**SAT-2G.302-1-CSNT-02**

# Current problems in monitoring modern types of special technical means and ways to solve

Vasya Iliev, Stefan Parvanov

# Актуални проблеми при мониторинг на съвременните видове специални технически средства и пътища за тяхното преодоляване

Вася Илиев, Стефан Първанов

***Abstract:*** *A review and comparative analysis have been made of the modern methods for secretly obtaining of information by special technical means. The problems of detecting this type of equipment have been analyzed. Requirements have been defined for the functioning of the hardware and software complex used for monitoring of the secured site. Specific methods have been marked for detecting and counteracting the unauthorized leaks of information from standard and custom telecommunication channels.*

***Key words:*** *special technical means, radiomonitoring*, *radiofrequency spectrum, ultra-wideband signals.*

## ВЪВЕДЕНИЕ

Съвременните специални технически средства (СТС), използвани за негласно придобиване на информация по радиоканал (за простота наричани радиомикрофони), през последното десетилетие напреднаха в своето развитие толкова напред, че много от комплексите за радиомониторинг и контрол не са в състояние да ги разкрият с нужната степен на вероятност за осигуряване на надеждна защита на информацията. На практика търсенето и откриването на този вид устройства се усложнява от няколко фактора. Първо, разработчиците на този вид устройства прилагат все по-нови и съвършени методи за скрито излъчване на своите изделия. Така например, още на етапите на проектиране на СТС, се залагат прости и ефективни методи за маскиране, чрез задаване на работните им честоти в близост до мощни легални радиопредаватели, излъчването на които обърква и блокира системите за мониторинг, както и маскирането им в стандартни канали за свръзка, чрез теснолентово излъчване вътре в спектъра на легален широколентов канал. Второ, продължава пренасищането на радиоефира от излъчванията на влизащи в експлоатация на нови радиокомуникационни мрежи и системи. В момента практически целият радиочестотен спектър е зает от работата на легални радиопредаватели. Това силно усложнява не само електромагнитната съвместимост, но и мониторинга на радиоизлъчванията. Трето, високата интензивност на индустриалните смущения, особено в големите градове, прави практически невъзможно прихващането и разкриването на СТС използващи свръхширококолентови UWB сигнали.

## СЪВРЕМЕННИ МЕТОДИ ЗА НЕГЛАСНО ПРИДОБИВАНЕ НА ИНФОРМАЦИЯ

За създаване на ефективни методи и алгоритми за търсене и разкриване на съвременните видове СТС, трябва да се анализират насоките и направленията, по които се работи в настоящия момент за повишаване на тяхната скритост.

Основните направления [3,4,6,10] в тази насока са следните :

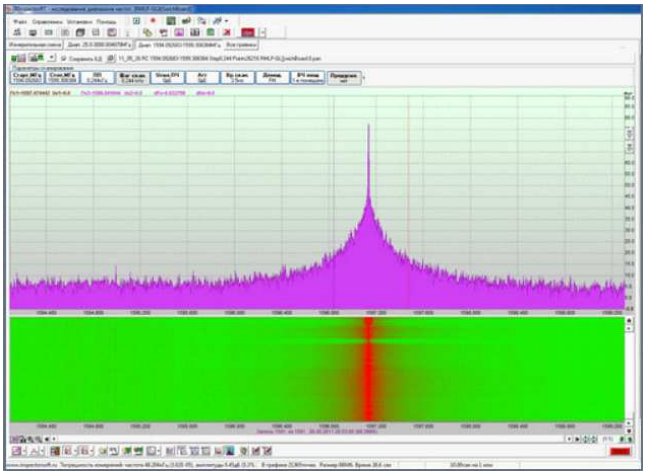
- използване на сложни видове радиосигнали за предаване на прихванатата информация (шумоподобни, хаотични, фрактални, свръхширококолентови и др.), работещи под нивото на шума;

- използване на СТС с натрупване на прихванатата информация и последващото и компресиране и излъчване за кратък период от време, от порядъка

на няколко секунди или милисекунди;

- използване на стандартни (легални) канали за предаване на прихванатата информация (DECT, Bluetoot, Zigbee, Wi-Fi, GSM, CDMA, TETRA и др.) явяващо се най-опасното направление в момента.

