УДК 004.65
О. В. БАРАБАШ[1], доктор техн. наук, професор;
О. А. ЛАПТЄВ[1], канд. техн. наук, доцент, ст. наук. співробітник;
А. П. МУСІЄНКО[1], доктор техн. наук, доцент;
В. В. СОБЧУК[2], канд. фіз.-мат. наук, доцент,
[1] Державний університет телекомунікацій, Київ
[2] Східноєвропейський національний університет ім. Лесі Українки, Луцьк

МЕТОДИКА ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВА У ЦИФРОВОМУ ДІАПАЗОНІ

Проведено аналіз принципу дії телефонного зв'язку стандарту DECT та алгоритму ідентифікації «бази» та «трубки» цього стандарту. Приділено увагу якості передавання голосової інформації, що обґрунтовує використання такого виду зв'язку ще на тривалий період. Розглянуто можливість отримання інформації з використанням радіопристроїв, що працюють у легальному діапазоні стандарту DECT. Розроблено методику пошуку засобів негласного отримання інформації з інформаційної системи підприємства, що працює під прикриттям DECT, за допомогою розширеного функціонала телефонної станції Замовника. Зазначена методика ґрунтується на використанні методу RSS-визначення всіх базових станцій і мобільних трубок із нанесенням їх на схему об'єкта перевірки. Доведено, що такі радіозакладки можна виявити та локалізувати, застосувавши метод сканування по файлу «зразка», однак особливість буде полягати саме в отриманні файла «зразка». Такий файл потрібно формувати вдень за умови відімкнення баз DECT, які обслуговують дану інформаційну мережу, або вночі, коли є можливість отримати стабільну картину радіоефіру.

Ключові слова: інформаційна система; несанкціонований доступ; стандарт DECT; цифровий діапазон.

Вступ

Сьогодні на ринку технічного захисту інформації маємо широкий вибір систем радіоконтролю (радіомоніторингу) із різними технічними параметрами. Таким системам притаманна одна спільна властивість — вони можуть тільки унаочнювати та (у кращому разі) зберігати панорами спектрів сигналів у радіоефірі. Завдання аналізу цифрових легальних каналів зв'язку вони або не розв'язують взагалі, або виконують це формально, абияк. Причини різні — починаючи від незадовільної якості радіоприймального тракту і неможливості підімкнення до ПЕОМ (апарати типу Oscor Green), і закінчуючи простим нерозумінням або небажанням розв'язувати проблему. Навіщо щось змінювати, якщо споживач продовжує купувати застарілі рішення? А споживач зчаста навіть не знає про те, що виробник йому пропонує техніку, яка не може забезпечити якісну протидію сучасним загрозам.

Аналіз останніх публікацій та постановка проблеми. В [1] проаналізовано складність сучасного радіомоніторингу задля забезпечення захисту інформації в інформаційних системах підприємств. Проблема полягає в тому, що сучасні закладні пристрої з передавання інформації по радіоканалу все частіше використовують для передавання інформації ті ж самі стандарти, що і пристрої, які легально перебувають у приміщеннях. Тому наявні методи радіомоніторингу не в змозі визначити заставні пристрої, які працюють під прикриттям легальних пристроїв. Одним із найпоширеніших легальних діапазонів є діапазон безпроводового зв'язку DECT. Отже, дослідження методик виявлення несанкціонованих пристроїв в інформаційних системах підприємства, які працюють у даному діапазоні, є актуальним завданням.

У [2] розглянуто питання про користь «класичного радіоконтролю», де не розв'язуються питання аналізу цифрових каналів зв'язку стосовно сфери захисту інформації. І чи потрібен такий радіоконтроль на сучасному етапі розвитку засобів негласного отримання інформації. Особливо для виявлення цифрових засобів, які працюють на підвищених частотах. Окрім того, автори зазначають, що класичні методи радіоконтролю втрачають свою актуальність на сучасному етапі розвитку засобів негласного отримання інформації.

