OFDM) в таких технологіях, як Wi-Fi, Wi-Max, LTE, DVB та інші.
Спосіб захисту інформації на фізичному рівні систем зв'язку з багаточастотними сигналами, що базується на шифруванні символів квадратурної амплітудної (QAM) модуляції піднесучих частот у відповідності з псевдовипадковою ключовою послідовністю, додатково здійснює скремблювання порядку появи символів OFDM в часовій області кожного фрейму OFDM у відповідності з другою псевдовипадковою ключовою послідовністю та псевдовипадкове перестроювання середньої частоти групового багаточастотного сигналу (FH-OFDM) при передачі кожного фрейму OFDM у відповідності з третьою псевдовипадковою ключовою послідовністю для підвищення рівня захищеності системи зв'язку від перехоплення інформації, що передається, крім того перша, друга та третя псевдовипадкові ключові послідовності формуються узгоджено з застосуванням загального системного ключа і з урахуванням структури фрейму OFDM.

Запропоновано також пристрій для реалізації способу.
Технічним результатом заявленого винаходу є підвищення скритності роботи системи зв'язку, протидії радіотехнічній розвідці та завадостійкості системи від вузько-смугових завад.



Фіг. 1

Областю використання є радіотехніка, винахід належить до бездротових систем зв'язку з використанням багаточастотних сигналів (OFDM) в таких технологіях як Wi-Fi, Wi-Max, LTE, DVB та інші.

Найбільш близьким способом є спосіб, що описаний у патенті US 2005/0055546 A1, що був опублікований 10.03.2005, МПК H04L 9/00. Схема передавальної частини прототипу складається з послідовно з'єднаних блоків: кодеру джерела даних, блока послідовно-паралельного перетворення, QAM модулятору піднесучих частот, шифратора символів, блока додавання пілот-тону, блока зворотного швидкого перетворення Фур'є (IFFT), блока паралельно-послідовного перетворення, блока введення захисного інтервалу, цифро-аналогового перетворювача, а також блока генератора тактових імпульсів, вихід якого зв'язаний з входами модулятора, блока зворотного швидкого перетворення Фур'є та генератора псевдовипадкової ключової послідовності, виходи якого підключені до керуючих входів шифратора символів. Приймальна частина складається з послідовно з'єднаних блоків: аналого-цифрового перетворювання, блока видалення захисного інтервалу, блока послідовно-паралельного перетворення, блока швидкого перетворення Фур'є (FFT), дешифратора, демодулятора QAM піднесучих частот, блок паралельно-послідовного перетворення, декодера потоку даних одержувача, а також містить блок видалення пілот-тону, вхід якого з'єднаний з виходом блока швидкого перетворення Фур'є, а вихід з'єднаний зі входом блока оцінки каналу зв'язку та синхронізації, виходи якого з'єднані зі входом демодулятора та входом генератора псевдовипадкової ключової послідовності, виходи якого підключені до керуючих входів дешифратора символів.

Розглянемо детальніше проходження сигналу в способі прототипу. Інформація, яку необхідно передати, надходить до кодера потоку даних джерела, де формується завадостійка кодова послідовність, за рахунок внесеної певної надлишковості до передаючої інформаційної послідовності, що приводить до зменшення ймовірності помилки отриманої інформаційної послідовності на приймальній частині. Блок послідовно-паралельного перетворювача формує з послідовного потоку в паралельний потік даних, після чого, в блоці QAM модулятор, кожний паралельний потік модулюється різним рівнем QAM модуляції, в залежності від співвідношення сигнал/шум у каналі зв'язку. Блок шифрування виконує шифрування QAM символів. Шифрування відбувається внаслідок перемноження послідовно комплексних чисел z_n на послідовно комплексні числа k_n, послідовність k_n надходить з блока генератора псевдовипадкової ключової послідовності. Отримуємо зашифровану послідовність v_n, $v_n = k_n * z_n$. Генерація псевдовипадкової послідовності k_n формується як $k_n = e^{j\phi\phi}$, де $0 < \phi_n < 2 \leq \pi$. Після формування зашифрованої послідовності, послідовність потрапляє до блока зворотношвидкого перетворення Фур'є (IFFT), на виході блока отримуємо сформовані піднесучі x_k:

