DOI:**10.33099/2311-7249/2019-35-2-35-42**

УДК 004.056

Олександр Анатолійович Лаптєв *(кандидат технічних наук, с.н.с.)*[1]
Роман Іванович Грозовський[2]

[1]*Державний університет телекомунікацій, Київ, Україна*
[2]*Національний університет оборони України імені Івана Черняховського, Київ, Україна*

АНАЛІЗ ТА ТЕНДЕНЦІЇ РОЗВИТКУ ЗАСОБІВ ПОШУКУ ЦИФРОВИХ РАДІОЗАКЛАДОК

У статті розглянуто питання витоку або втрачання інформації, що може спричинить матеріальний збиток або може привести до катастрофічних наслідків в об'єкті управління - виробництві, транспорті та військовій справі. Сучасна військова наука стверджує, що повне позбавлення засобів зв'язку зводить боєздатність армії до нуля. Проведено аналіз різних за принципом роботи, пошукових приладів, та методів пошуку засобів негласного отримання інформації. Аналіз дозволяє зробити висновок, що на сучасному етапі розвитку суспільства процес пошуку засобів негласного отримання інформації виходить якісно на інший рівень. Тому методи пошуку та обладнання, які використовуються для цього потребують удосконалення, а проблема аналізу засобів пошуку цифрових радіозакладок з метою виявлення тенденції розвитку та розробки сучасних вимог до них стає актуальною. Розглянуто методи приховування роботи радіозакладок, що застосовуються при розробці радіозакладок. Відзначено, що в даний час набагато легше зробити цифровий передавач, використовуючи сучасну елементну базу стандартних засобів зв'язку, ніж конструювати і налагоджувати «аналогову» закладку на транзисторі з позитивним зворотним зв'язком. Тому сучасні і перспективні технології впливають на можливості сучасних засобів негласного отримання інформації. Сучасні радіозакладки можуть використовувати різні методи приховування каналу передачі даних, що дуже ускладнює процес їх пошуку. Особливо, якщо вони використовують комбіновані методи приховування каналу передачі даних.

Враховуючи особливості сучасних розробок засобів негласного отримання інформації, надано повний методичній набір вимог щодо проектування та створення сучасних автоматизованих пошукових комплексів, які відповідають процесу сучасного автоматизованого пошуку цифрових радіозакладок в повному обсязі. Дані вимоги можуть використовуватися як технічне завдання при проектуванні автоматизованих програмних комплексів пошуку цифрових радіозакладок.

Ключові слова: *радіозакладка, пошук, радіоканал, радіомоніторинг, автоматизований програмний комплекс*.

Вступ

Постановка проблеми. У сучасному світі з підвищенням значності та цінності інформації відповідно зростає важливість її цілісності та захисту. Інформація коштує грошей, отже, витік або втрата інформації спричинить за собою значні матеріальні збитки. З іншого боку, інформація-це засіб управління. Несанкціоноване втручання в управління може привести до катастрофічних наслідків в об'єкті управління-в першу чергу на транспорті та військовій справі. Наприклад, сучасна військова наука стверджує, що повне позбавлення засобів зв'язку зводить боєздатність армії до нуля. Тому питання збереження цілісності інформації сьогодні стають актуальними як ніколи раніше. Кількість використовуваної цифрової техніки в сучасному світі продовжує зростати, отже, зростає і значущість організаційної та програмно-технічного захисту від витоку або порушення цілісності інформації. Під витоком інформації з технічного каналу розуміється неконтрольоване поширення інформації від носія інформації, що захищається через фізичне середовище до технічного засобу, який здійснює перехоплення інформації. Залежно від фізичної природи виникнення інформаційних сигналів, середовища їх поширення-технічні канали витоку акустичної або речовій інформації можна розділити на прямі акустичні (повітряні), акустовібраційні (вібраційні), акустооптичні (лазерні), акустоелектричні (параметричні) [1]. Причому інформацію, не санкціоновано отриману з перерахованих вище каналів витоку інформації найпростіше передати по радіоканалу, у зв'язку з чим пошук радіоканалів засобів несанкціонованого отримання інформації (ЗНОІ) і методи їх нейтралізації стають особливо актуальними на сучасному етапі розвитку.