У [3] порушено проблему щодо уявного «цифрового» аналізу, коли йде підміна понять для введення в оману користувачів. Розглянуто реальні умови роботи на підприємстві, яке знаходиться в межах міста, найчастіше в місцях із щільною забудовою офісними, адміністративними та житловими будівлями. У радіоефірі активно працюють оператори мобільного зв'язку 2G/3G/4G, працюють мережі Wi-Fi, аналогове і цифрове телебачення та радіомовлення, службові радіомережі МВС, МНС, системи радіосигналізації, радіоаматори, авіація тощо. Показано, що оператор із комплексом радіоконтролю без розв'язання завдань аналізу цифрових каналів зв'язку не може визначити цифрові закладки при класичному радіомоніторингу, оскільки всі джерела радіосигналу

цифрового діапазону на екрані оператора мають однаковий вигляд.

З огляду на проведений аналіз, можна дійти висновку, що застосування «класичного радіоконтролю» на сучасному етапі розвитку електроніки для пошуку цифрових засобів негласного отримання інформації можливе тільки в обмеженому обсязі. Проблему пошуку цифрових засобів негласного отримання інформації (передусім тих, які працюють в легальних діапазонах радіоефіру), даний метод вирішити не може. Тому завдання створення методики пошуку засобів негласного отримання інформації в цифровому діапазоні радіоефіру стандарту DECT є дуже актуальним.

Основна частина

Для розуміння ситуації необхідно уявити, що сьогодні являє собою типовий об'єкт, який потребує захисту. Оператор із комплексом радіоконтролю без вирішення завдань аналізу цифрових каналів зв'язку отримує спектр, наведений на рис. 1.

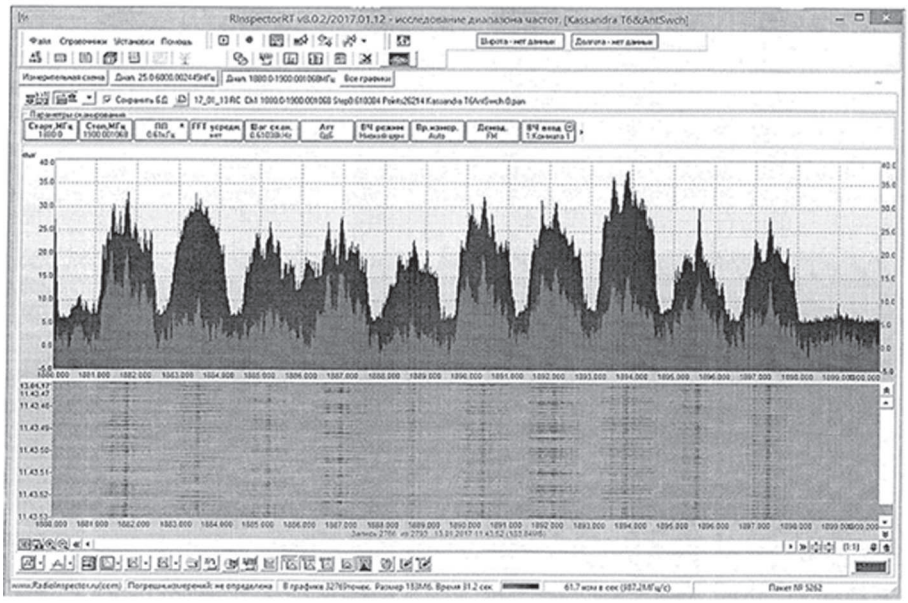

Рис. 1. Спектограма реально працюючих «баз» і «трубок» DECT

Як виявити на об'єкті працюючу закладку з передаванням у діапазоні DECT? Згідно з описом стандарту на кожній частоті може одночасно працювати 24 пристрої — 12 базових станцій («баз») і 12 абонентських пристроїв («трубок»). У діапазоні 1880…1900 МГц таких частот 10 і практика показує, що майже скрізь, у великих бізнес-центрах або адміністративних будівлях, зазвичай зайняті всі 10 каналів, тобто 240 пристроїв DECT, робота на яких ведеться неперервно.

При класичному радіоконтролі фахівець із пошуку і блокування засобів негласного отримання інформації вимикає свою «базу» DECT (бажано і «трубки», які зареєстровано на ній) і аналізує рівні сигналів. Сигнал, який залишився на екрані комп'ютера комплексу радіомоніторингу, і буде сигналом (випромінюванням) засобів негласного отримання інформації, що працює під прикриттям стандарту DECT. Локалізація такого засобу відбувається за допомогою додаткової апаратури пошуку: детектора поля, універсального пошукового приладу, нелінійного локатора та ін.