$$x_k = \sum_{n=0}^{N-1} v_n \cdot e^{j2\cdot\pi\frac{nk}{N}}.$$

Між піднесучими додається захисний інтервал (циклічний префікс) для зменшення інтерференції в приймачі. Цифро-аналоговий перетворювач виконує перетворення цифрової послідовності (послідовність двійкових імпульсів-сигналів) на аналоговий сигнал певної модуляції в залежності від системи зв'язку. Після цифро-аналогового перетворювача сигнал потрапляє до каналу зв'язку. Аналого-цифровий перетворювач виконує перетворення на цифровий сигнал, що являє собою послідовність двійкових імпульсів-сигналів. Після чого сигнал потрапляє до блока видалення захисного інтервалу (циклічний префікс). Отримуємо паралельний потік символів після швидкого перетворення Фур'є (FFT). В дешифраторі виконується дешифрування за допомогою псевдовипадкової послідовності k_n, яка надходить з ключа генератора. Дешифрована послідовність потрапляє до QAM демодулятору, потім сигнал потрапляє до паралельно-послідовного перетворювача, вихід якого з'єднаний з декодером, на виході якого отримуємо переданий сигнал. Для нормального дешифрування сигналів в приймальній частині необхідно, щоб приймач був синхронізований з передавачем, і був відомий системний ключ. Синхронізація та оцінка каналу зв'язку є важливими параметрами для приймача, за це відповідає блок синхронізації та оцінки каналу зв'язку. Під час синхронізації окремо формується пілот-сигнал. За допомогою пілот-сигналу виконується передача службової інформації, яка необхідна для синхронізації та оцінки каналу зв'язку. Пілот-сигнал формується внаслідок окремого QAM модулятора та блока шифрування, отримує ключ від генератора ключа, після чого потрапляє до блока швидкого перетворення Фур'є, а вихід з'єднаний зі входом

блока оцінки каналу зв'язку та синхронізації. Внаслідок чого отримуємо окремо зашифрований пілот-сигнал.

Забезпечення скритності системи зв'язку є одним із важливих вимог інформаційної безпеки відомчих систем зв'язку. Під скритністю розуміється здатність систем та засобів радіозв'язку протидіяти радіотехнічній розвідці, яка вимагає три основні задачі: вияв факту роботи системи зв'язку (вияв сигналу); визначення структури виявленого сигналу та його основних параметрів; розкриття інформації, що передається.

В системах, в яких використовується більше змінних параметрів для шифрування даних на фізичному рівні, підвищується скритність та зменшені ймовірності виявлення факту роботи системи зв'язку.

Недоліком способу та схеми прототипу є використання тільки однієї змінної для шифрування даних на фізичному рівні, що призводить до зменшення скритності сигналу в порівнянні з системами, в яких використовується більше змінних параметрів.

Технічною задачею пропонованого винаходу є створення способу і пристрою, в яких ефективно виконується шифрування даних на фізичному рівні систем зв'язку з багаточастотними сигналами та підвищується скритність роботи системи зв'язку, що в свою чергу підвищує протидію радіотехнічній розвідці та підвищує завадостійкість системи від вузько-смугових завад.

Ця задача вирішена наступним чином. У способі захисту інформації на фізичному рівні системи зв'язку з багаточастотними сигналами, який базується на шифруванні символів квадратурної амплітудної (QAM) модуляції піднесучих частот у відповідності з псевдовипадковою ключовою послідовністю, згідно з винаходом, додатково вводиться скремблювання порядку появи символів OFDM в часовій області кожного фрейму OFDM у відповідності з другою псевдовипадковою ключовою послідовністю та псевдовипадкове перестроювання середньої частоти групового багаточастотного сигналу (FH-OFDM) при передачі кожного фрейму OFDM у відповідності з третьою псевдовипадковою ключовою послідовністю для підвищення рівня захищеності системи зв'язку від перехоплення інформації, що передається, крім того перша, друга та третя псевдовипадкові ключові послідовності формуються узгоджено з застосуванням загального системного ключа і з урахуванням структури фрейму OFDM.