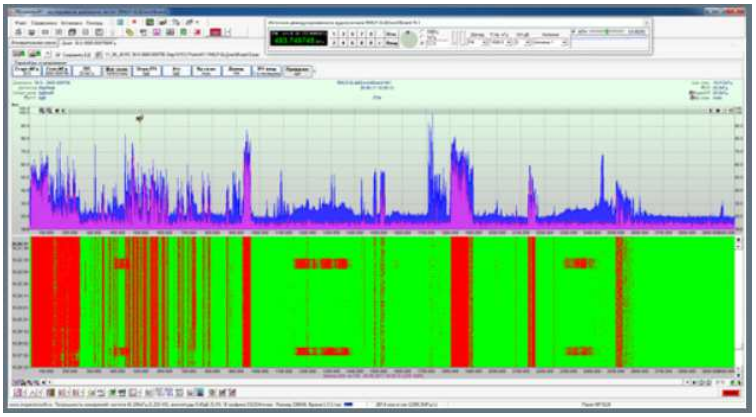
В класическите случаи, когато радиомикрофонът работи непрекъснато, обикновено излъчва на една честота и проблеми с разкриването му не трябва да има (фиг. 1).



***Фиг. 1.*** *Честотен спектър в близката зона на аналогов радиомикрофон излъчващ на честота 1597,2 MHz. Нивото на сигнала значително превъзхожда стандартните излъчвания, а обвиващата на спектъра е модулирана в съответствие с изменението на говора в охранявания обект*

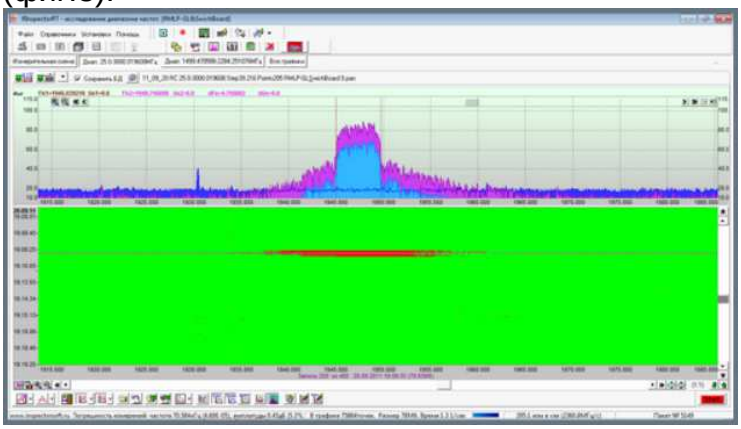
В съвременните СТС с междинно натрупване на информацията, както например SIM-BURST и INCA ULL [3], при честотна лента на излъчвания сигнал 12 MHz, позволява компресиране на информацията от порядъка на 100 към 1. Това означава, че при натрупване на говорна информация в продължение на 100 секунди, времето за нейното предаване ще бъде 1 секунда. В случаите на използване на свръхшироколентови UWB сигнали с ширина на спектъра от 3MHz до 3GHz, е възможно излъчване на информацията, натрупвана в рамките на един месец буквално за 30 секунди. От това веднага става ясно, че търсенето и разкриването на този вид СТС налага непрекъснато провеждане на целодневен радиомониторинг и контрол в района на охранявания обект.

На фиг. 2 е показана спектрограмата на излъчвания сигнал на СТС от този вид [6]. Вследствие на специфичната и нестандартна форма на спектъра им, те привличат вниманието на специалистите, разполагащи с необходимата апаратура, благодарение на което при непрекъснат системен мониторинг те могат да бъдат засечени и разкрити.



***Фиг. 2.*** *Форма на спектъра на широколентов радиосигнал излъчен от радиомикрофон с междинно натрупване на информацията за 100 секунди и кратковременно излъчване в рамките на 300 милисекунди*

При търсене и разкриване на СТС работещи с шумоподобни и свръхшироколентови сигнали, може да се отбележи следното: методите за тяхното разкриване се основават на факта, че в близката зона и в непосредствена близост до СТС, нивото на спектъра на сигнала обикновено е над нивото на шума, поради което при «надигането му» в отделни честотни диапазони е свидетелство за работа на такъв вид СТС (фиг.3).



