DOI: 10.18372/2410-7840.26.18817
УДК 004.42

ПРОБЛЕМА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ ПРОФЕСІЙНОГО РАДІОЗВ'ЯЗКУ В КРИТИЧНИХ ІНФРАСТРУКТУРАХ

Ярослав Шавловський, Сергій Передерій, Володимир Бичков

В даній роботі здійснено огляд існуючих та очікуваних сценарії недозволених впливів на системи зв'язку в критичних інформаційних структурах. Встановлено, що зона підвищеного ризику таких впливів зосереджена на інтерфейсах між зовнішніми пристроями та чипом SoC. Наведено приклади групування великої кількості абонентських терміналів, що працюють під єдиною програмою недозволених впливів, при цьому рівень проникнення може бути багаторазово підвищений. Зазначено, що такі можливості стають реальнішими з впровадженням систем покоління 5G, які передбачають режим роботи M2M. Метою такого огляду є визначення підходу до моделювання процесів захисту інформації від витоку по радіоканалам систем зв'язку та для розробки інженерно-технічних заходів щодо проектування та впровадження відповідних систем інформаційного захисту.

Ключові слова: *SoC-чіп, несанкціонований вплив, периферійні пристрої, 5G, модель відкритої системи X.200.*

ВСТУП

Актуальність

Мобільний радіозв'язок поколінь 4G і 5G спрямований на максимальну концентрацію процесів обробки та управління, що відбуваються на абонентських терміналах (АТ), в одному чипі SoC (System-on-Chip). Чіпи SoC відзначаються високим рівнем інтеграції та забезпечують обмін да-ними з усіма зовнішніми пристроями. Це робить їх основною мішенню для несанкціонованих впливів.

Розмаїття периферійних пристроїв, які підтримуються сучасними АТ, створює потенційні можливості для формування складних сценаріїв впливів як на абонентів, так і на системи зв'язку загалом. Для оцінки масштабів та ризиків цього явища необхідно провести загальний аналіз та оцінити рівні можливих проникнень, доступних для сучасних і майбутніх технічних засобів. Це особливо актуально для систем професійного радіозв'язку критичних інформаційних структур.

Постановка задачі

Основним завданням в даній роботі є здійснити огляд всіх можливих сценаріїв деструктивного впливу на системи зв'язку в критичних інформаційних системах.

ОСНОВНА ЧАСТИНА

Області найбільшої вразливості до несанкціонованих впливів

На рисунку наведено загальну структуру сучасного абонентського термінала у формі основних периферійних пристроїв, що взаємодіють із SoC. Зона ризику несанкціонованих впливів знаходиться на інтерфейсах між SoC та периферійними пристроями (рис. 1).

Останні досягнення в технологіях запису та зберігання інформації дозволяють у реальному часі організувати практично необмежене зчитування даних з будь-яких периферійних пристроїв, включаючи відеодані, з подальшим записом у оперативну пам'ять (ОЗП) або зовнішню пам'ять (ПЗП). Наприклад, сучасні схеми ОЗП LPDDR4 забезпечують швидкість запису до 2 Гбіт/с [1] на один канал, а схеми ПЗП UFS 3.1, які можна використовувати для несанкціонованого запису "на пам'ять", до 1,2 Гбіт/с [2]. Цього зазначеного рів-ня пропускної здатності достатньо навіть для відео формату 8К.

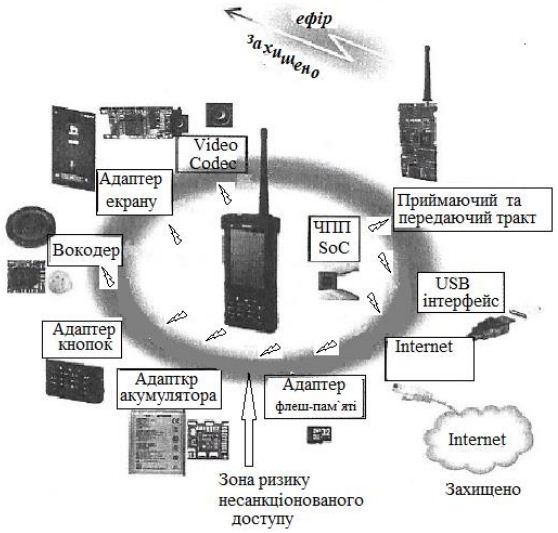

Рис. 1. Зона ризику несанкціонованих впливів АТ

Програмне забезпечення базових станцій (БС) та ядра систем зв'язку, незалежно від виробника, спрямоване на реалізацію стандартів і протоколів, затверджених Міжнародним союзом електрозв'язку. Ці стандарти допускають наявність резервних полів в форматах повідомлень, що відкриває можливості для несанкціонованих впливів.