У пристрої для захисту інформації на фізичному рівні системи зв'язку з багаточастотними сигналами, що складається з передавача та приймача, при цьому передавач містить послідовно з'єднані кодер потоку даних джерела, перший блок послідовно-паралельного перетворення, перший модулятор QAM піднесучих частот, шифратор символів, блок додавання пілот-тону, блок зворотного швидкого перетворення Фур'є (IFFT), перший блок паралельно-послідовного перетворення, блок введення захисного інтервалу, цифро-аналоговий перетворювач, перший змішувач, перший радіохвильовий процесор, генератор тактових імпульсів, перший генератор псевдовипадкової ключової послідовності, де вихід генератора тактових імпульсів зв'язаний з входом модулятора QAM, виходи якого підключені до керуючих входів шифратора символів, виходи першого генератора псевдовипадкової ключової послідовності підключені до керуючючих входів шифратора символів, приймач містить послідовно з'єднані другий радіохвильовий процесор, другий змішувач, аналого-цифровий перетворювач, блок видалення захисного інтервалу, другий блок послідовно-паралельного перетворення, блок швидкого перетворення Фур'є (FFT), блок видалення пілот-сигналу, дешифратор символів, четвертий генератор псевдовипадкової послідовності, блок оцінки каналу зв'язку, блок синхронізації, демодулятор QAM піднесучих частот, другий блок паралельно-послідовного перетворення, декодер потоку даних отримувача, де виходи четвертого генератора псевдовипадкової ключової послідовності підключені до керуючих входів дешифратора символів, вхід блока синхронізації з'єднаний з виходом аналого-цифрового перетворювача, вхід блока оцінки каналу з'єднаний з виходом блока видалення пілот-сигналу, який відрізняється тим, що передавач додатково містить перший блок керування ключами, другий та третій генератори псевдовипадкової ключової послідовності, скремблер, перший синтезатор частоти, де на вхід першого блока керування ключами подають системний ключ, а виходи з'єднані з відповідними входами першого, другого та третього генераторів псевдовипадкової ключової послідовності, вхід скремблера з'єднано з виходом першого блока паралельно-послідовного перетворення, а вихід з входом блока введення захисного інтервалу, керуючі входи скремблера підключені до виходів другого генератора псевдовипадкової ключової послідовності, вихід першого синтезатора частоти підключено до першого змішувача, а керуючі входи першого синтезатора частоти - до виходів третього генератора псевдовипадкової ключової послідовності, вихід генератора тактових імпульсів підключено до

тактових входів другого та третього генераторів псевдовипадкової ключової послідовності, приймач додатково містить другий синтезатор частоти, дескремблер, п’ятий та шостий генератори псевдовипадкової ключової послідовності, другий блок керування ключами, де вихід другого синтезатора частоти підключено до другого змішувача, а керуючі входи - до виходів шостого генератора псевдовипадкової ключової послідовності, виходи блока оцінки каналу зв'язку підключені до тактових входів четвертого, п’ятого та шостого генераторів псевдовипадкових ключових послідовностей, а також до блока синхронізації, вихід якого зв'язано з додатковим входом шостого генератора псевдовипадкової ключової послідовності, входи дескремблера підключені до виходів блока швидкого перетворення Фур'є (FFT), виходи з'єднані з входами дешифратора символів, керуючі входи дескремблера підключені до виходів п’ятого генератора псевдовипадкової ключової послідовності, на вхід другого блока керування ключами подається системний ключ, а виходи з'єднані з відповідними входами четвертого, п’ятого та шостого генераторів псевдовипадкової ключової послідовності.

На фіг. 1 зображено структурну схему запропонованого пристрою.

На фіг. 2 зображено структуру скремблювання та дескремблювання порядку видачі символів OFDM.

На фіг. 3 зображено утворення псевдовипадкової перестройки частоти OFDM фрейму.