***Фиг. 3.*** *Честотен спектър на СТС работещо с шумоподобен сигнал (DSSS) в близката зона [7]*

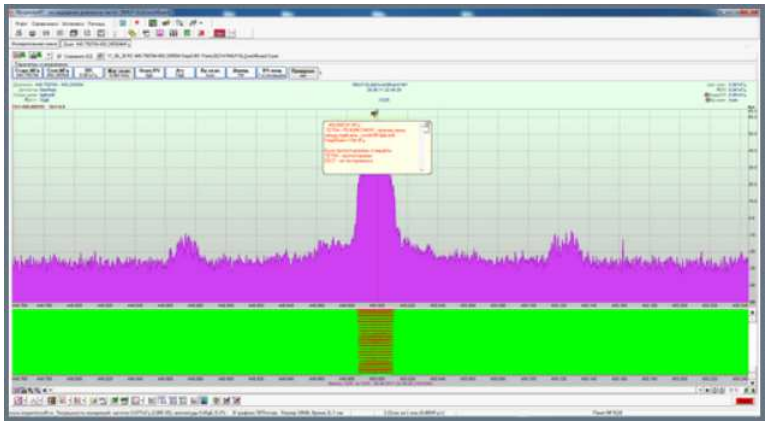
За търсене на «хитри» СТС, които са маскирани под спектъра на легалните радиосигнали във вид на теснолентови сигнали е необходимо радиомониторинговият комплекс да има възможност за детайлно изследване на спектъра на сигнала с разрешаваща способност от порядъка на херци. Несъмнено, опитът на оператора и неговата интуиция в случая имат решаващо значение. Освен това апаратурата и програмното осигуряване на комплекса трябва да позволят на оператора да изпълнява такъв вид задачи.

Как стои въпросът с търсенето и откриване на СТС, работещи в легалните канали за предаване на данни, като DECT, Bluetoot, Zigby, Wi-Fi, GSM, CDMA и др.

Спектърът на сигнала, излъчван от този вид СТС, изглежда напълно еднакво със спектъра, излъчван от легалните канали за предаване, независимо от това, дали се излъчват от СТС или от напълно «мирно» устройство. Високата степен на опасност в този случай се заключава в това, че специалистът, даже и да разполага със съвременни технически средства за мониторинг и контрол, не е в състояние да различи работещите по своето предназначение легални радиотехнически устройства от СТС. За разкриването им е необходимо те да са съоръжени с допълнителни апаратни и програмни средства за анализ на цифровите пакети с данни в реален мащаб от времето. Освен това комплексът за радиомониторинг на този вид СТС трябва да има и възможност за допълнителен анализ на мрежите, позволяваща да се идентифицират адресите на „чуждите" абонатни устройства.

Заплахите, с които биха могли да се сблъскат специалистите по разкриване на СТС, използващи радиоканалите за транкингова комуникация, ще бъдат разгледани чрез конкретен пример [8] в стандарта TETRA. Основният режим на работа в този стандарт е транкинговият - ТМО, с използване на базовите станции. При този режим системата за сигурност и контрол на достъпа в мрежата не допуска използването на радиотерминалите извън предназначението им. В случаите, когато се работи в режим на директна връзка между абонатите – DMO (без участието на базовите станции), е възможно несанкционирано придобиване на информация с помощта на TETRA терминална станция в качеството и на СТС. Този режим позволява дистанционно включване и активиране на друга TETRA станция в режим DMO, без каквито и да е демаскиращи признаци, че станцията работи в режим на предаване. В

случая тя не издава никакви предупреждаващи сигнали, не работи дисплеят и, и не засветват бутоните. При това, микрофонът на станцията е с максимална чувствителност и позволява спокойно прослушване на разговорите на няколко метра от него. По аналогичен начин могат да бъдат включени в режим «акустика» и други видове станции, използващи съвременни стандарти за професионална мобилна комуникация като: DRM, APCO, P25 и др, естествено трябва само да се знае как.