Аналіз останніх досліджень і публікацій. Питанням пошуку і локалізації радіоканалів ЗНОІ присвячено значну кількість публікацій.

Так, у [2] розглядаються питання пошуку та локалізації радіозакладок «класичним» методом за

допомогою універсальних приладів, індикаторів поля та інше. Ця методика задовольняла потреби пошуку ЗНОІ раніше. Приладами які викладені в цій методиці виявити і локалізувати ЗНОІ які працюють в цифровому діапазоні дуже і дуже важко. Тому потрібно удосконалювати методику та використовувати другу пошукову технику.

У [3] розглянуто тенденції розвитку радіозакладок, технічні розробки стають все більш досконалими, алгоритми передачі інформації дозволяють створювати стійкі, які не піддаються перешкодам канали зв'язку на набагато більш високих частотах, ніж раніше. Умови розповсюдження радіохвиль не виглядають настільки великою перешкодою. Радіорелейні станції, наприклад, використовують діапазон, близький до сотні ГГц, а в діапазоні 5 ГГц організований широкосмуговий доступ з гігагерцевим трафіком. Виходячи з цього пошукові засоби, що працюють в діапазоні до 3 ГГц, вже не задовольняють сучасним потребам та потребують удосконалення або заміни.

У [4] Розглядається частотний діапазон Wi-Fi якій застосовується в різних бездротових системах на всіх видах транспорту і громадських мережах інтернет доступу. Практично всі бездротові відеокамери та реєстратори швидкості, встановлені на автомагістралях, використовують Wi-Fi технологію. Слід підкреслити, що частотний діапазон Wi-Fi стандарту 802.11 ac (5 ГГц) є найкращим для організації промислових локальних мереж при наявності перешкод високого рівня. Доведено, що «класичним» методом пошуку цей частотний діапазон проаналізувати неможливо. Тобто для пошуку ЗНОІ, потрібні інші методи. Розглянута методика виявлення радіозакладок, що працюють в діапазоні роботи Wi-Fi. Але вона використовується окремо і входить до складу пошукового комплексу тільки опціонально і навіть ця опція не дозволяє локалізувати такого виду радіозакладки.

У [5] аналізується складність сучасного радіомоніторингу в інтересах забезпечення захисту інформації. Проблема полягає в тому, що сучасні цифрові закладні пристрої з передачею інформації по радіоканалу все частіше використовують для передачі інформації ті ж стандарти, що і легальні пристрої. Тому колишні «класичні» методи радіомоніторингу не в змозі визначити заставні пристрої, що працюють під прикриттям легально діючих пристроїв. Що підштовхує до розробки нових пошукових пристроїв та методики пошуку ЗНОІ які працюють у легальних частотних діапазонах. Перераховані вище фактори дозволяють зробити висновок, що на сучасному етапі розвитку суспільства процес пошуку ЗНОІ виходить якісно на інший рівень. Тому методи пошуку та обладнання, які використовуються для цього потребує удосконалення, а проблема аналізу засобів пошуку цифрових радіозакладок з метою виявлення тенденції розвитку та розробки сучасних вимог до них є дуже актуальною.

Метою статті є обгрунтування набору вимог щодо проектування та створення сучасних автоматизованих пошукових комплексів, які відповідають процесу сучасного автоматизованого пошуку цифрових радіозакладок

Виклад основного матеріалу дослідження

На сучасному етапі розвитку суспільства, пошук цифрових радіоканалів ЗНОІ ускладняються декількома факторами.Розробники цифрових ЗНОІ застосовують все більш заплутані алгоритми приховування випромінювання цифрових радіозакладок. Далі на етапі установки цифрових ЗНОІ застосовуються спеціальні методи маскування, створюється канал знімання інформації під прикриттям випромінювання працюючих поблизу об'єкта легальних радіозасобів, що заважають роботі пошукової техніки.

Наступним важливим фактором, є продовження застосування частот радіоефіру для організації зв'язку, передачі даних, різних команд управління. Зараз практично весь радіочастотний діапазон залучений під роботу легальних радіопередавачів. Це викликає ускладнення радіо ефірної обстановки, особливо в великих містах.

Виходячи з вищевикладеного можливо зробити висновок що розробники сучасних ЗНОІ з передачею інформації по радіоканалу переходять на цифрові стандарти дуже близьких до легальних або в легальному діапазоні радіоефіру.