Пропонований спосіб підвищує скритність роботи системи зв'язку, та збільшує завадостійкість. Для реалізації цього способу потрібен новий пристрій. Його вдосконалена схема передавача та приймача наведена на фіг. 1. Передавач 1 складається з послідовно з'єднаних блоків: кодера 3 потоку даних джерела, блока послідовно-паралельного перетворення 4 (S/P), модулятора QAM 5 піднесучих частот, шифратора 6 символів, блока зворотного швидкого перетворення Фур'є 8 (IFFT), блока паралельно-послідовного перетворення 9 (P/S), скремблер 29, блока введення захисного інтервалу 10 (CP), цифро-аналогового перетворювача 11 (D/A), змішувача 12, блок радіохильового процесору 13 (RF). Блок БКК (блок керування ключем) 33 має три виходи, $К_{1Т}$, $К_{2Т}$, $К_{3Т}$, перший $К_{1Т}$ вихід підключений до блока генератора псевдо випадкової послідовності 15 (ПВП), який в свою чергу підключений до шифратора 6. Другий вихід $К_{2Т}$ підключений до блока генератора псевдовипадкової послідовності 30 (ПВП), котрий підключений до скремблера 29. Третій вихід $К_{3Т}$ підключений до блока генератора псевдовипадкової послідовності 32 (ПВП), вихід якого з'єднаний з синтезатором частоти 31. Вихід синтезатора частоти з'єднаний зі змішувачем 12. Блок генератор тактового імпульсу (ГТИ) 14 має два виходи: перший вихід з'єднаний з модулятором QAM 5, других паралельно з'єднує чотири блоки генератор псевдовипадкової послідовності 15 (ПВП), 30 (ПВП), 32 (ПВП) та блок зворотного швидкого перетворення Фур'є (IFFT) 8. Вихід блока вставка пілот-сигнал 7 (ПТ) підключений до блока зворотного швидкого перетворення Фур'є (IFFT) 8. Прийомна частина приймача 2 складається з послідовно з'єднаних блоків: блок радіохильового процесору 16 (RF), змішувач 17, аналого-цифровий перетворювач 18 (A/D), блок видалення захисного інтервалу 19 (CP), блок послідовно-паралельного перетворення 20 (S/P), блок швидкого перетворення Фур'є (FFT) 21, дескремблер 37, дешифратор 24, демодулятор QAM 26 підносійних частот, блок паралельно-послідовного перетворення 27 (P/S), декодеру 28 потоку даних отримувача. Блок БКК (блок керування ключем) 39 має три виходи, $К_{1R}$, $К_{2R}$, $К_{3R}$, перший вихід $К_{1R}$ підключений до блока генератор псевдо випадкової послідовності 25 (ПВП), який в свою чергу підключений до дешифратора 24. Другий вихід $К_{2R}$ підключений до блока генератор псевдо випадкової послідовності 38 (ПВП), котрий підключений до дескремблера 37. Третій вихід $К_{3R}$ підключений до блока генератор псевдо випадкової послідовності 35 (ПВП), вихід якого з'єднаний з синтезатором частоти 34. Вихід синтезатора частоти з'єднаний зі змішувачем 17. Вихід блока швидкого перетворення Фур'є (FFT) 21 з'єднаний з блоком видалення пілот-сигнал 22 (ПТ) який послідовно з'єднаний з блоком оцінки каналу 23 котрий має два виходи. Перший вихід з'єднаний з блоком FH синхро 36 що має один вхід и один вихід, вихід з'єднаний з блоком генератор псевдовипадкової послідовності 35 (ПВП), вхід підключений з виходом змішувача 17. Другий вихід блока оцінки каналу паралельно з'єднаний з блоками: генераторами псевдовипадкової послідовності 35 (ПВП), 38 (ПВП), 25 (ПВП) та блоком демодулятор QAM26.