Стандартний набір периферійних пристроїв абонентського термінала, як це представлено (рис. 2), охоплює практично всі сенсори, які людина може відчувати, з винятком смаку, запаху і кінестезії. Проте з введенням систем покоління 5G кінестезія також може стати доступною. Смак і запах можуть бути реалізовані

через мікро-хімічну лабораторію в абонентському терміналі. В цьому напрямку вже проводяться активні роботи, і ці функції можуть широко підтримуватися в найближчому майбутньому.

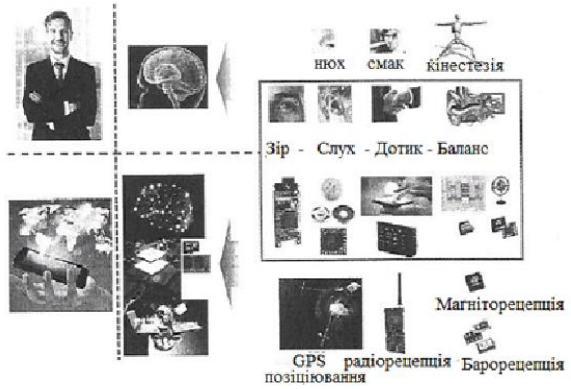

Рис. 2. Порівняльна схема «органів чуття» людини і сучасного АТ

Послідовність периферійних датчиків, недоступних для людини, включає чутливість до електромагнітних хвиль інфрачервоного та радіодіапазонів, магнітного поля, тиску. Ці датчики демонструють вищу точність і швидкість реакції порівняно з рецепціями, доступними для людини, і тому абонентські термінали мають перевагу в конкурентних сценаріях взаємодії з абонентами.

Наприклад, абонентські термінали можуть визначати наміри абонентів, а також виявляти нерегламентоване програмне забезпечення, використовуючи ключові слова. Шляхом аналізу близькості розташування до координат лабораторій контролю за допомогою GPS і точного визначення висоти за допомогою MEMS датчика тиску, абонентські термінали можуть виявляти "небезпечне" програмне забезпечення і вживати відповідних заходів.

Факт прихованого прослуховування акустичного оточення та мови через термінали, навіть з сертифікованим програмним забезпеченням, підтверджено [3]. Наприклад, журналіст Сем Ніколе протягом п'яти днів двічі розмовляв по телефону про бажання повернутися до навчання в університеті та придбати дешеві сорочки, не використовуючи ключові слова "Hey Siri" чи "OK, Google". У результаті, у перший день Facebook почав показувати рекламу університетських курсів та магазинів одягу. Це свідчить про те, що загроза прослуховування існує не тільки з боку Facebook.

Нелегальне програмне забезпечення на абонентських терміналах може бути завантажене різними способами. Один з основних методів полягає в використанні легальної функції модернізації програмного забезпечення, що відбувається "з ефіру". Згідно з загальними правилами, абонент повинен погодитися на модернізацію програмного забезпечення, але насправді це обмеження може бути обійденою за наявності або витоку відомостей від виробника програмного забезпечення. Це дозволяє проводити модернізацію приховано, у фоновому режимі.

Один з найбільш важко контрольованих каналів зовнішнього доступу - це інтернет-з'єднання, яке проходить через внутрішній процесор SIM-карти абонентського термінала. SIM-карта взаємодіє з широким спектром зовнішніх пристроїв та є ключовим елементом внутрішньої організації абонентського термінала в стільникових мережах. Тому контроль за такими каналами доступу можливий лише за умови фундаментальної модернізації загальних принципів функціонування стільникових мереж. Присутність SIM-карти є ознакою підвищеного ризику несанкціонованих впливів.

Приклади несанкціонованих дій, що реалізуються

Наведено варіанти найпростіших сценаріїв несанкціонованих впливів на абонентські термінали (рис. 3). На нижній частині малюнка на прикладі платформи смартфона Galaxy S10 показано чипи периферійних пристроїв, які задіяні в цих сценаріях.

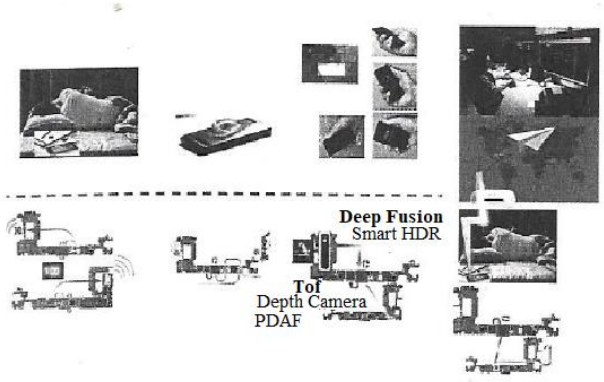

Рис. 3. Приклад технологічної організації несанкціонованого контролю та зняття інформації на платформі смартфона (Galaxy S10)

Перший сценарій пов'язаний із контролем часу, який здійснюється таймером чипа SoC (позначений червоною рамкою). Програма "будильник" контролюється сценарієм через активність чипа акустичних сигналів (у жовтій рамці). Збираючи інформацію про переміщення та розмови, абонентські термінали складають розклад контрольованого абонента.

