РЕКОМЕНДОВАНО
Експертною комісією з питань проведення державної експертизи в сфері криптографічного захисту інформації Держспецзв’язку (протокол від 09.07.2022 № 551)

# РЕКОМЕНДАЦІЇ

## з програмування, конфігурування параметрів безпеки та функцій захисту інформації в радіостанціях цифрової системи радіозв'язку Motorola Solutions MOTOTRBO™ стандарту DMR

Київ - 2022

## 1. ТЕРМІНИ ТА СКОРОЧЕННЯ

У даному документі використовуються наступні терміни і скорочення:

**DMR** - Digital Mobile Radio (цифровий рухомий радіозв'язок), відкритий стандарт цифрового радіозв’язку для користувачів професійного рухомого радіозв’язку (PMR) за стандартами Європейського інституту телекомунікаційних стандартів (ETSI) TS 102 361, частини 1-4;

**ETSI** - European Telecommunications Standards Institute (Європейський інститут телекомунікаційних стандартів);

**TDMA** - Time Division Multiple Access (Множинний доступ з розподілом у часі);

**Розмовна група (Talkgroup)** – віртуальний радіоканал, створений для магістральних радіосистем.

## 2. РОЗРОБНИКИ РЕКОМЕНДАЦІЙ

Рекомендації розроблялись Зведеною оперативною групою Держспецзв’язку спільно з офіційним представником компанії Motorola в Україні ТОВ «ДОЛЯ І КО. ЛТД».

## 3. ЗАГАЛЬНІ ВІДОМОСТІ

MOTOTRBO™ — це цифрова система радіозв'язку компанії Motorola. Система заснована на європейському стандарті DMR з двома слотами та сумісна з ним і використовує множинний доступ з поділом часу (TDMA) для ефективного розміщення двох користувачів одночасно. Організація двох логічних каналів зв'язку в межах одного радіоканалу 12,5 кГц дозволяє скоротити потребу у частотному ресурсі вдвічі. Один фізичний канал 12,5 кГц здатний передавати дві одночасні та незалежні розмови або одночасні та незалежні канали голосу та даних, кожен з яких еквівалентний 6,25 кГц. В системі MOTOTRBO™ реалізовано роботу різних розмовних груп, передачу мови подібно до транкінгу, роботу в широкому радіусі через IP-з'єднання. Приймачі та ретранслятори MOTOTRBO можуть бути ретросумісними з аналоговим FM за допомогою CTCSS або CDCSS.

Технічно стандарт DMR є структурою таймслотів з тривалістю 30 мілісекунд. У цьому проміжку часу 27.5 мс призначаються безпосередньо для корисної інформації, що кодується 216 бітами, а решта часу - 48 бітів супроводу. У DMR можливі два режими – симплексний зв'язок та двочастотний

симплекс з дуплексним розносом (за наявності ретранслятора). У першому режимі виграшу за щільністю передачі не буде, оскільки система залишиться одноканальною подібно аналоговій. У другому випадку реалізується два незалежні голосові з'єднання в одному частотному каналі.

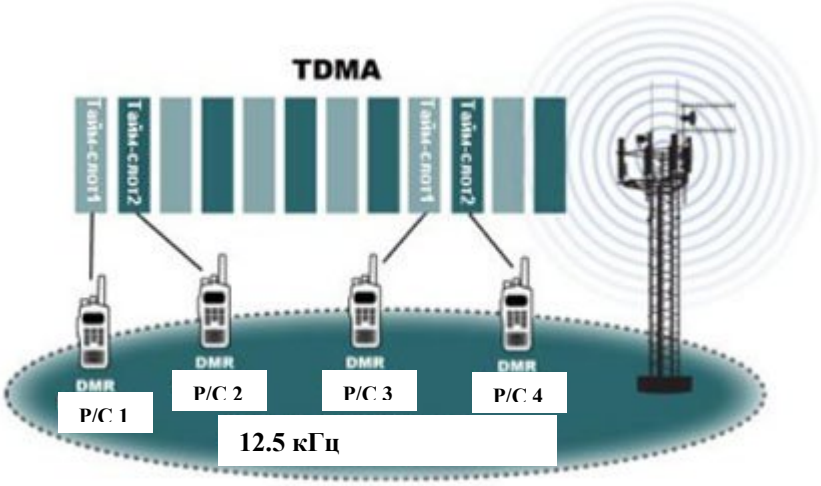


Рис. 1. TDMA структура стандарту DMR

Устаткування MOTOTRBO™ базується на наступних стандартах ETSI :

- ETSI TS 102 361-1 Повітряний інтерфейс
- ETSI TS 102 361-2 Голосові та загальні послуги та засоби
- ETSI TS 102 361-3 Протокол даних
- ETSI TS 102 361-4 Протокол транкингу

Стандарти є відкритими, що гарантує користувачам реалізацію певного набору функціональних можливостей та сумісність між собою обладнання різних виробників.

В системі MOTOTRBO™ для передачі голосу та даних використовується цифрова модуляція 4FSK з наступними індикаторами випромінювання:

- 7K60F1D і 7K60FXD (2-слотовий DMR TDMA дані);
- 7K60F1E і 7K60FXE (2-слотовий DMR TDMA голос);
- 7K60F1W (2-слотовий DMR TDMA дані + голос).

MOTOTRBO підтримує IPv4-адресацію та використовує одноадресну UDP/IP для передачі голосу та даних між радіостанціями та ретрансляторами. Голос стискається та кодується за допомогою вокодера AMBE+2 від DVSI Inc. Цей вокодер дозволяє працювати з двома часовими слотами на одному каналі 12,5 кГц, зменшити фоновий шум, використовувати шифрування AES, здійснювати передачу сигналів телеметрії.

Система MOTOTRBO вимагає достатньої пропускної здатності IP для передачі голосу та даних між ретрансляторами і , як правило, вимагає стабільної затримки в обидва боки менше ніж приблизно 700 мс. Багатоадресна передача не використовується для зворотного зв'язку IP.

Motorola розробила три транкінгові системи для MOTOTRBO: Connect Plus, Capacity Plus і Capacity Max.

Дані Рекомендації призначені для вивчення обслуговуючим персоналом роботи програмного забезпечення MOTOTRBO CPS 2.0 і містить відомості, які необхідні для забезпечення правильного програмування обладнання з метою повного використання його технічних можливостей.

MOTOTRBO CPS 2.0 відрізняється деякими новими, унікальними функціями від MOTOTRBO CPS.