Розглянемо більш детальніше роботу запропонованого пристрою, який здійснює спосіб захисту інформації на фізичному рівні системи зв'язку з багаточастотними сигналами. Інформація, яку необхідно передати поступає до кодеру 3, де формується завадостійка кодова послідовність, за рахунок внесеної певної надлишковості до передаючої інформаційної послідовності, що приводить до зменшення ймовірності помилки отриманої інформаційної послідовності на приймальній частині. На виході кодеру 3 отримуємо послідовний потік даних. Блок послідовно-паралельного перетворення 4 (S/P) формує з послідовного потоку в

паралельний потік двійковий код для подальшого формування несучих. До блока модулятор QAM 5 надходять паралельні потоки, кожний потік модулюється різним рівнем QAM модуляцією в залежності від заданого відношення сигнал/шум. Блок шифратор символів 6 виконує шифрування паралельно модульованих потоків в псевдовипадковій послідовності, ключ псевдо випадкової послідовності надходить з блока генератор псевдовипадкової послідовності 15 (ПВП). Блок зворотного швидкого перетворення Фур'є (IFFT) 8 виконує роль створення піднесучих, та виконується створення пілот-сигналу оскільки блок вставка пілот-сигнал 7 (ПТ) підключений до блока зворотного швидкого перетворення Фур'є (IFFT) 8. Перетворення паралельної послідовності в послідовну відбувається в блоці блока паралельно-послідовного перетворення 9 (P/S). Після цього сигнал потрапляє до блока сркемблер 29 в якому формується псевдо випадкова послідовність символів, оскільки другий вхід скремблера підключений до генератора псевдо випадкової послідовності 30 (ПВП). Блок введення захисного інтервалу 10 (CP) створює захисний інтервал між піднесучими частотами для кращого прийому сигналу приймачем. Цифро-аналоговий перетворювач 11 (D/A) виконує перетворення цифрової послідовності (послідовність двійкових імпульсів-сигналів) на аналоговий сигнал певної модуляції в залежності від системи зв'язку. Після проходження сигналу цифро-аналогового перетворювача сигнал потрапляє до змішувача 12. Змішувач має два входи и один вихід. Перший вхід з'єднаний з цифро-аналоговим перетворювачем, другий вхід з'єднаний з виходом синтезатора частоти 31, в свою чергу синтезатор частоти має вхід який з'єднаний з виходом генератором псевдо випадкової послідовності 32 (ПВП). На виході змішувача отримуємо сигнал с псевдовипадковою перестройкою частоти після чого потрапляє до радіохвильового процесору 13 (RF), після якого сигнал потрапляє до антени (A). Після прийому сигналу на антенні (A) приймача сигнал потрапляє до блока радіохвильового процесору 16 (RF) після якого сигнал потрапляє до змішувача 17 другий вхід змішувача з'єднаний з синтезатором частоти 34. На вхід синтезатора частоти подається сигнал з генератора псевдо випадкової послідовності 35 (ПВП) який має два входи. На один вхід з'єднаний з блоком керування ключем БКК 39, другий вхід з'єднаний з блоком FH синхро 36 що відповідає за синхронізацію символьної послідовності. Блок FH синхро 36 має два входи: один вхід з'єднаний з виходом змішувача 17 інший вхід з'єднаний з блоком оцінки каналу 23, який має ще вихід, який з'єднаний з генератор псевдо випадкової послідовності 35 (ПВП), 38 (ПВП), 25 (ПВП) та блоком демодулятор QAM 26. Блок оцінки каналу 23 має вхід, який з'єднаний з блоком видалення пілот-сигналу 22 (ПТ), вхід якого з'єднаний з блоком перетворення Фур'є (FFT) 21. Блоки генераторів псевдовипадкових послідовностей 35 (ПВП), 38 (ПВП) та 25 (ПВП) мають вхідне з'єднання з блоком керування ключем БКК 39 який задає алгоритм псевдовипадкової послідовності. Аналого-цифровий перетворювач 18 (A/D) виконує перетворення у цифровий сигнал, що являє собою послідовність двійкових імпульсів - сигналів, які набувають двох значень. Після чого сигнал потрапляє до блок видалення захисного інтервалу 19 (CP). Блок послідовно-паралельне перетворення 20 (S/P) виконує перетворення послідовного потоку в паралельні потоки, після чого виконується швидке перетворення Фур'є (FFT) 21. Дескремблер 37 перетворює псевдовипадкову послідовність символів до послідовності, яка надходила до скремблеру 29. Дешифратор 24 відтворює паралельний потік до шифрування шифратором 6. Дешифрована паралельна послідовність потрапляє до демодулятору QAM 26, після чого сигнал потрапляє до паралельно-послідовного перетворювача 27 (P/S) вихід якого з'єднаний з декодером 28 на виході якого отримуємо переданий сигнал.