Другий сценарій показує несанкціоноване прослуховування. Фрагменти мови з ключовими словами записуються в ПЗП (Flash-пам'ять у фіолетовій рамці).

Третій сценарій стосується фотографій та обробки відеоданих. Абонентські термінали, використовуючи контрольні слова, визначають наявність носіїв інформації у доступній близькості та фіксують відповідні події. Наприклад, вони можуть встановити факт присутності абонента на переговорах і виявити фрази про розташування документів. Потім термінал імітує прийом SMS (реклами). Коли абонент піднімає телефон,

термінал за допомогою MEMS-акселераторів та гіроскопів контролює своє розташування та відповідно виконує фотографування.

Технічні можливості дозволяють отримувати якісні знімки навіть у складних умовах. Сучасні абонентські термінали підтримують кілька камер, які забезпечують різні функції, такі як високо роздільна, ширококутна, інфрачервона зйомка тощо. Комбінування функцій автоматичного фокусу, режиму Deep Fusion та інших технологій дозволяють отримувати високоякісні знімки в різних умовах освітлення.

За допомогою камери зондування ToF абонентський термінал здатний проводити приховане розпізнавання обличчя і створювати 3D-моделі навколишнього простору (рис. 4) [4]. Режим формування 3D-моделі називається SLAM (Simultaneous localization and mapping). В АТ і мобільних гаджетах він застосовується для локалізації формування карти оточення.

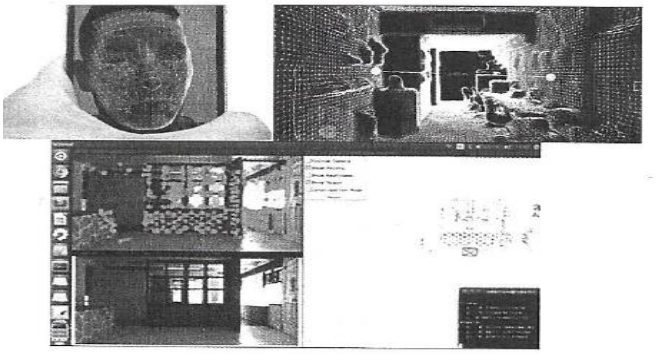

Рис. 4. Приклади використання ToF камери для прихованої ідентифікації обличчя і формування об'ємних схем невідомих просторів методом SLAM

Останній сценарій на рисунку 3 показує, як збережена "за оперативною пам'яттю" (у ПЗП) інформація може бути передана третім особам, наприклад, через Wi-Fi. Під час реалізації сценарію на платформі Galaxy S10 у ньому беруть участь: SoC (Exynos 9820), виділений червоною рамкою, Flash ПЗП (KLUDG4U1EA UFC 2.1) – фіолетовою, RF-трансивер (Shannon 5500) – білою і Wi-Fi модуль (292402) – жовтою.

Несанкціоновані дії у мережах 5G і 5G+ в майбутньому

У сучасних системах зв'язку досягнення, що відносяться до штучного інтелекту, в основному пов'язані з удосконаленням оброблення даних від датчиків і периферійних пристроїв. Фактично, ці досягнення полягають у розвитку математичного апарату адаптивних алгоритмів і дисперсійного аналізу для розв'язання прикладних завдань.

В перспективних системах зв'язку, зокрема, у 5G, передбачається значна вага когнітивних алгоритмів, які генерують нові знання. Це суттєво розширює можливості невповноважених сценаріїв. Наразі можна лише загально описати можливі варіанти таких негативних проявів.

Зручно описувати невповноважені втручання за рівнями моделі відкритих систем X.200. Сценарії, що належать до мережевого (L3) і транспортного (L4) рівнів, досить добре досліджені. Вони зазвичай полягають у дублюванні даних для нелегальної передачі, зміні маршрутів доставки для блокування у зонах, чутливих до перевантажень, а також у блокуванні серверів на рівні TCP (L4) за допомогою атак DDoS (розподілене відмова в обслуговуванні). Тому ми тут не будемо розглядати ці сценарії. Зосередимося на можливому втручанні, яке належить до L1-L2 і L5-L7 рівнів.

На рівні L1 (фізичний) у мережах 5G і 5G+ передбачається підтримка режимів, що дозволяють терміналам організовувати колективну роботу. Ці режими можуть бути застосовані для поліпшення характеристик акустичних і радіоканалів. Такі застосунки є ймовірними у несанкціонованих сценаріях на рівні L1.