Програмне забезпечення MOTOTRBO CPS 2.0 може відкривати файли з розширенням .ctb2 та .ctb

Одночастно на комп'ютері може бути встановлено ПЗ MOTOTRBO CPS ver.16.0 та CPS 2.0 ver.02.21.61.0.

Для того щоб CPS2.0 міг працювати з обладнанням MotoTRBO версії нижче r02.10.0 на комп'ютері повинно бути встановлено ПЗ CPS (крайня версія - ver.16.0).

## 4. ЗАХОДИ З ПРОТИДІЇ ПЕЛЕНГАЦІЇ, РАДІОПЕРЕХОПЛЕННЮ ТА ПОВ'ЯЗАНИХ З ЦИМ ПРОВОКАЦІЙ

4.1 Обов'язковим елементом забезпечення захисту в радіостанціях є шифрування цифрових каналів за допомогою ключів шифрування. В базовому пакеті налаштувань радіостанцій Motorola є можливість використовувати 40-бітні ключі шифрування (Рис. 2).

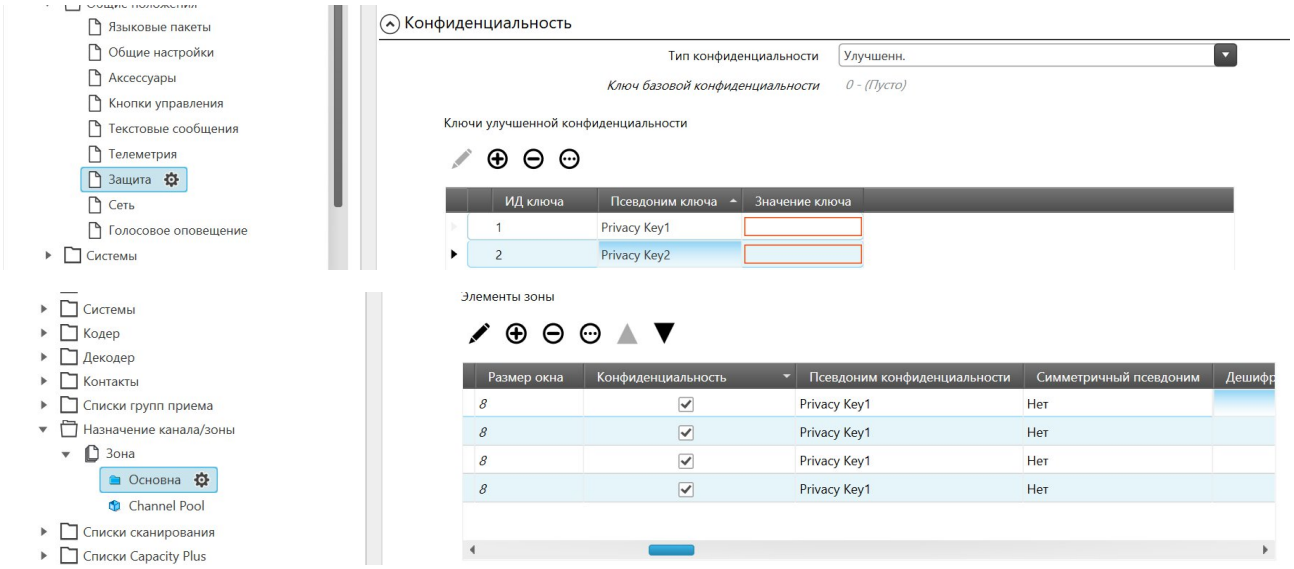


Рис. 2

Для кожного з каналів адміністратор (зв'язківець) може створити окремий ключ. Таким чином в разі перехоплення та злому каналу зв'язку, є можливість здійснити перехід на резервні канали, які використовують інші ключі шифрування.

4.2 У випадку отримання ліцензії на використання більш стійких до злому ключів, а саме, 256 біт (Рис. 3), адміністратор (зв'язківець) має у найкоротший час змінити ключі шифрування на всіх радіостанції у підрозділі на більш стійкі.

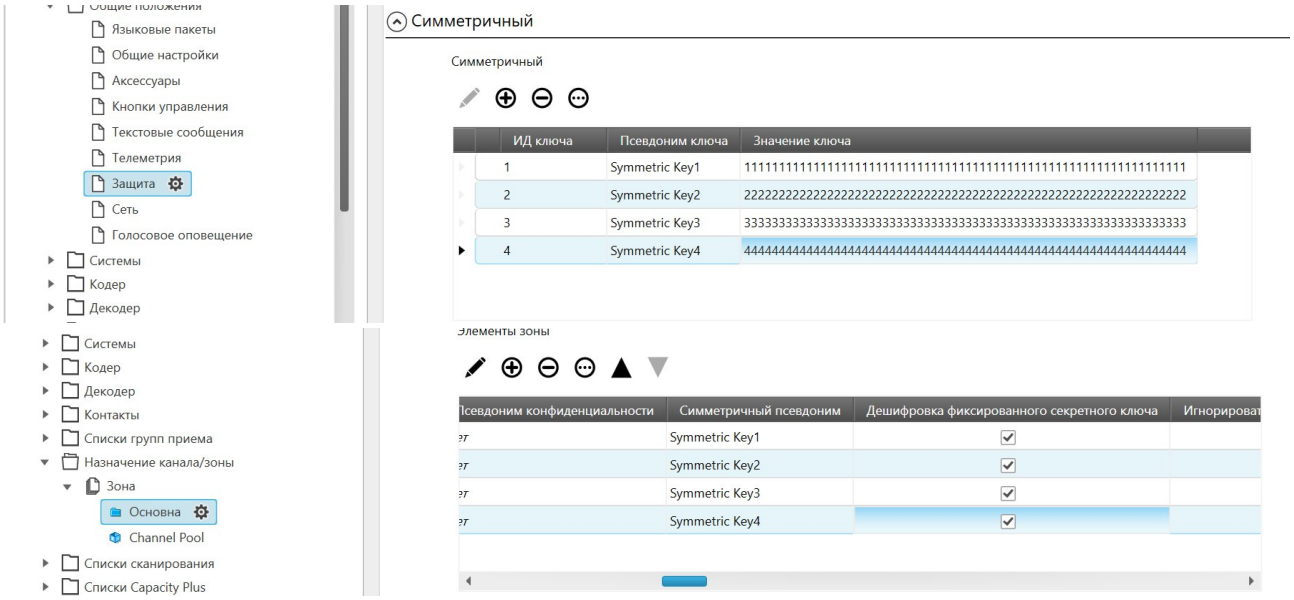


Рис. 3

4.3 З метою унеможливлення провокацій та нав'язувань спотвореної (неправдивої) інформації ворогом через передачу ним нешифрованих викликів на каналах прийому з шифруванням ОБОВ'ЯЗКОВО:

в усіх радіостанціях застосовувати функцію «**Ігнорування прийому нешифрованих голосових/пакетних даних**» (Рис. 4).