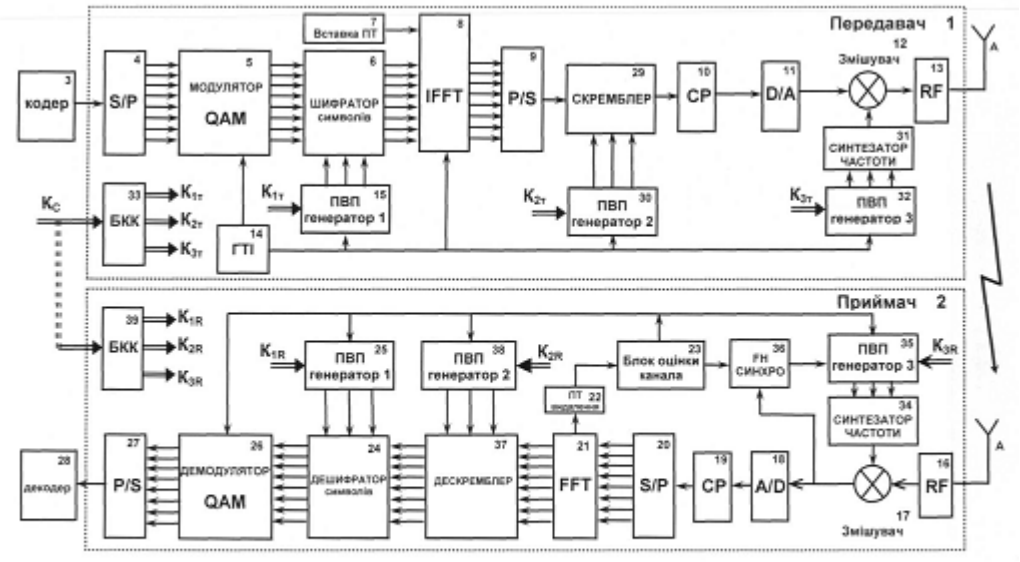
Таким чином досягнуто: зменшення вияву факту роботи системи зв'язку, тобто збільшується скритність системі, та зменшення ймовірності визначення структури сигналу та його основних параметрів, що забезпечить в загалом захищеність системи зв'язку.

ФОРМУЛА ВИНАХОДУ

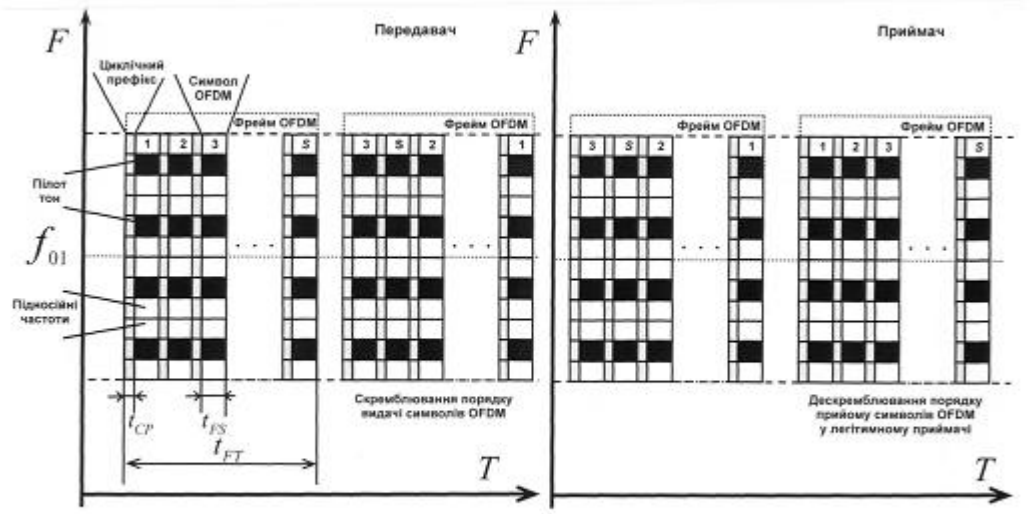
1. Спосіб захисту інформації на фізичному рівні систем зв'язку з багаточастотними сигналами, що базується на шифруванні символів квадратурної амплітудної (QAM) модуляції піднесучих частот у відповідності з псевдовипадковою ключовою послідовністю, який **відрізняється** тим, що додатково здійснюють скремблювання порядку появи символів OFDM в часовій області кожного фрейму OFDM у відповідності з другою псевдовипадковою ключовою послідовністю та псевдовипадкове перестроювання середньої частоти групового багаточастотного сигналу (FH-OFDM) при передачі кожного фрейму OFDM у відповідності з третьою псевдовипадковою ключовою послідовністю для підвищення рівня захищеності системи зв'язку від перехоплення інформації, що передається, крім того першу, другу та третю псевдовипадкові ключові