На прикладі типового об'єкта, де проводяться перевірки на наявність засобів негласного знімання інформації, можливо проаналізувати завантаження частотного діапазону та в цілому наявність різного роду каналів витоку інформації, так на типовому об'єкті знаходяться сотні різних комп'ютерів, бездротових цифрових телефонних абонентів, мобільних телефонів різних стандартів (тільки в Києві їх п'ять: CDMA-2000, GSM-900 / 1800,3G (UMTS), 4G (WiMax)), велика кількість різних підсилювачів мобільного та аналогового зв'язку, бездротові гарнітури, різні пристрої Wi-Fi, електронні зчитувачі систем контролю і управління доступом, охоронні відеокамери, які мають побічні електромагнітні випромінювання (ПЕМВ),на рівні або спів мірні з випромінюванням цифрових радіозакладок) і т.п. З урахуванням того що крім цього, на об'єкті наводиться або точніше знаходяться радіосигнали які реально призначені для роботи поза об'єктом, це-всі авіаційні переговори, радіотелефони сусідніх приміщень, радіоаматорський зв'язок, відомчі канали зв'язку оперативних працівників, причому ці радіосигнали все активніше йдуть в цифрові стандарти. Всі ці

сигнали можливо прийняти, перебуваючи на об'єктах. Наприклад, в Києві в діапазоні до 3ГГц, в залежності від району та умов прийому, можливо виявити більше ніж 3500 радіосигналів. Проводячи скорочений аналіз засобів пошуку ЗНОІ, наведених в сучасній літературі, а також використовуючи дані пошукових засобів, які наведені в табл.1.

Таблиця 1.

Частотний діапазон засобів пошуку ЗНОІ

Засоби пошуку ЗНОІ	Основний діапазон пошуку	Наявність приладу, для збільшення діапазону частоті
Детектори поля		
NR-D	50-3500 МГц	
ST-110	50-2500 МГц	антенна-перетворювач до 7 ГГц
SEL SP-75 Black Hunter	100-3000 МГц	
Універсальні пошукові пристрої		
ST-033 "Пиранья"	30 кГц -2500 МГц	ST 03.SHF до 10 ГГц
ST-131 "Пиранья-2"	30 кГц -4100 МГц	ST 131.SHF до 18 ГГц
СРМ-700	200 Гц - 3 ГГц	ВМР-1200 до 12 ГГц
Скануючи приймачі		
AOR 8200	30 кГц -3000 МГц	
Скорпион-XL	30 кГц -2500 МГц	
Контур	30 кГц -2500 МГц	
Апаратно програмні комплексі радіомоніторингу		
"Кассандра-М"	24кГц-3000 МГц	СВЧ-конвертер до 18 ГГц
ОМЕГА	25кГц-3000 МГц	ОМЕГА-К18 до 18 ГГц
OSC-5000	10 кГц - 3 ГГц	MDC-2100 до 21 ГГц
КРОНА	30кГц-3000 МГц	СВЧ-конвертер до 18 ГГц
RS digital Mobile	50кГц-2000 МГц	СВЧ-конвертер RS/DC до 12 ГГц
Delta 2000/6 Real-time	40кГц-6000 МГц	

Можливо зробити висновок про те, що основні їх технічні характеристики, а саме частотні діапазони роботи наявних пошукових засобів - СВЧ (30-300 МГц) плюс УВЧ (300-3000 МГц), не дозволяють ім в повній мірі робить аналіз радіоефіру, особливо стосовно завдань пошуку цифрових радіозакладок. Це доводить що частотний діапазон вже вийшов за рамки аналогових радіосигналів і вже актуальним є створення пошукової техніки саме цифрового частотного діапазону. Сучасна тенденція розвитку техніки доводить, що діапазон її роботи переміщується у цифровий діапазон.