Якщо потрібно виконати роботи з пошуку і блокування засобів негласного отримання інформації таємно або, як мінімум, не порушуючи режим роботи співробітників підприємства, цей варіант неприйнятний. Оскільки, по-перше, не дозволять вимкнути «бази» і «трубки» DECT і, по-друге, якщо інформацію отримують у реальному часі і цей процес контролюється, то зловмисник вимкне свою радіозакладку (вочевидь, використовуючи такий рівень підготовки, закладка буде дистанційно керованою). До того ж, неможливо вимкнути «бази» і «трубки» DECT у суміжних приміщеннях (якщо вони належать іншим власникам). Як наслідок, дістаємо постійно змінний рівень сигналів і складність у визначенні закладки, що працює у стандарті DECT.

Варіант спроби прослухати DECT нами відхилявся, тому захищеність зв'язку досягатиметься завдяки прописку (прив'язці): безпроводової трубки до однієї або кількох базових станцій. У разі прив'язки трубка і станція отримують ідентифікаційний ключ. Тому при кожному встановленні зв'язку за допомогою цього ключа база і трубка будуть впізнавати один одного і будь-яке підмикнення, яке не змогло «назвати пароль», буде розірвано.

Одним із запропонованих варіантів виявлення закладки, що працює в стандарті DECT, є отримання так званого радіоефіру зразка (у пошукових

автоматизованих комплексах його найчастіше називають файлом «зразка») у даному приміщенні вночі. Нічний час обрано через можливість лише в цей період отримати стабільну картину радіоефіру, тобто файл «зразка». Однак такий варіант не дає повної гарантії виявлення радіозакладки. Тобто додатково до цього способу необхідно додавати щонайменше один прямий або кілька непрямих ознак виявлення роботи радіозакладки.

Розглянемо технологію позиціонування і моніторингу рухомих об'єктів у мережах DECT. Її засновано на періодичному (раз у 5-10 секунд) вимірі кожним абонентським пристроєм потужності сигналу (метод **RSS** — *Received Signal Strength*) від усіх базових станцій (БС) своєї мережі, які пристрій здатний виявити. Виміряні значення передаються по радіоканалу DECT на контролер БС і далі на сервер бази даних (СБД). Програмне забезпечення сервера, що забезпечує позиціонування, аналізує пропозиції, які надійшли на СБД, і визначає відстань від абонента до кожної з БС. Якщо розташування всіх БС у DECT-системі відомо і нанесено на план, то місцезнаходження абонента може бути визначено розв'язком геометричної задачі або завдання кластеризації і розпізнавання. Отже, абонент, що постійно перебуває на одному місці, і є радіозакладка. Це варіант визначення «чужого» приймача і джерела в своєму офісному діапазоні DECT, тобто без залучення зовнішніх фахівців пошуку і блокування засобів негласного знімання інформація [4].

Остаточним вирішенням проблеми пошуку радіозакладок DECT ми вважаємо аналіз заголовків цифрових пакетів. **RFPI** (*Radio Fixed Part Identity*) — це унікальний радіоідентифікатор базової станції DECT. Теоретично RFPI має бути винятковий для будь-якої БС в глобальному сенсі. Практично — він може бути унікальний для БС DECT у масштабі окремої мікросотовой системи. RFPI — це аналог MAC-адреси в стандарті DECT.

На жаль, пакети, що передаються від абонентських пристроїв («трубок») до базової станції («бази») під час передавання даних (мови), не містять унікальних ідентифікаційних номерів абонентських пристроїв. Унікальні номери абонентських пристроїв передаються від «трубки» до «бази» тільки в процесі їх синхронізації. Записати і проаналізувати цей процес досить проблематично. Однак у кожному пакеті від «трубки» до «бази» і від «бази» до «трубки» міститься унікальна 20-бітова адреса базової станції. Тому завдання пошуку незаконно працюючих передавачів у стандарті DECT можна звести до аналізу «видимих» базових станцій і порівнянню їх зі списком легальних базових станцій. Такого висновку можна дійти з огляду на постулат, що для організації нового каналу зв'язку в стандарті DECT необхідні щонайменше одна «трубка» і одна «база» [5]. Базову станцію може бути не видно з контрольованого приміщення, але її наявність буде визначено в ПЗ за допомогою модулювання заголовку пакета абонентського пристрою. Амплітуда базової станції, якої не видно, та її наявність визначається тільки за прийнятим пакетом абонентського пристрою, у програмному забезпечені позначається як 40 дБ.