послідовності формують узгоджено з застосуванням загального системного ключа і з урахуванням структури фрейму OFDM.

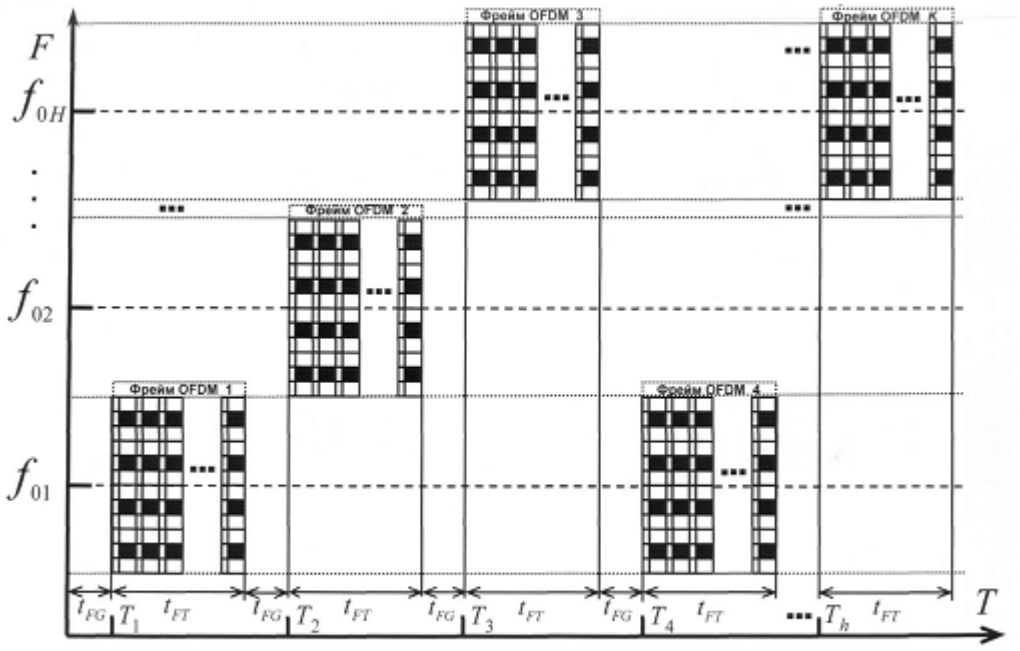
2. Пристрій для захисту інформації на фізичному рівні системи зв'язку з багаточастотними сигналами, що складається з передавача та приймача, при цьому передавач містить послідовно з'єднані кодер потоку даних джерела, перший блок послідовно-паралельного перетворення, перший модулятор QAM піднесучих частот, шифратор символів, блок додавання пілот-тону, блок зворотного швидкого перетворення Фур'є (IFFT), перший блок паралельно-послідовного перетворення, блок введення захисного інтервалу, цифро-аналоговий перетворювач, перший змішувач, перший радіохвильовий процесор, генератор тактових імпульсів, перший генератор псевдовипадкової ключової послідовності, де вихід генератора тактових імпульсів зв'язаний з входом модулятора QAM, виходи якого підключені до керуючих входів шифратора символів, виходи першого генератора псевдовипадкової ключової послідовності підключені до керуючих входів шифратора символів, приймач містить послідовно з'єднані другий радіохвильовий процесор, другий змішувач, аналого-цифровий перетворювач, блок видалення захисного інтервалу, другий блок послідовно-паралельного перетворення, блок швидкого перетворення Фур'є (FFT), блок видалення пілот-сигналу, дешифратор символів, четвертий генератор псевдовипадкової послідовності, блок оцінки каналу зв'язку, блок синхронізації, демодулятор QAM піднесучих частот, другий блок паралельно-послідовного перетворення, декодер потоку даних отримувача, де виходи четвертого генератора псевдовипадкової ключової послідовності підключені до керуючих входів дешифратора символів, вхід блока синхронізації з'єднаний з виходом аналого-цифрового перетворювача, вхід блока оцінки каналу з'єднаний з виходом блока видалення пілот-сигналу, який **відрізняється** тим, що передавач додатково містить перший блок керування ключами, другий та третій генератори псевдовипадкової ключової послідовності, скремблер, перший синтезатор частоти, де на вхід першого блока керування ключами подають системний ключ, а виходи з'єднані з відповідними входами першого, другого та третього генераторів псевдовипадкової ключової