4.4 З метою унеможливлення провокацій та нав'язувань спотвореної (неправдивої) інформації ворогом через передачу ним викликів з застосуванням застарілого або скомпроментованого ключа шифрування ОБОВ'ЯЗКОВО:

в усіх радіостанціях застосовувати функцію «**Дешифровка фіксованого секретного ключа**» (Рис. 4).

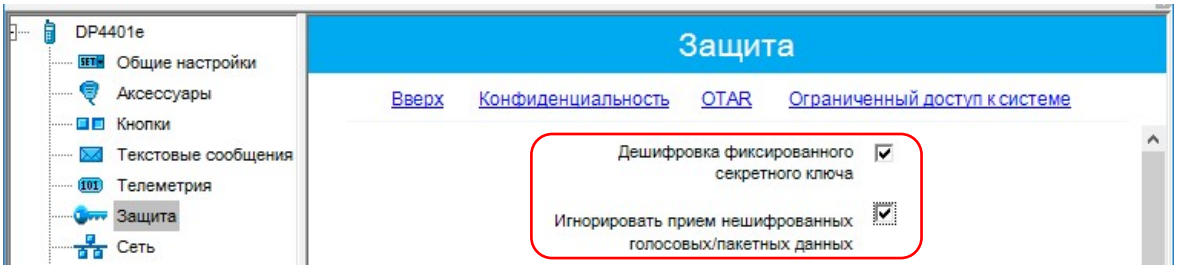


Рис. 4

4.5 Для запобігання навмисного неавторизованого дистанційного блокування радіостанцій, РЕКОМЕНДОВАНО або повністю вимикати можливість блокування радіостанції (зняття галочки біля функції «Декодування деактивації радіостанції») або, за наявності в радіостанції функції авторизованого блокування, використовувати Блокування/розблокування

автентифікованої радіостанції» - «Автентифікація користувача» за встановленим паролем/кодовою фразою (рис. 5).

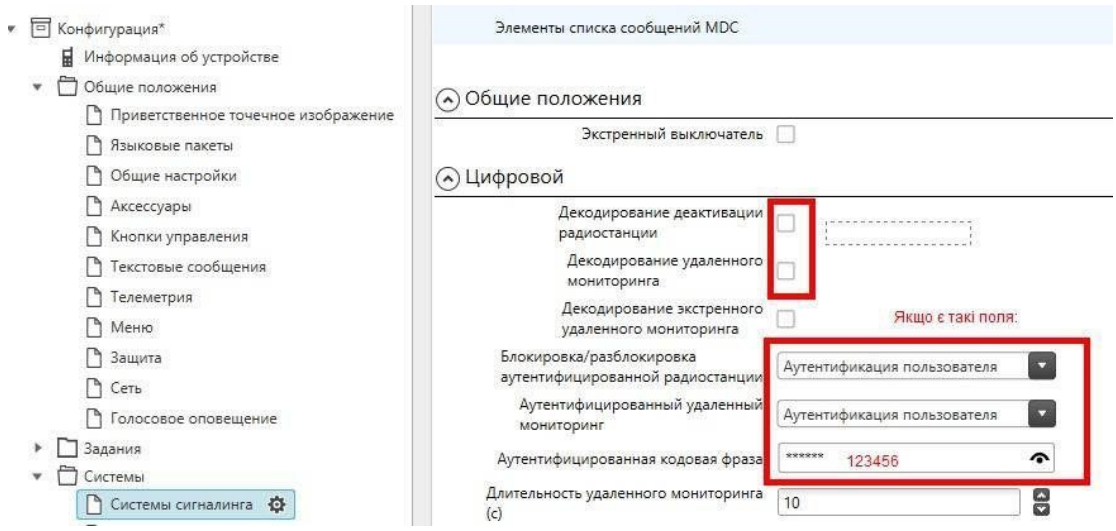


Рис. 5

4.6 Для виключення несанкціонованого реагування радіостанцій на будь-які зовнішні запити до них по радіоканалу, наприклад, запит на наявність в мережі, пінг по радіоканалу, підтвердження доставки текстового повідомлення та інше, РЕКОМЕНДОВАНО застосовувати в радіостанціях функцію «Заборона реагування» (Рис. 6). При активації даної функції залишається можливість санкціонованого виходу на передачу через натискання користувачем тангенти радіостанції. Функція активується натисканням на радіостанції відповідної заздалегідь запрограмованої кнопки «Заборона відповіді Вмик./Вимк.».

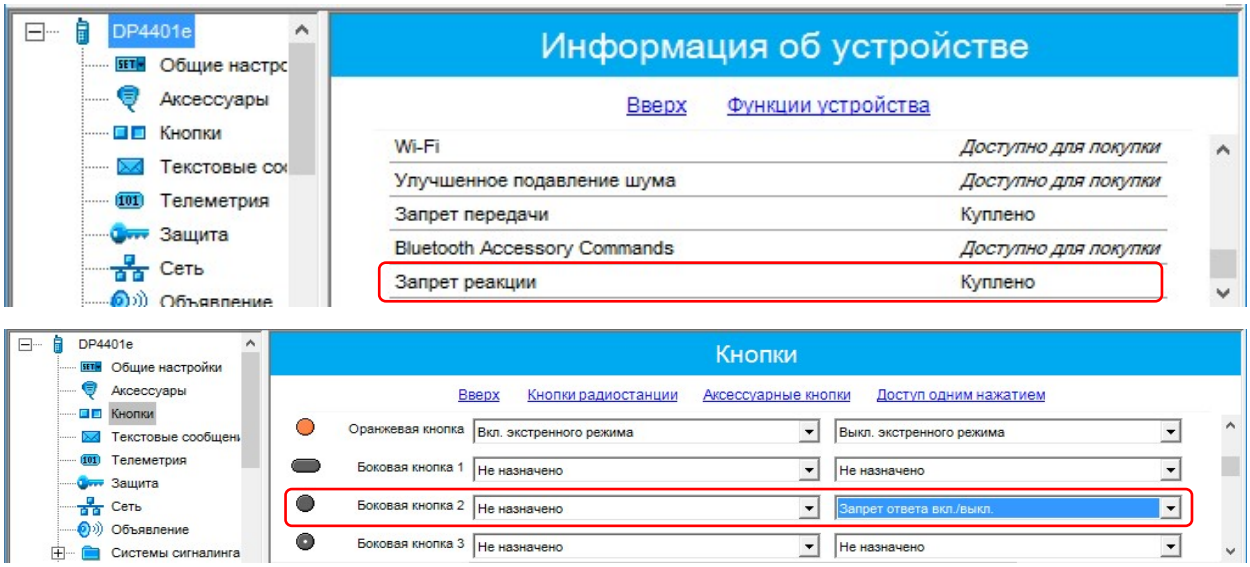


Рис. 6

4.7 З метою зменшення ризику несанкціонованої пеленгації радіозасобів та забезпечення прихованої роботи в радіоефірі під час проведення спеціальних заходів