У режимі аналізу сигналів безпроводових мереж стандарту DECT програмне забезпечення автоматичних пошукових комплексів направлено на вирішення актуальної задачі щодо ідентифікації всіх працюючих у радіусі приймання пристроїв даного стандарту. Для аналізу пакетів ПЗ демоделює і аналізує їх відкриті заголовки. Прикладом такого аналізу може бути аналіз за допомогою ПЗ «DTest» [6]. Аналіз стандартів цифрового передавання даних за допомогою цього ПЗ зображено на рис. 2.

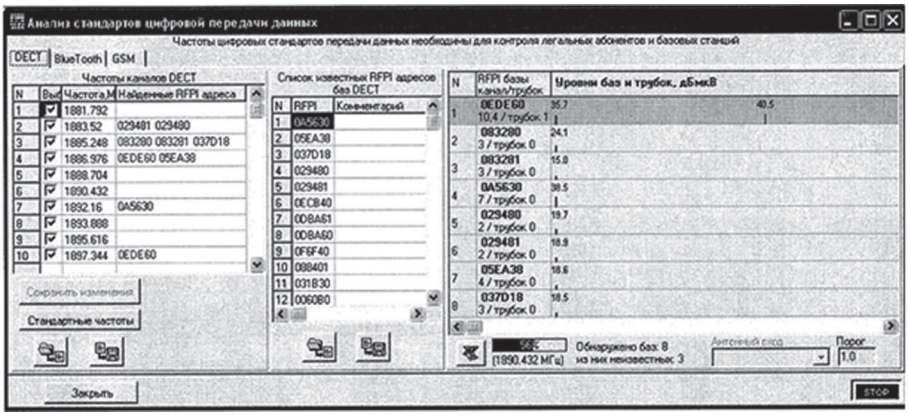

Рис. 2. Аналіз стандартних цифрових сигналів за допомогою програмного забезпечення «DTest»

Порівнюючи RFPI всіх виявлених пристроїв, можна розпізнати засіб негласного отримання інформації, який працює в стандарті DECT із високим ступенем достовірності.

Отже, з огляду на проведений аналіз можна сформулювати методику пошуку засобів негласного отримання інформації, що працюють під прикриттям у діапазоні DECT в інформаційній

системі підприємства. Дана методика полягає в таких заходах:

1. Використовувати розширений функціонал телефонної станції Замовника. За потреби встановлювати необхідні програмні засоби. Ці програмні засоби мають бути індивідуальні для кожної АТС.

2. Застосовувати метод RSS-визначення всіх базових станцій і мобільних трубок із нанесенням їх на схему об'єкта перевірки.

3. Послуговуватися методом сканування по файлу «зразка». Особливість полягатиме саме в отриманні файла «зразка». Створювати його треба вдень із можливістю вимикання баз DECT, які обслуговують дане приміщення, або вночі, коли можна отримати стабільну картину радіоефіру.

4. Найнадійніший метод — це метод, заснований на аналізі заголовків цифрових пакетів. RFPI — це унікальний радіоідентифікатор базової станції DECT. Порівнюючи відомі (свої) ідентифікатори баз DECT зі всіма визначеними в результаті сканування, отримуємо найбільш достовірну інформацію про радіозакладку, що працює в діапазоні DECT.

Висновки

1. Здійснено короткий огляд принципу роботи телефонного зв'язку DECT та пристроїв негласного отримання інформації, які працюють у частотному діапазоні стандарту DECT в інформаційній системі підприємства. Приділено увагу якості передавання голосової інформації, яка обґрунтовує використання такого виду зв'язку ще на тривалий період.

2. Наведено спектрограму і реальний Web-інтерфейс апаратно-програмного комплексу, фактично отриманих сигналів сканування радіодіапазону стандарту DECT.

3. Розроблено методику пошуку засобів негласного отримання інформації, що працюють під прикриттям частоти DECT, яка дає можливість із дуже високим ступенем імовірності визначати засоби отримання інформації, що функціонують у стандарті частоти DECT.