***Фиг. 4.*** *Форма на спектъра и съобщение за несанкционирано излъчване от негласно активиран терминал TETRA в режим на работа DMO*

За откриването на такъв вид СТС, системата за радиомониторинг трябва да е в състояние да анализира режимите на работа в отделните честотни канали на съответния стандарт и да определи дали измежду тях има неконтролируемо активиран режим за директна връзка (DMO) и да издаде съобщение на екрана на мониторинговия комплекс, както е показано на фиг.4.

**Изисквания към алгоритъма на работа на апаратно-програмните комплекси за мониторинг и контрол на съвременните видове СТС**

Изхождайки от горепосочените съображения, могат да се формулират конкретните изисквания към алгоритъма на работа на мониторинговия комплекс за разкриване на съвременните видове СТС.

1. Апаратната част на съвременният комплекс за радиомониторинг и разкриване на СТС трябва да притежава **достатъчно висококачествени трактове за аналогова и цифрова обработка на сигнала**, които да му осигурят нормална работа в присъствието на мощни смущения. Ситуацията, при която съвместно със заложеното СТС в лентата на преселектора работи мощно легално свързочно средство, нивото на което надвишава нивото на СТС с 80 – 100 dB, в момента не е рядкост. Ако сигналът от СТС или „смущението“ превишават динамичният диапазон на приемния радиотракт, то в спектрограмата на сигнала ще се съдържат множество лъжливи странични и комбинационни сигнали, крайно нестабилни по честота, амплитуда и време. Като пример, ще бъде посочен един от най-съвременните и качествени измерителни приемници за тази цел, Rohde&Schwarz - *EM100* [10] със следните техническите параметри:

- честотен диапазон: 5 kHz – 3 GHz;
- чувствителност: - 158 dBm (1GHz, BW = 8 Hz);
- динамичен диапазон без атенюатор: по-добър от 85dB;
- скорост на сканиране: до 1400 MHz/s при лента 40 kHz;
- честотна лента на анализ: от 8Hz до 40kHz.

2. Съвременният комплекс за радиомониторинг трябва да има достатъчно гъвкаво и многофункционално програмно осигуряване, което да позволява реализирането на следните функции:

• да осигурява целодневен радиомониторинг в определени честотни диапазони

и да съхранява всички измерени спектрограми за последващ анализ и сравнение;

• да осигурява анализ на амплитудно-честотно-времевото представяне на резултатите от радиомониторинга в реално време;

• да осигурява детайлен анализ на спектъра на прихванатите сигнали с разрешаваща способност от порядъка на 1 Hz;

• Да може допълнително да изследва излъчванията на стандартните канали за свръзка, като DECT, Bluetoot, Zigby, Wi-Fi, GSM, CDMA и др., за наличието на „чужди" абонати в мрежата.

3. Съвместно с изброеното по-горе, програмното осигуряване трябва да може да подържа и традиционните методи за търсене, използвани широко в практиката като:

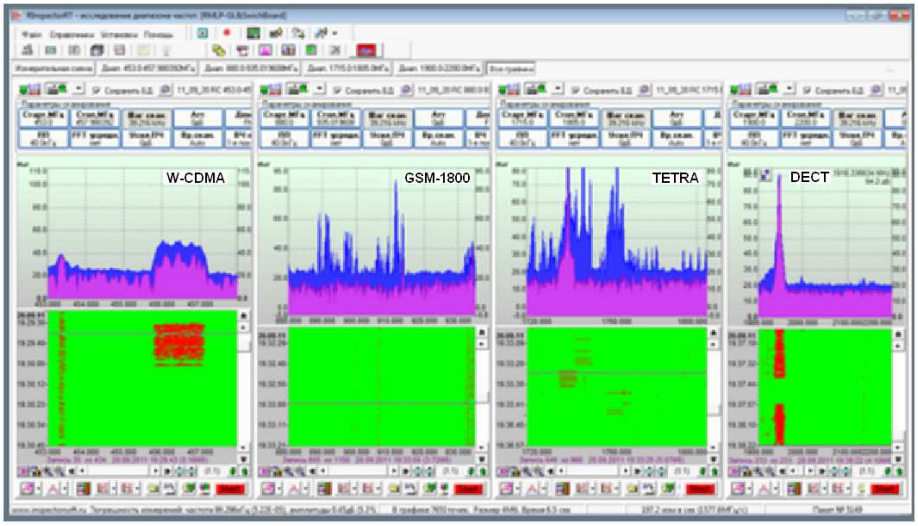
- методи с разнесени антени реагиращи на градиента на полето;
- метод за сравнение с еталонна панорама;