РЕКОМЕНДОВАНО:

4.7.1 У разі застосування мобільних ретрансляторів або ранцевих радіостанцій для локального зв’язку з віддаленими кореспондентами використовувати спрямовані антени. При цьому прихованість досягається за рахунок:

- зменшення потужності передавача, яка компенсується більшим коефіцієнтом підсилення антени у напрямку на кореспондента;

- меншою радіопомітністю в напрямках, відмінних від напрямку на кореспондента, через малий коефіцієнт підсилення антени у тильному та бічних напрямах.

4.7.2 В «Загальних налаштуваннях» мобільного ретранслятора слід застосовувати наступні налаштувння:

4.7.2.1 Мінімальне значення параметру «Таймер неактивності абонента» –1000 мс (при цьому автоматично зменшиться значення таймерів часу очікування групового та приватного викликів) (рис. 7). При цьому в усіх радіостанціях, що працюватимуть через мобільний ретранслятор, слід налаштувати відповідні таймери з однаковим значеннями з ретранслятора;

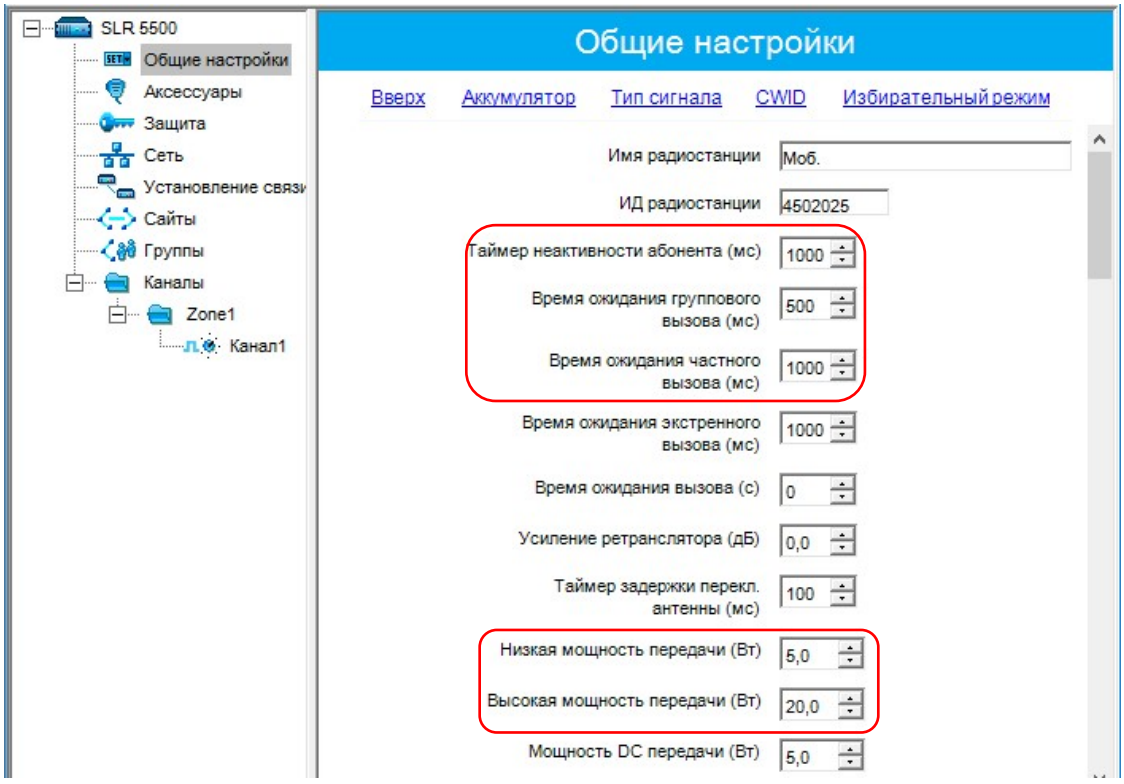


Рис. 7

4.7.2.2 Встановити мінімальне значення потужності передавача ретранслятора, за якої досягається потрібна дальність зв’язку (значення визначається заздалегідь експериментальним шляхом) (рис. 7).

4.7.2.3 Тип встановлення зв’язку налаштовується як локальний – Значення параметру «Тип з’єднання» встановлюється як «Ні» (рис. 8).

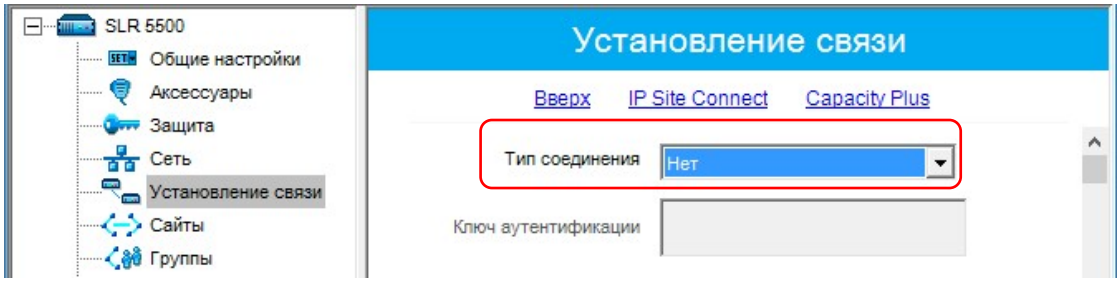


Рис. 8

4.7.3 Якщо ретранслятори працюють в режимі IP Site Connect, РЕКОМЕНДОВАНО вимкнути на них «радіомаячок» з метою скорочення часу небажаного випромінювання та зниження радіопомітності. Для вимикання «радіомаячка» потрібно ввести «0» в полі Тривалість маячка (Рис. 9).

