

РЕКОМЕНДАЦІЇ **з питань забезпечення безпеки цифрового** **радіозв'язку MOTOTRBO**

Радіостанція аналого-цифрового радіозв'язку MOTOTRBO стандарту DMR, має у своєму складі систему захисту голосової інформації та даних, які циркулюють в межах радіомережі.

Захист циркулюючої у мережі інформації забезпечується у всіх режимах роботи (прямий режим, режим роботи через ретранслятор і "IP Site Connect") і через усі канали зв'язку між передавальними та приймальними радіостанціями.

Голосові й інформаційні повідомлення залишаються захищеними в наступних ситуаціях:

- в ефірі, у прямому режимі;
- в ефірі та в середині ретранслятора, у режимі роботи через ретранслятор;
- в ефірі, в середині ретрансляторів і в допоміжній мережі, у режимі "IP Site Connect".

Радіостанція, що використовує канал із включеними налаштуваннями захисту, завжди здійснює передачу у захищеному режимі, у той же час коли радіостанція, що використовує канал з відключеними налаштуваннями захисту, завжди здійснює передачу в незахищеному режимі.

Проте радіостанція здійснює приймання, як у незахищеному, так і в захищеному режимі незалежно від налаштувань захисту каналу.

При одержанні радіостанцією захищеного повідомлення, незалежно від налаштувань захисту каналу, радіостанція завжди намагається виконати розшифрування повідомлення.

У випадку якщо радіостанції не потрібно приймати захищені повідомлення, у цьому випадку їй слід призначити ключ, що відрізняється від ключа, використовуваного в мережі. Просте відключення налаштувань захисту каналу не призведе до того, що радіостанція перестане одержувати захищені повідомлення.

Користувач радіостанції, що одержує захищену передачу, побачить швидке миготіння світлоіндикатора зеленого кольору. При прийманні, користувачу радіостанції, що приймає, необхідно взяти до уваги зміну налаштування захисту для забезпечення відповідності налаштуванням ініціатора виклику.

Система захисту MOTOTRBO не підтримує дистанційне або ефірне програмування ключів у радіостанціях. Ключі можуть бути запрограмовані в радіостанції тільки з використанням програмного забезпечення для конфігурування радіостанції (CPS).

Ключі повинні періодично мінятися, бажано щомісячно.

Негайна зміна ключів необхідна у разі коли:

- ключі скомпрометовані;
- втрачена радіостанція, у результаті чого виникають припущення про те, що це може привести до компрометації ключів або до прослуховування і надання фальшивої інформації або команд.

Найпростішим способом заміни ключів є збір усіх радіостанцій і їх перепрограмування за один захід. Але, іноді зібрати всі радіостанції і не вплинути на щоденну роботу може бути попросту неможливим. Тоді альтернативним методом є створення двох зон, де одна зона працює в незахищеному режимі (або захищеному за Базовим механізмом), інша зона – у захищеному Розширеному механізмі. Спочатку ключі можуть бути замінені в захищеній зоні і користувачі будуть використовувати незахищену зону доти, поки не будуть оновлені всі радіостанції. Після того, як було виконане відновлення всіх радіостанцій, диспетчер передає користувачам радіостанцій команду виконати перемикання зон. Це дозволяє користувачам забезпечити нормальний зв'язок доти, поки не буде виконана установка нових ключів у всіх радіостанціях, після чого всі користувачі одночасно змінять ключі.

Аналогічна стратегія з використанням зон може використовуватися для виконання періодичних замін наборів ключів.

Наприклад, коли одна зона має жовтневі ключі, а інша парна зона має листопадові ключі. Першого листопада користувачі перемикаються на листопадову зону. Протягом листопада здійснюється відновлення жовтневої зони з використанням грудневих ключів і її перейменовують в «грудневі ключі».

Першого грудня користувачі перемикаються і цикл починається знову. Завдяки цьому, у випадку втрати або крадіжки радіостанції будуть скомпрометовані ключі лише за двомісячний період.

Необхідно взяти до уваги те, що така конфігурація не є рекомендованою, і при ухваленні рішення про використання в системі декількох ключів слід прийняти до уваги низку питань, а саме: при використанні декількох ключів не рекомендується ділити групи на групи меншого розміру. Результатом того стане те, що користувачі однієї підгрупи будуть чути нерозбірливий звук (або «цифрові трелі») при спробі зв'язатися з іншою підгрупою.

Доцільно розділити користувачів на групи і забезпечити неможливість передачі або приймання користувачами повідомлень іншої групи.

У випадку якщо користувачам з різними ключами буде дозволений зв'язок з використанням Базового механізму захисту, наприклад, за допомогою захищеного персонального виклику, ключі не збіжаться і буде чутний нерозбірливий звук.

Хоча дані користувачі з різними ключами зможуть зв'язуватися в персональному режимі, якщо буде відключена опція захищеності. Наприклад, дві різні групи будуть ізольовані шляхом встановлення різних ключів. Коли користувачам у кожній із груп необхідно зв'язатися один з одним за допомогою персонального виклику, для цього їм необхідно відключити опції захисту.

У випадку якщо користувачу радіостанції необхідно зв'язатися з обома групами за допомогою загального виклику, користувач радіостанції повинен здійснювати передачу у відкритому режимі таким чином, щоб обидві групи могли здійснювати моніторинг.

Якщо користувачі відповідають із включеними налаштуваннями захисту, то користувач, що ініціював загальний виклик лише може здійснювати моніторинг відповідей, захищених з використанням співпадаючого ключа.

У випадку якщо в системі використовуються додавання для роботи з даними й зв'язок із сервером додавання повинна здійснюватися через станцію управління, усі радіостанції на слоту повинні мати той самий ключ або ж усі вони не зможуть забезпечити правильний зв'язок зі станцією управління.

У якості загального правила рекомендується, щоб групи з різними налаштуваннями системи захисту завжди перебували в різних групах і на різних слотах.

При необхідності у захисті голосу та даних однієї групи від іншої на тому ж самому каналі (ті ж частота і слот) і деякі користувачі радіостанцій можуть бути абонентами однієї або декількох груп, то у цьому випадку, якщо групі не тільки необхідно захистити з'єднання від вторгнення, але, також, захистити і від інших груп, у цьому випадку кожній групі слід використовувати окремі ключі для захисту.

Системному установникові необхідно встановити для кожної групи, що вимагає захисту, опцію "TX Group" для учасника. Взаємовідношення між учасником і групою становить 1:1. Системному установникові слід привласнити ключ учасникові. Взаємовідношення між ключем і учасником становить 1:1 і тому взаємовідношення між ключем і групою також буде 1:1.

Якщо радіостанції "X" необхідно виконати захищений персональний виклик радіостанції "Y" і якщо обидві радіостанції є елементами групи "T", то у цьому випадку радіостанція "X" звертається до учасника зі значенням "T" для опції "TX Group". При відсутності групи, елементами якої є обидві радіостанції, можливість відправлення захищених повідомлень відсутня.

Для захищеного "загального виклику" радіостанції, що передає, необхідно щоб ключ, привласнений даному учасникові, був присутнім на всіх радіостанціях. Для захищеного "персонального виклику" радіостанції, що передає, необхідно перейти до певного учасника. Ключ, привласнений даному учасникові, повинен бути присутнім на радіостанції, що приймає.