Наприклад, показано можливий сценарій включає самоорганізацію в єдиний спрямований мікрофон багатьох терміналів, розташованих перед приміщенням, де відбувається закрита нарада (рис. 5).

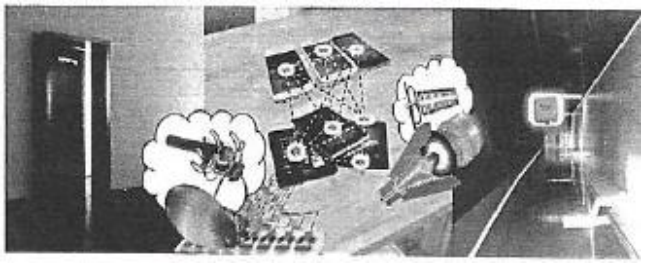

Рис. 5. Самоорганізація групи АТ у спрямовані мікрофон і Wi-Fi антену з метою несанкціонованого зняття і передачі інформації

У цій групі терміналів може підтримуватися локальна синхронізація генераторів для здійснення функції спрямованої антени радіоз'єднання, наприклад, Wi-Fi або Bluetooth.

Взаємне розташування терміналів з високою точністю (приблизно 1-2 мм) може бути досягнуто шляхом акустичного "калібрування", навіть на дуже "тихих" сигналах (з рівнем шепоту $20дБ$). Практично оцінку Δ похибки розташування за рівнем власних шумів в акустичному каналі можна визначати в межах, представлених нерівністю (1):

$$\frac{v_{звуку}}{f_{\max}}\cdot\left(10^{0.1\cdot\left(f_{шепоту}-f_{вшуму}\right)}\right)^{-0,5}\le\Delta\le\frac{v_{звуку}}{f_{\max}}\cdot\left(10^{0.1\cdot\left(f_{шепоту}-f_{вшуму}\right)}\right)^{-0,5},\quad(1)$$

де $v_{звуку}$ – швидкість звуку в середовищі, $f_{\min}=25ГГц$ – мінімальна частота 5G, $f_{\max}=39ГГц$ – максимальна частота 5G, $f_{шепоту}$ – частота шепоту, $f_{вшуму}$ – частота власного шуму.

Для калібрування тактових генераторів акустичної смуги 20 кГц самою акустичною смугою може бути

недостатньо. Тому група акустичних терміналів (АТ) повинна додатково використовувати радіосигнали. Оскільки робоча смуга в 5G технічно становить сотні мегагерц, то взаємна синхронізація генераторів після калібрування може бути забезпечена з точністю до кількох наносекунд. Тобто після калібрування група терміналів 5G (5G+) відновить геометрію взаємного розташування і забезпечить синхронну роботу з високим рівнем якості. Це є достатньою умовою для організації адаптивного просторово-часового оброблення сигналів (акустичних, електромагнітних) і пеленгації джерел.

Дослідження в [5, 6] показали, що за допомогою частотної та часової селекції можна виділяти напрямки на промені приходу корисного сигналу та пригнічувати спрямовані завади, базуючись виключно на геометричних відмінностях хвильових фронтів у зоні розміщення мікрофонів або антен. При цьому адаптивне налаштування зазвичай забезпечує просторово-спектральне придушення джерел, які заважають, не менше ніж на 30-40 дБ. У результаті перешкоди рівня 50 дБ (А) (гучність спокійної розмови) пригнічуватимуться під поріг чутливості слуху, і група малорозмірних мікрофонів АТ забезпечить характеристики хорошого студійного мікрофона.

Використовуючи техніку MIMO з керуванням числом каналів [7], група акустичних терміналів (АТ) може одночасно приймати (передавати) сигнали (акустичні або радіо) від декількох незалежних джерел, очищаючи їх від взаємних перешкод. Під час організації обміну службовою інформацією та калібрування можуть застосовуватися алгоритми стислих розкладів [8, 9], забезпечуючи високу швидкість налаштування.

Після відновлення геометрії розміщення і синхронізації опорних генераторів група АТ здатна зондувати оточення за допомогою акустичних хвиль і пружних коливань, що генеруються вібромоторами (рис. 6).