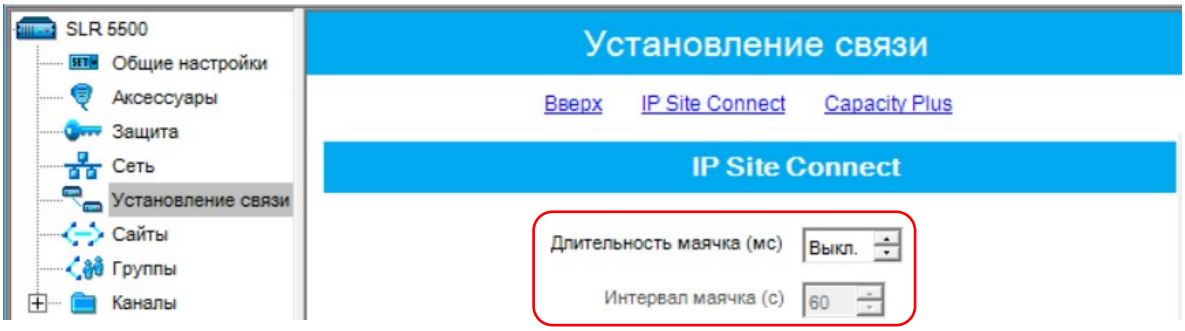


Рис. 9

4.7.4 Для локального радіообміну всередині тактичної групи на прямих каналах та коротких відстанях РЕКОМЕНДОВАНО застосовувати:

4.7.4.1 Понижену потужність передавача радіостанції. Крім радіоприхованості, застосування малої потужності передавача також збільшує тривалість роботи від одного заряду акумуляторної батареї. Функція активується натисканням на радіостанції відповідної заздалегідь запрограмованої кнопки «Вис./низьк. потужність».

4.7.4.2 В радіостанціях параметр «Автоматична служба реєстрації» (на каналах) встановлюється в значення «Вимк.» (рис. 10).

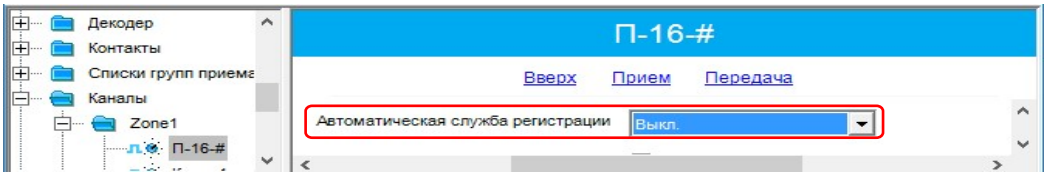


Рис. 10

4.7.5 У підрозділах, що знаходяться в зоні бойових дій та/або мають збільшений ризик терористичного нападу, ОБОВ'ЯЗКОВО вимикати підсвічування дисплеїв командирських радіостанцій (радіостанції типу DP4800/4801) та деактивовувати всі світлодіоди (рис. 11).

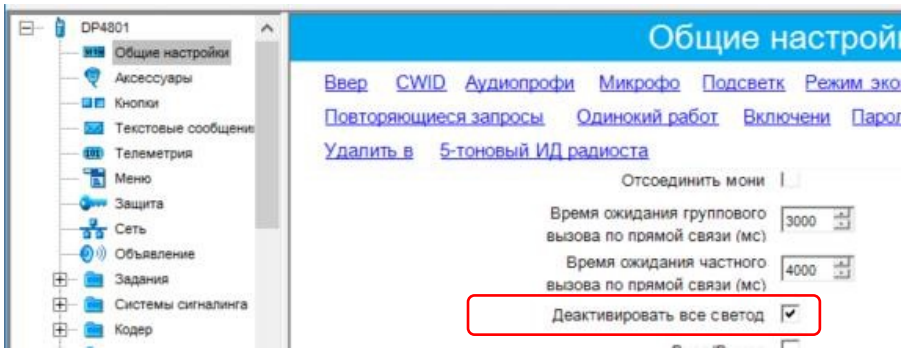


Рис. 11

4.8 Деактивація прийому GPS-сигналів (за необхідності).

У разі наявності вбудованого GPS-модулю відкриття вкладки «Общие настройки» дозволяє деактивувати прийом GPS сигналів відповідно з рис. 12.