послідовності, вхід скремблера з'єднано з виходом першого блока паралельно-послідовного перетворення, а вихід - з входом блока введення захисного інтервалу, керуючі входи скремблера підключені до виходів другого генератора псевдовипадкової ключової послідовності, вихід першого синтезатора частоти підключено до першого змішувача, а керуючі входи першого синтезатора частоти - до виходів третього генератора псевдовипадкової ключової послідовності, вихід генератора тактових імпульсів підключено до тактових входів другого та третього генераторів псевдовипадкової ключової послідовності, приймач додатково містить другий синтезатор частоти, дескремблер, п'ятий та шостий генератори псевдовипадкової ключової послідовності, другий блок керування ключами, де вихід другого синтезатора частоти підключено до другого змішувача, а керуючі входи - до виходів шостого генератора псевдовипадкової ключової послідовності, виходи блока оцінки каналу зв'язку підключені до тактових входів четвертого, п'ятого та шостого генераторів псевдовипадкових ключових послідовностей, а також до блока синхронізації, вихід якого зв'язано з додатковим входом шостого генератора псевдовипадкової ключової послідовності, входи дескремблера підключені до виходів блока швидкого перетворення Фур'є (FFT), виходи з'єднані з входами дешифратора символів, керуючі входи дескремблера підключені до виходів п'ятого генератора псевдовипадкової ключової послідовності, на вхід другого блока керування ключами подається системний ключ, а виходи з'єднані з відповідними входами четвертого, п'ятого та шостого генераторів псевдовипадкової ключової послідовності.


Передавач 1
Приймач 2
кодер
S/P
МОДУЛЯТОР QAM
ШИФРАТОР символів
Вставка ПТ
IFFT
P/S
СКРЕМБЛЕР
CP
D/A
Змішувач
RF
СИНТЕЗАТОР ЧАСТОТИ
БКК
ГТІ
ПВП генератор 1
ПВП генератор 2
ПВП генератор 3
Блок оцінки канала
FH СИНХРО
ПТ
FFT
DESCRAMBLER
ДЕШИФРАТОР символів
ДЕМОДУЛЯТОР QAM
A/D
декодер

Фіг. 1


Передавач
Приймач
Циклічний префікс
Символ OFDM
Фрейм OFDM
Пілот тон
Підносійні частоти
Скремблювання порядку видачі символів OFDM
Дескремблювання порядку прийому символів OFDM у легітимному приймачі
F
T

Фіг. 2



Фіг. 3

Комп'ютерна верстка Д. Шеверун

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601