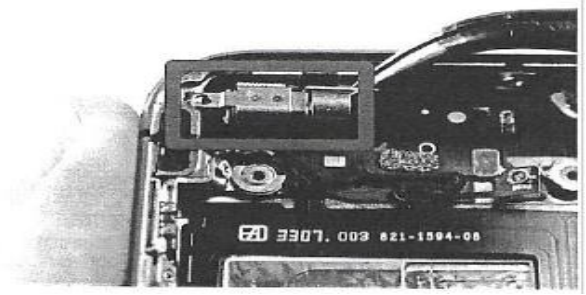

Рис. 6. Вібромотор смартфона, придатний для обміну в режимі пружних коливань

Метод над широкосмугового зондування [10] дозволить визначити напрямок можливого подолання ізолювального середовища, відповідні спектральні характеристики сигналів і природні об'єкти посилення (точки, що відбивають, предмети, що вібрують, тощо. Такий підхід здається одним з головних напрямків розвитку НВ на рівні L1. Звичайно, не слід ігнорувати процедури прихованого впровадження трафіку в складні закони модуляції [11-13] і виведення з ладу апаратури установкою неліквідних параметрів або штучного підвищення пік-фактору сигналів [14]. Але такі дії не потребують додаткових пояснень.

Рівень L2 (канальний). На цьому рівні, починаючи з покоління 5G, акустичні термінали (АТ) можуть таємно організовуватися в мережеві Mesh-структури, що дозволяє їм проникати у важкодоступні для перехоплення зони. Системи професійного радіозв'язку є найбільш підходящою платформою для цього, оскільки абоненти зазвичай розташовані рівномірно по території (рис. 7).

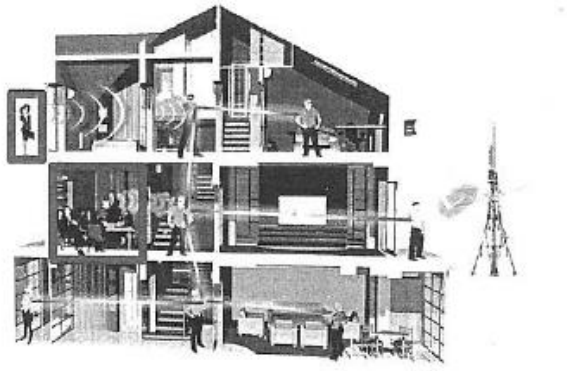

Рис. 7. Приклад прихованої організації Mesh-мережі на базі несанкціонованого використання АТ системи професійного радіозв'язку покоління 5G

Структура з ланок передавання даних (ЗПД) конфіденційно з'єднує АТ членів служби та організовує вторинну мережу, призначену для несанкціонованого зняття інформації в ізольованій будівлі. Шляхом естафетної передачі по ЗПД знята інформація доставляється на термінали, які можуть підключатися до зовнішніх мереж. Такі Mesh-мережі можуть мати гетерогенну структуру, використовуючи ЗПД з різним хвильовим характером, включно зі звуком і вібрацією.

Вищі рівні L5, L6 і L7 (сеансовий, представницький і прикладний). На вищих рівнях відкритих систем організація НВ в першу чергу орієнтується на когнітивні алгоритми. Тому головними об'єктами впливу є системи-на-чіпі (SoC), система в цілому і їх програмне забезпечення (ПЗ).

Багато процедур на вищих рівнях, спрямованих на НВ, вже пройшли "випробування" і дають змогу прогнозувати перспективи. Стримуючим фактором поки виступає відсутність ліквідних алгоритмів для організації сценаріїв налаштування під реакцію абонентів, тобто засобів, здатних враховувати людський фактор.

У цьому напрямку, безумовно, буде спостерігатися прогрес. Представлено дію наявних розробок несанкціонованих сценаріїв рівня L5 (рис. 8).

Вони зводяться до впровадження, розриву або встановлення сеансів зв'язку для передачі неправдивої інформації, а також блокують спроби повторної перевірки. Наступний рисунок ілюструє застосування рішень, які можуть бути використані на представницькому рівні: імітація голосу, відео, що створює ілюзію; відтворення манер мови/по веденню; SLAM-симуляція несправжніх інтер'єрів (рис. 9).

Рис. 8. Сеансовий рівень (L5): несанкціоноване впровадження, переривання та встановлення сеансів інформаційного обміну з метою активного впливу

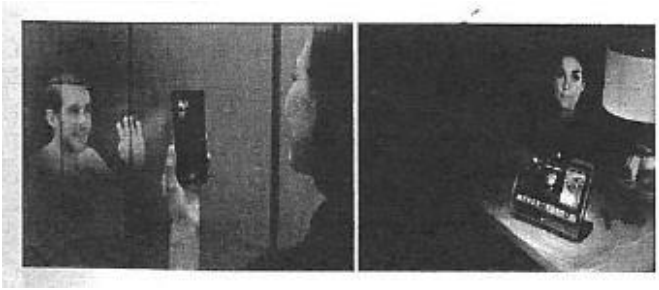

Рис. 9. Представницький рівень (L6): імітація відео, голосу, поведінки, манер

Наведено приклад маніпуляції сценаріями і процесами на представницькому рівні з метою введення в оману (рис. 10).