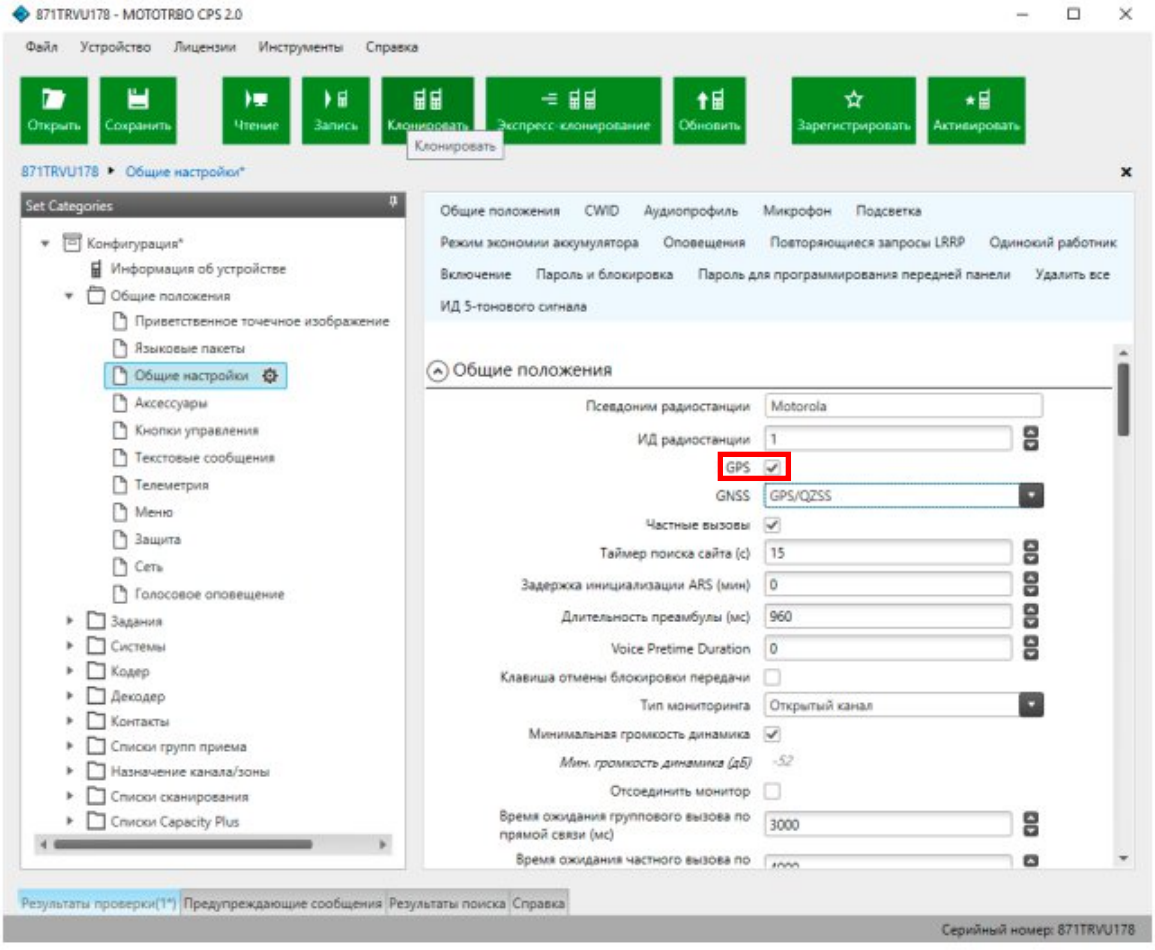


Рис.12

4.9 Деактивація радіовипромінюючих модулів Bluetooth та Wi-Fi (за необхідності).

На панелі ліворуч виберіть Мережа. На правій панелі натисніть Bluetooth і зніміть прапорець, щоб деактивувати функцію Bluetooth на радіостанції згідно з рис. 13.

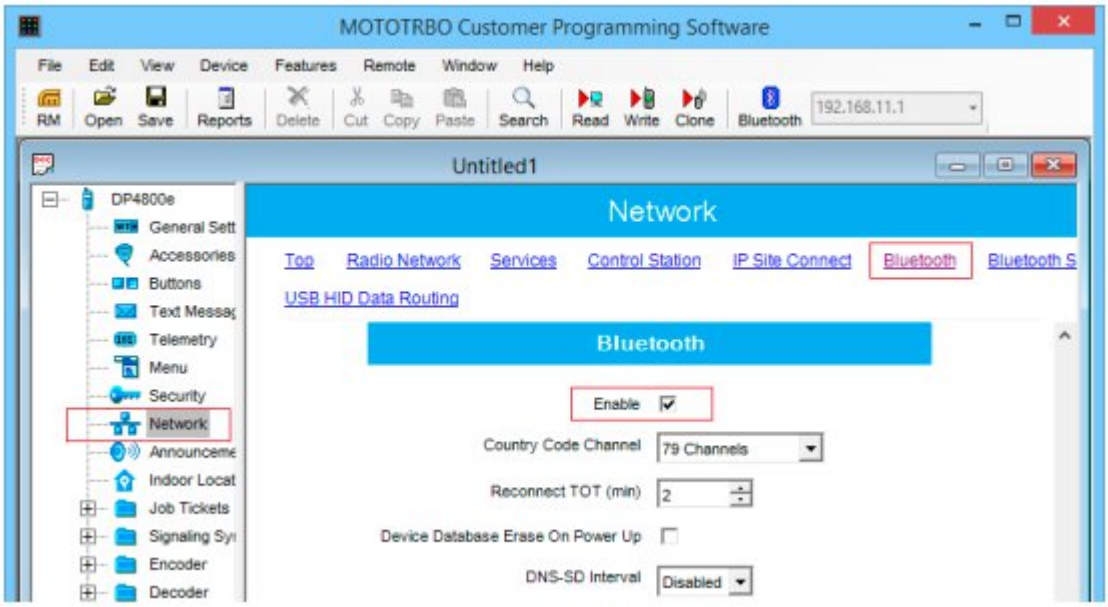


Рис. 13

На правій панелі натисніть Wi-Fi і зніміть прапорець, щоб деактивувати функцію Wi-Fi на радіостанції згідно з рис. 14.

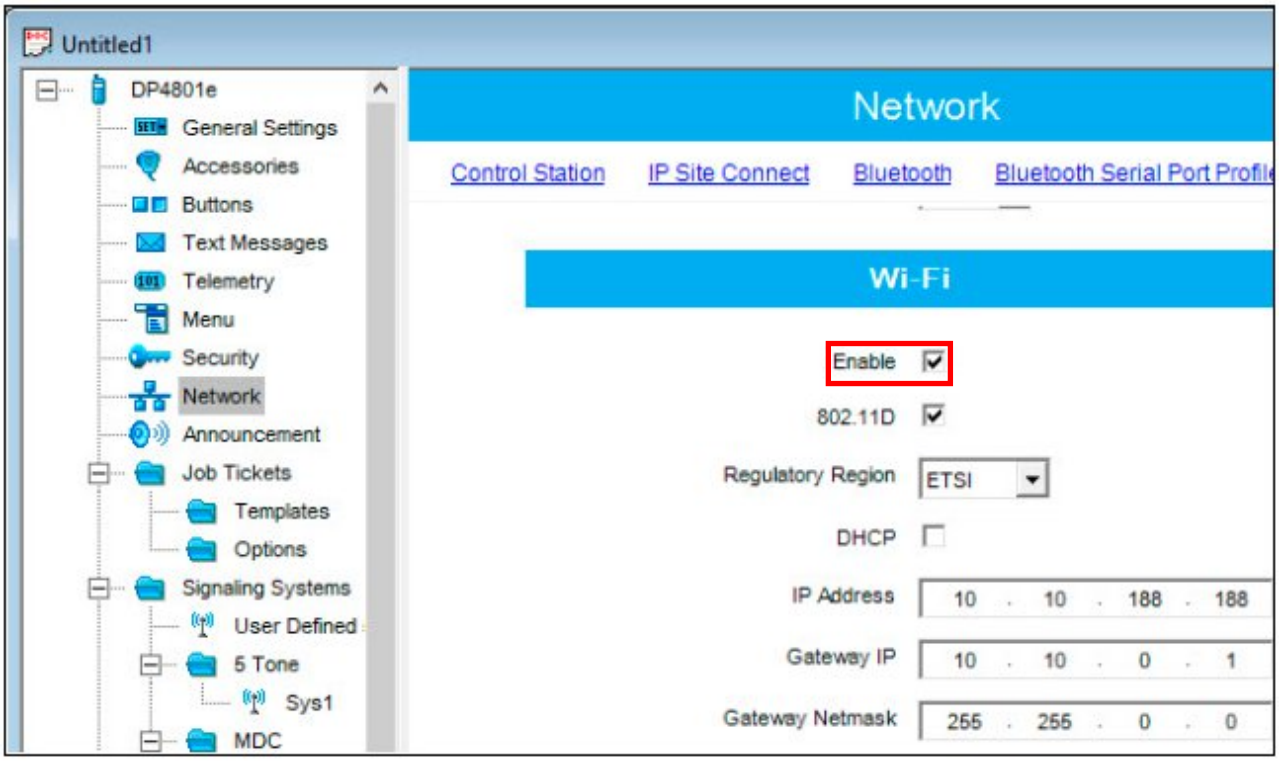


Рис.14

4.10 Зменшення потужності передавача (для зменшення ефективності засобів РЕР).