• използване на селективна линия за праг и формиране на списък от сигнали, превишаващи линията на прага;

• детайлен анализ на характеристиките на спектрите на приетите сигнали;

• автоматичен запис на фонограмите и нискочестотен анализ на демодулирания аудиосигнал.

Освен всичко казано до тук, за осигуряване на надеждна защита на охранявания обект е желателно мониторинговия комплекс да може да контролира излъчванията от няколко източника едновременно, чрез т. н. могопрозоръчен режим на работа, както е показано на фиг. 5.




***Фиг. 5.*** *Многофункционален режим на работа на система за радиомониторинг и контрол на СТС описана в [10] с едновременно контролиране и графично изобразяване на четири стандарта за мобилна комуникация*

## ЗАКЛЮЧЕНИЕ

Съвременните СТС за несанкционирано придобиване на информация в настоящия момент до такава степен са усъвършенствани, че на практика е невъзможно те да бъдат прихванати и разкрити с помощта на класическите средства и методи за тази цел. За разкриването им е необходимо да бъдат използвани сложни апаратно-програмни комплекси за непрекъснат радиомониторинг и контрол в района на охранявания обект. Те трябва да са съоръжени и с висококачествени измерителни радиоприемни устройства, както и с гъвкаво и многофункционално програмно осигуряване, позволяващо мониторинг и контролира в реално време както на стандартните, така и на нестандартните канали за връзка.

**ЛИТЕРАТУРА**

[1] Андрианов В.И., Бородин В.А., Соколов А.В.” Шпионские штучки “ и устройства для защиты объектов и информации: Справ. Пособие, Изд.Третое, С-Пб.: Лань, 2006.

[2] Василевский И.В. Sedif 2.0.Управляющая программа для сканирующих приемников R&S - *EM100* и AR-8000 // Защита информации. – 2008. № 6. – С. 49... 55.

[3] Вовченко В.В., Степанов И.О. Проблемы защиты информации от экономического шпионажа // Защита информации. – 2009. № 1. – С. 48...64.

[4] Лунегов А.Н., Рыжов А.Л. Технические средства и способы добывания и защиты информации. - М.: ВНИИ “Стандарт”, 2011. – 95 с.

[5] Технические средства разведки / Под ред. Мухина В.И.–М.: РВСН, 2002.– 335 с.

[6] Burmin, V.A. Multi-functional complex for Monitoring of Information Security Effectivenes. Special technologies, 2012, pp. 53-75.

[7] Robson, D. S. Techniques for wildlife investigations: Design and analysis of capture data. Academic Press, 2009, 237 pp.

[8] Jones, T.I. Radio monitoring: Problems, Methods and Equipment (Lecture Notes in Electrical Engineering), Springer 2009.

[9] Skalski, J. R.. A design for long-term status and trends monitoring. J. Envir. Manage. 2010, pp.139-144.

[10] Kuznets, Y. N. and Baev, A. B. Methods of CEE Measurement: Comparative Analysis. Confident, № 4, 2012, pp. 54.

**За контакти:**

доц. д-р инж. Вася Илиев, катедра „Техника” на факултет ПБЗН при Академия на МВР, тел.: 02/9821084, e-mail: viliev.24@abv.bg

ас. инж. Стефан Първанов, катедра „Тактика” на факултет ПБЗН при Академия на МВР, тел.: 02/9821279, e-mail: sip_81@abv.bg