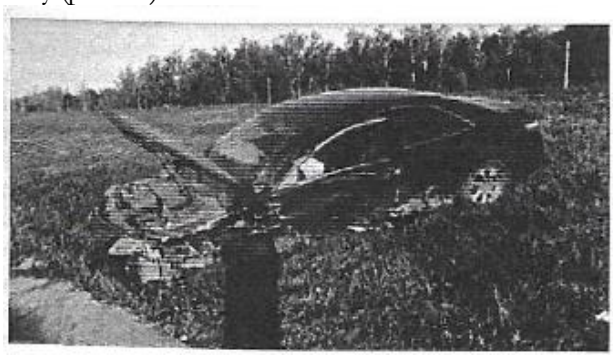

Рис. 10. Прикладний рівень (L7): маніпуляція сценаріями для введення в оману

Вплив на базові станції та систему загалом

Наведені вище приклади описують ризики, пов'язані з впливом на базові станції (БС), які можуть мати більш глобальні наслідки, ніж для акустичних терміналів (АТ). В мережах покоління 5G+ особливою рисою є орієнтація на підтримку високошвидкісних додатків у реальному часі, таких як управління дорожнім рухом, літальними апаратами та виробничими процесами. Через критичність часу реакції значна частина функціоналу була перенесена з ядра системи на БС.

Навіть невеликі затримки або сповільнення у роботі програмного забезпечення БС можуть призвести до серйозних техногенних катастроф через відсутність можливості швидкої реакції. Підвищений ризик виникає від використання продукції іноземного виробництва, оскільки може бути важко перевірити безпеку та стійкість до атак цих систем.

Відсутність повної інформації про програмне забезпечення БС, ядро системи або структуру застосованих сигналів відкриває можливості для запуску прихованих сценаріїв через ефір з будь-якого спеціалізованого терміналу. Показано приклад запуску описаного сценарію шляхом заземлення зарезервованих біт №2, 3, 5, 8-11 стандартного протоколу тунелювання на другому рівні L2 (рис. 11).

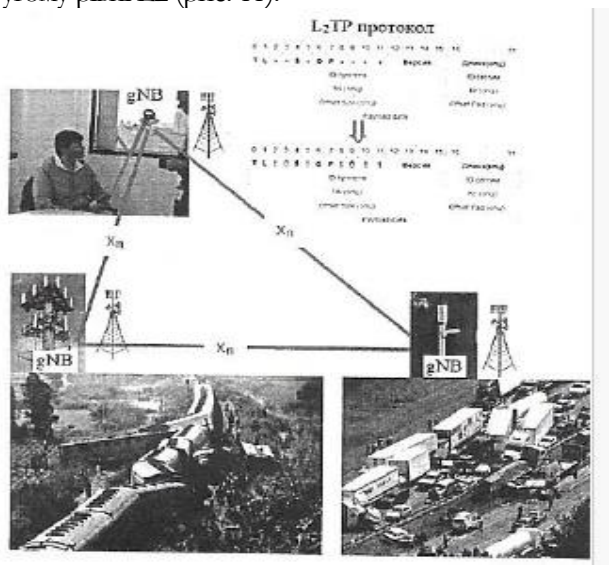

Рис. 11. Приклад злому системи зв'язку через БС шляхом використання недокументованих протоколом резервних біт

Такі команди можуть бути передані через мережу до віддалених БС, де і відбудеться активація несанкціонованих сценаріїв. Поділ у просторі та часі акту передачі команди та подальших дій ускладнює протидію таким атакам.

Уразливість професійних мереж, побудованих на основі WI-FI та WIMAX

Технології злому та протидії зломам для систем широкосмугового доступу (ШСД) Wi-Fi і WIMAX мають досить велику та багату історію. Анітрохи не претендуючи на повноту, можна вказати роботи [15-18] і матеріал відео навчання [19].

Зупинимося на поточному стані захищеності мереж Wi-Fi і WIMAX:

1. Нерозкритий захист залишає мережу вразливою до атак навіть при використанні останніх версій

програмного забезпечення. Наприклад, злам мережі може бути здійснений за допомогою скромних технічних засобів, якщо під час налаштувань буде допущена хоча б одна неточність;

2. Принципово незахищена процедура відкритого оповіщення про технічні параметри, такі як MAC-адреси, імена мереж і історія точок підключення, створює можливість для атак і порушення приватності;

3. Передача по ефіру незашифрованої команди відключення абонента від точки підключення може бути використана для здійснення атак типу "людина посередині" (MITM), що дає зловмиснику повний доступ до мережі;

4. Активний пошук ефективних атак на системи захисту докладається, і для нових методів захисту, наприклад, WPA2, пропонуються небезпечні методи, які можуть бути використані для перехоплення даних;

5. Відсутні ефективні способи протидії фізичним атакам на рівні WiMAX і Wi-Fi, такі як глушіння сигналу і лавинний наплив кадрів, що можуть призвести до виснаження батареї станції і втрати доступу до мережі.