Відповідно до рис. 15 до певного каналу можна встановити рівень потужності на даному каналі низька (1 Вт).

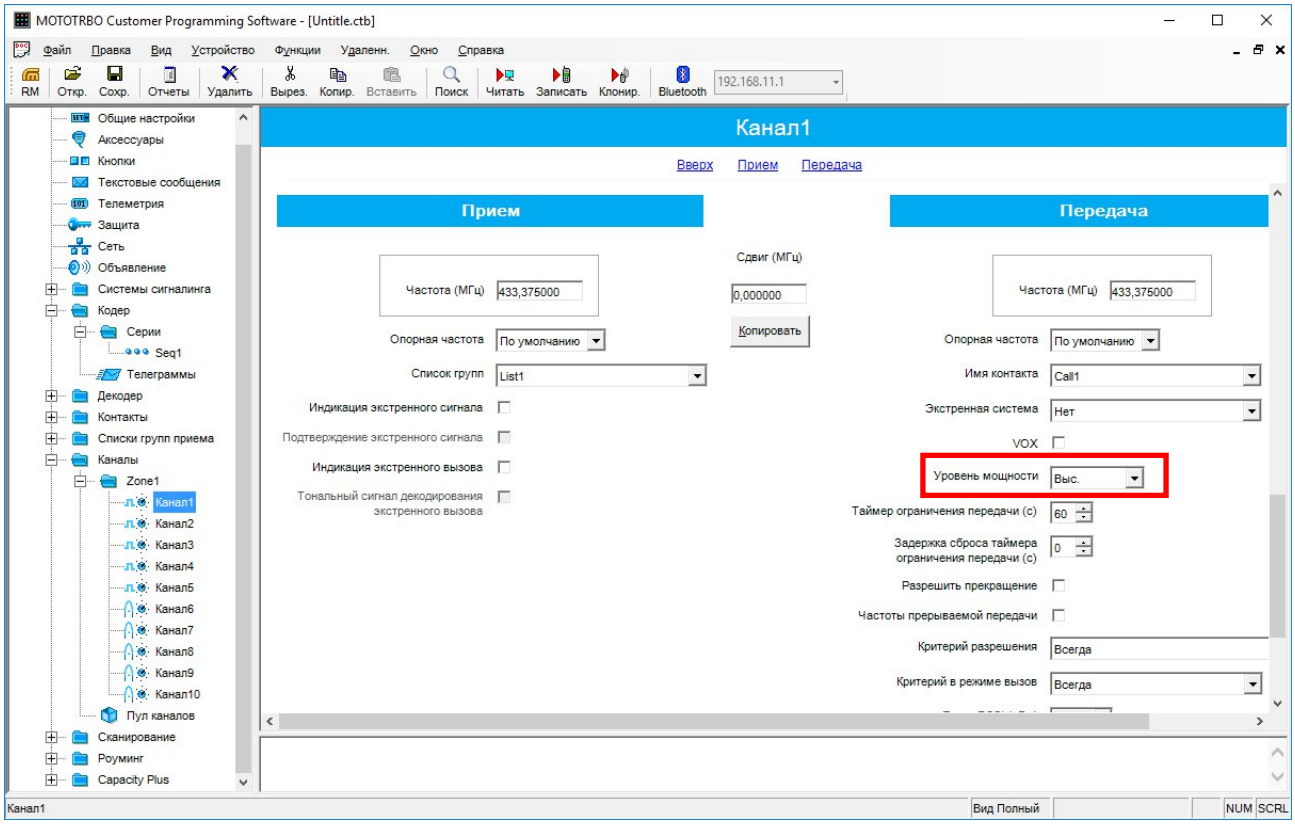


Рис. 15

## 5. ЗАХОДИ ДЛЯ ПОПЕРЕДЖЕННЯ ВИКОРИСТАННЯ ВОРОГОМ ВТРАЧЕНИХ РАДІОЗАСОБІВ

5.1 Для запобігання можливості користування ворогом втраченої радіостанції з метою скритого прослуховування переговорів або провокацій та нав'язувань спотвореної (неправдивої) інформації, ОБОВ'ЯЗКОВО встановлювати пароль на вмикання радіостанції (Рис. 16).

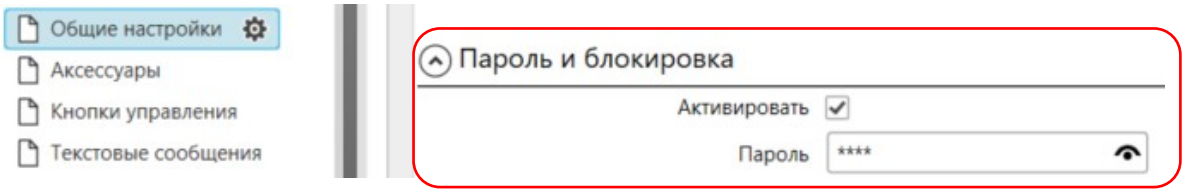


Рис. 16

5.2 Для запобігання можливості несанкціонованого зчитування налаштувань радіостанції, ОБОВ'ЯЗКОВО використання пароля на зчитування радіостанції та файлу конфігурації (кодплага) (Рис. 17).

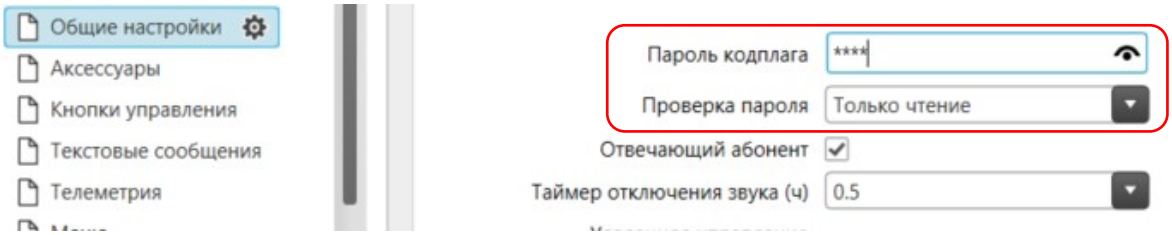


Рис. 17

5.3 Для запобігання можливості перепрограмування ворогом втраченої радіостанції з метою подальшого її використання для власних потреб, а також для попередження крадіжок радіостанцій з метою подальшого нелегального збуту, РЕКОМЕНДОВАНО встановлювати пароль автентифікації TLS-PSK (Рис. 18). Не рекомендується використовувати ключ TLSPSK «за замовчуванням з назвою DEFAULT»!