Список використаної літератури

*1. **Хорев А. А.** Техническая защита информации: учеб. пособие для студентов вузов. Т. 1. // Технические каналы утечки информации. Москва: «НПЦ Аналитика», 2008. 436 с.*

*2. **Мусієнко А. П., Лукова-Чуйко Н. В., Коваль М. О.** Використання мереж Петрі для побудови моделі виявлення зовнішніх впливів на інформаційну систему // Системи управління, навігації та зв'язку, 2018. Вип. 2 (48). С. 77–82.*

*3. **Блиялкин П. А.** Выявление электронных устройств перехвата акустической речевой информации, построенных на базе средств беспроводной связи // Молодой ученый. 2016. №14. С. 124–128. [Электронный ресурс]. URL: https://moluch.ru/archive/118/32820/ (07.06.2019).*

*4. **Власов А. М.** Беспроводная офисная связь: DECT и Wi-Fi // [Электронный ресурс]. URL: http://www.dect.ru/dect.html (05.05.2016)*

*5. **Забезпечення** функціональної стійкості інформаційних мереж на основі розробки методу протидії DDoS-атакам / О. В. Барабаш, Н. В. Лукова-Чуйко, А. П. Мусієнко, В. В. Собчук // Сучасні інформаційні системи, 2018. Т. 2. № 1. С. 56–64.*

*6. **Форум** технической поддержки ПО «Радио-Инспектор» – Опция DTest (Digital Test) [Электронный ресурс]. URL: http://inspectorsoft.ru/forum/viewtopic.php?id=2222 (05.05.2019).*

Рецензент: доктор техн. наук. професор **В. А. Савченко**, Державний університет телекомунікацій, Київ.

О. В. Барабаш, А. А. Лаптев, А. П. Мусиенко, В. В. Собчук

МЕТОДИКА ВЫЯВЛЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ ПРЕДПРИЯТИЯ В ЦИФРОВОМ ДИАПАЗОНЕ

Проведен анализ принципа действия телефонной связи стандарта DECT и алгоритма идентификации «базы» и «трубки» этого стандарта. Уделено внимание качеству передачи голосовой информации, обосновывая использование такого вида связи еще на длительный период. Рассмотрена возможность получения информации с использованием радиоустройств, работающих в легальном диапазоне стандарта DECT. Разработана методика поиска средств негласного получения информации из информационной системы предприятия, работающего под прикрытием DECT, с помощью расширенного функционала телефонной станции Заказчика. Данная методика базируется на использовании метода RSS-определения всех базовых станций и мобильных трубок с нанесением их на схему объекта проверки. Доказано, что такие радиозакладки можно обнаружить и локализовать, применив метод сканирования по файлу «образца», однако особенность будет заключаться именно в получении файла «образца». Данный файл нужно формировать в дневное время, если есть возможность отключить базовые станции DECT, обслуживающие данную информационную сеть, или в ночное время, когда мы можем получить стабильную картину радиоэфира.

Ключевые слова: информационная система; несанкционированный доступ; стандарт DECT; цифровой диапазон.

O. V. Barabash, O. A. Laptev, A. P. Musienko, V. V. Sobchuk

METHOD OF DETERMINING NONSANCED ACCESS TO INFORMATION SYSTEMS OF THE ENTERPRISE IN DIGITAL RANGE

In the work the analysis of the principle of telephone service DECT standard and algorithm identification of the base and tube of this standard. Attention is paid to the quality of voice information transmission, which substantiates the use of this kind of communication for a long period of time. The possibility of receiving information using radio devices operating in the legal range of the DECT standard is considered. The method of searching for means of secretly receiving information from the information system of the enterprise, which operate under the cover of DECT with the help of the expanded functionality of the telephone exchange of the Customer, is developed. This methodology is based on the use of the method of RSS determination of all base stations and mobile handsets, and their application to the scheme of the object of verification. It is proved that such radio libraries can be detected and localized using the «sample» file scan method, but the feature will be to get the sample file. This file needs to be formed during the day if it is possible to disconnect DECT databases that serve this information network or at night when we can obtain a stable picture of the airspace.

Keywords: information system; unauthorized access; DECT standard; digital range.