Зважаючи на масове використання та афішування технічних параметрів, загроза злому й атак для Wi-Fi і WiMAX залишається постійною.

ВИСНОВКИ

Несанкціоновані впливи через чіпи SoC абонентських терміналів і базових станцій підкреслюють складність і потенційні ризики, пов'язані з розвитком цифрових технологій. З урахуванням цих викликів важливо, щоб національні виробники зосередилися на розробці та випуску власних чіпів SoC та систем радіозв'язку.

Це дозволить підвищити рівень контролю за безпекою та захистом цих систем, зменшуючи ймовірність несанкціонованих втручання і забезпечуючи більшу стійкість до потенційних атак.

ЛІТЕРАТУРА

[1]. JEDEC. Глобальні стандарти для індустрії мікроелектроніки. Standards & Documents Search [Електронний ресурс]. Режим доступу: https: // www. jedec. org / document _ search? search_api_views_ fultest=jesd209-4, вільний. Заголовок з екрана (24. 07.2020).

[2]. UFS 3. 1 vs UFS 3.0 Comparison: What's New and Different? [Електронний ресурс]. Режим доступу: https://www.smartpris.com/byles/uls-3-1-vs-ufs-3-0-comparison-new- features.

[3]. Your Phone Is Listening and it's Not paranoia [Електронний ресурс]. Режим доступу: https: // www. vice.com/en_au/article/wjazzy/your-phone-is-listaning-and-as-not-paranoia/utm_campaign=global& ut_source=vicefbartzi#javascript.

[4]. Navigation using ORB-SLAM [Електронний ресурс]. Режим доступу: https://ccc inacep.mx/Quetzaicuauhti/fotos.html.

[5]. Аджемов, С.С. Дослідження алгоритмів надвисокої роздільної здатності адаптивних антенних решіток /С.С. Аджемов, Г.О. Бокк, О.Г. Зайцев // Радіотехніка: 2000, 11. С. 68-71.

[6]. Аджемов, С.С. Модифікований алгоритм просторової роздільної здатності джерел радіовипромінювання SDS-MUSIC, що працює за багатопроменевого розповсюдження сигналів /С.С. Аджемов, Г.О. Бокк, О.Г. Зайцев та ін.//Радіотехніка. 2003. 11. 80 с.

[7]. Бокк, Г.О. Алгоритм ММО із застосуванням керування числом логічних каналів./Г.О. Бокк // Економіка та якість систем зв'язку. 2017. № 1 (3). С. 60-69.

[8]. Патент 2640030 C1 РФ: МПК H04917/00. Спосіб адаптивного розподілу частотно-часового ресурсу / Бокк Г.О. Шорін О.А. Заявник і патентовласник Товариство з обмеженою відповідальністю "НІРІТ-СІНВЕЙ Телеком Технолоджи" № 2017-112131; заявлено 11.04.2017; опубл. 26.12.2017. Бюл. № 36. 26 с.

[9]. Патент 170231 U1 РФ: МГПК H010 21/20 Всеспрямована кільцева антенна решітка / Бокк Г.О., Шорін О.А. Заявник і патентовласник Товариство з обмеженою відповідальністю "НІРІТ-СІН ВЕЙ Телеком Технолоджи" №2017103746; заявлено 06. 02.2017: опубл. 18.04.2017. Бюл. № 11. 7 с.

[10]. Патент 225459201 РФ: МПК 6015 13/04, 0015 3/74, G01S 7/295, G06F 17/15 Спосіб локації цілі (варіанти) / Дунаєв І.Б., Бокк Г.О.; заявник і патентовласник Дунаєв І.Б. №2003134395/09; заявлено 28.11.2003; опубл. 20.06.2005, Бюл. №17. 22 с.

[11]. Шорін, О.О. Аналітичне розв'язання варіаційної задачі Шеннона щодо визначення оптимальної структури сигналу в умовах обмеженої пікової потужності /О.О. Шорін, Г.О. Бокк // Економіка та якість систем зв'язку. 2013. № 1 (7). С. 30-39.

[12]. Шорін, О.О. Чисельні результати розв'язування варіаційної задачі Шеннона на визначення оптимальної структури сигналу в умовах обмеженої пікової потужності / О.О. Шорін, Г.О. Бокк // Економіка та якість систем зв'язку. 2018. № 1 (7). С. 39-47,

[13]. Шорін, О.О. Оптимальна структура дискретної ОАМ-модуляції, що забезпечує максимум інформаційної пропускної спроможності радіоканалу / О.О. Шорін, Г.О. Бокк // Економіка та якість систем зв'язку. 2018. №3 (9).С. 9-17.