*Можливість захисту доступу з автентифікацією TLS-PSK доступна лише з версії мікропрограмного забезпечення радіостанції R2.10 та новіше.*

*УВАГА: втрата ключа TLS-PSK унеможливлює подальше перепрограмування та зчитування радіостанції.*

***УВАГА: Використання автентифікації TLS-PSK дозволяється лише в CPS2.0 версії 2.122.70 або новіше!***

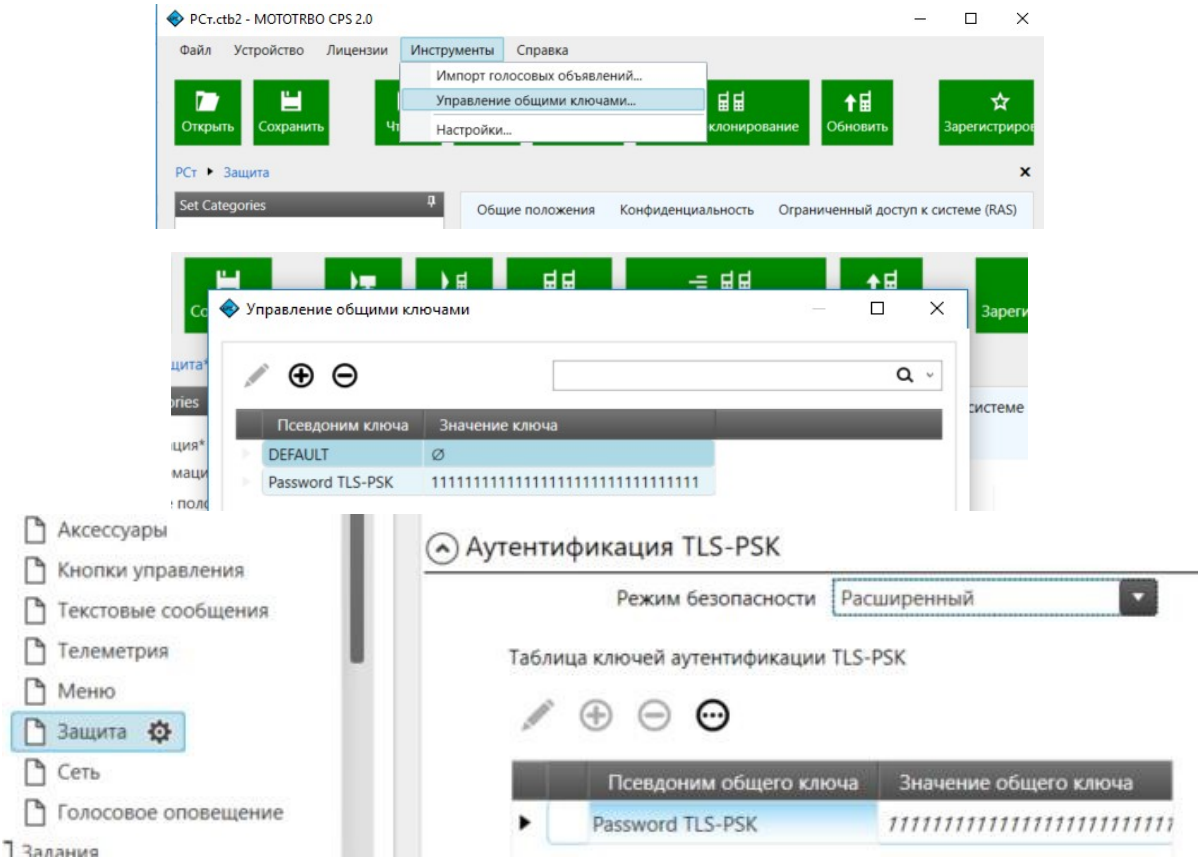


Рис. 18

5.4 В разі наявності підтвердженої інформації про втрату однієї або декількох радіостанцій з ключовими даними та загрозі компрометації РЕКОМЕНДУЮТЬСЯ організаційні заходи:

5.4.1 За спеціальним наказом командира всім підлеглим слід перейти на резервний канал зв’язку, а адміністратор (зв’язківець) повинен у найкоротший час перепрограмувати (змінити ключі шифрування) всі радіостанції у підрозділі.

5.4.2 При неможливості швидкого перепрограмування (зміни ключів шифрування) всіх радіостанцій у підрозділі, наприклад, під час активної фази спецоперації:

за спеціальним наказом командира всім підлеглим слід перейти на заздалегідь запрограмований канал індивідуального виклику (радіонапрямок) командира (або іншої призначеної особи). Командир (або інша призначена відповідальна особа) також повинен перейти на відповідний резервний канал зв'язку. Таким чином виключається можливість прослуховування через втрачену радіостанцію викликів у напрямку від особового складу до командирів та їх відповідей на такі виклики, а також знижується (але не виключається) ризик прослуховування групового виклику від командира до підлеглих (через зміну основного канала на резервний).

5.5 В окремих випадках, РЕКОМЕНДОВАНО застосовувати індивідуальний тип виклику особам, яким за призначенням необхідно забезпечити додатковий захист від прослуховування, та які виконують завдання відокремлено від загальної групи, наприклад: наглядач, навідник, «під прикриттям» та інші. Для радіостанцій з перемикачем каналів фіксованої кількості з 1 по 16 канал (DP4400/4401 та DP3441) доцільно налаштовувати 16-й (крайній канал) на індивідуальний виклик командира (або іншої призначеної відповідальної особи).

**ВИСНОВКИ**

Перелічені заходи дозволяють:

1. Мінімізувати ефективність засобів РЕР в частині локалізації, ідентифікації, перехоплення інформації та можливі ризики щодо її дешифрування.

2. Унеможливити неавторизований доступ та управління радіостанціями.

У разі неможливості зміни налаштувань згідно рекомендацій (недоступне поле тощо) при використанні радіостанції враховувати ризики пов'язані з безпекою інформації. Якщо відсутня можливість зміни ключів та алгоритму шифрування радіостанцію рекомендується передати представникам Держспецзв'язку для подальших досліджень.