[14]. Шорін, О.А. Зниження негативного впливу високих значень пік-фактору сигналів у системі Mc-

WILL. / О.О. Шорін, Г.О. Бокк // Економіка та якість систем зв'язку. 2019. №1(11). С. 9-13.
[15]. W-Fi мережі: проникнення та захист. Ч.1. Матчастина (Електронний ресурс). Режим доступу: https: //habr.com/ru/ post/224955, вільний.
[16]. Wi-Fi мережі: проникнення та захист. 4.2. Кай. Приховування SSID. MAC-фільтрація WPS (Електронний ресурс]. Режим доступу: https://tabir. com /ru/post/225483, вільний. Заголовок з екрана (25.08.2020).
[17]. Wi-Fi мережі: проникнення та захист. 4.3. WPA. OpenCL/CUDA. Статистика підбору (Електронний ресурс]. Режим доступ https://habe.com/ru/ post/220431, вільний Заголовок з екрана (25.08. 2020).
[18]. Ahson, S. Wimax: Standards and Security/S. Ahson, M. Ilyas-CRC Press, 2007. 276 p.
[19]. Злом і захист Wi-Fi. Опис технології. Hacking and Protection wi-fi. Description of technology [Електронний ресурс]. Режим доступу: https: // youtube.com/watch?v=uh0R:94408O, вільний.
[20]. Vanhoef, M. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2/M. Vanhool, F. Piessens [Електронний ресурс] Режим доступу: https:// papers.mathyvanhoef.com/ cos2017.pdf, вільний.

THE PROBLEM OF ENSURING THE SECURITY OF PROFESSIONAL RADIO COMMUNICATION SYSTEMS IN CRITICAL INFRASTRUCTURES

This paper reviews the existing and expected scenarios of unauthorized impacts on communication systems in critical information structures. It has been established that the area of increased risk of such impacts is focused on the interfaces between external devices and the SoC chip. Examples are given of grouping a large number of subscriber terminals operating under a single program of unauthorized influences, and the level of penetration can be increased many times over. It is noted that such possibilities become more realistic with the introduction of 5G generation systems that provide for M2M operation. The purpose of this review is to determine an approach to modeling the processes of protecting information from leakage through radio channels of communication systems and to develop engineering and technical measures for the design and implementation of appropriate information security systems.

Keywords: SoC chip, tampering, peripherals, 5G, X.200 open system model.

Шавловський Ярослав Сергійович, аспірант кафедри Систем інформаційного та кібернетичного захисту Державного університету інформаційно-комунікаційних технологій.

Yaroslav Shavlovsky, PhD student of the Department of Information and Cyber Defense Systems of the State University of Information and Communication Technologies.
E-mail: redwaveplus@ukr.net.
Orcid ID: 0009-0002-4737-9049.

Передерій Сергій Андрійович, завідуючий лабораторією кафедри Систем інформаційного та кібернетичного захисту Державного університету інформаційно-комунікаційних технологій.

Serhii Perederii, Head of the Laboratory of the Department of Information and Cyber Defense Systems at the State University of Information and Communication Technologies.
E-mail: seriy127@gmail.com.
Orcid ID: 0000-0002-1949-7868.

Бичков Володимир В'ячеславович, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету, помічник ректора Державного університету інформаційно-комунікаційних технологій.

Volodymyr Bychkov, Senior Lecturer at the Department of Information Technology Security at the National Aviation University, Assistant to the Rector of the State University of Information and Communication Technologies.
E-mail: bychkov.v@duikt.edu.ua.
Orcid ID: 0000-0002-1054-9182.

DOI: 10.18372/2410-7840.26.18820
УДК 336.71:004.056

МАТЕМАТИЧНИЙ АПАРАТ ЗНАХОДЖЕННЯ ОПТИМАЛЬНОЇ КОНФІГУРАЦІЇ ЗАХИЩЕНОЇ МЕРЕЖІ ЗВ'ЯЗКУ ІЗ ЗАДАНИМ ЧИСЛОМ АБОНЕНТІВ

Олександр Лаптєв, Аблуллах Аль-Далваш

Інформаційні потоки у світі зростають дуже швидко. Швидко зростає обмін інформацією. У зв'язку з цим фактом постійно розвивається існуючий математичний апарат та його практичне застосування. Науково-математичний апарат спрямовано на знаходження оптимальної конфігурації мережі інформаційного зв'язку, вирішенню проблеми побудови захищених каналів передачі великої кількості даних. Виникає наукове завдання щодо розробки нового та удосконалення існуючого математичного апарату для знаходження оптимальної конфігурації захищеної мережі зв'язку із заданим числом абонентів. Вирішенню цього актуального завдання і присвячена дана наукова робота. У ній сформульовано та доведено чотири Леми. Формулювання Леми дозволили довести дві нові теореми, які дозволяють вирішити завдання ефективного рішення