Для визначення вимог до автоматизованих пошукових комплексів ЗНОІ, коротко розглянемо можливі методи приховування роботи цифрових радіозакладок, що застосовуються розробниками таких ЗНОІ. У даний час значно легше виготовити цифровий радіопередавач, використовуючи сучасну радіоелектронну базу стандартних засобів виготовлення засобів зв'язку, ніж конструювати і налагоджувати радіозакладки на транзисторі з позитивним зворотним зв'язком. Тому сучасні і перспективні вимоги до автоматизованих комплексів пошуку ЗНОІ випливають з аналізу можливостей сучасних цифрових засобів передачі даних. Розглянемо де які з них, спираючись безпосередньо на використання розробниками методів приховування роботи цифрових радіозакладок так і методів приховування самих каналів передачі даних.

Сучасні цифрові радіозакладки використовують такі методи приховування своєї роботи і роботи каналів передачі перехоплених даних:

- метод накопичення отриманої інформації з дискретної її передачею за короткий час, в залежності від ступеня стиснення інформації (цей час може становити кілька мілісекунд).
- наступний метод є продовженням вищевикладеного, але виведений в окремий ряд з огляду на те що накопичення інформації відбувається тривалий час і передається виключно в призначений час або при отриманні зовнішньої команди оператора;
- метод, точніше спосіб, періодичної або хаотичної перебудови частоти каналу радіовипромінювання;
- використання широкосмугових сигналів, метод, коли спектр сигналу розподілений у широкій смузі частот та сигнал не має яскраво вираженого піка перевищення над шумами;
- реалізація так званих «шумоподібних» радіозакладок, які використовують спеціальні алгоритми кодування, що дозволяють приймати інформацію при негативному відношенні сигнал / шум саме в точці знаходження приймача;
- дуже складний для визначення метод приховування вибором частоти випромінювання поряд з потужними джерелами легальних сигналів, які перевантажують прийомні тракти пошукової апаратури при недостатньому динамічному діапазоні або маскуються спектром легального сигналу при недостатньо низьких фазових шумах радіо трактів пошукових комплексів;
- маскують цифрові радіозакладки і під стандартні канали зв'язку, маючи у своєму розпорядженні частоту радіозакладки в безпосередній близькості від легального джерела або ж використовуючи вузько смугове

випромінювання всередині спектра легальних широкосмугових сигналів;

- втручаються, саме втручаються, а не намагаються перехопити і дешифрувати інформацію стандартних каналів зв'язку таких як GSM, CDMA, Wi-Fi.

Використовувані методи та засоби можуть успішно комбінуватися один з одним. Так, наприклад, можливе використання радіозакладки з накопиченням інформації та передачею цієї інформації в вузько направленому сигналі легального діапазону радіочастот. Радіозакладки, що використовують методи накопичення інформації з наступною її передачею в короткий проміжок часу з перебудовою радіочастоти випромінювання та дистанційним управлінням, надійно можна ідентифікувати тільки за двома демаскирующими ознаками, перша ознака побічне електромагнітне випромінювання (ПЕМВ)(дуже складно виявити через дуже низької величини сигналу) та друга ознака визначення перевищення амплітуди на певній частоті та короткий час роботи цифрової радіозакладки. Додатково хотілося відзначити що які б складні алгоритми, методи і засоби приховування каналу передачі даних не застосовувалися в цифрових радіозакладками, вони все одно себе демаскують, виходячи з певної закономірності, наприклад, періодичністю виходу в радіоефір. Ці демаскуючі ознаки радіозакладок визначаються в основному, оператором пошукового комплексу при виконанні аналізу радіочастотного спектра. Саме амплітудно-частотної-часової закономірністю цифрові радіозакладки відрізняються від випадкових сплесків побічного шуму в радіоефірі, який недосвідчений оператор може прийняти за радіозакладками. Очевидно при пошуку таких цифрових радіозакладок ми можемо говорити про їх миттєвому виявленні тільки по побічному електромагнітному випромінюванню. Але як зазначалося вище це дуже складний і трудомісткий процес виходячи з чого в цій статті ми його ретельно не розглядаємо. Для надійного ж виявлення описаних вище радіозакладок необхідний радіомоніторинг протягом тривалого часу (для накопичення статистики) від доби і більше з подальшим ретельним аналізом всіх виміряних і виявлених радіосигналів в поданні спектрограми так званої спектрограми - «водоспаду». Виходячи з вищевикладеного, випливають додаткові вимоги до алгоритмів та методів, які повинні бути реалізовані у програмному забезпеченні автоматизованого пошукового комплексу.

Щодо виявлення наступного ряду прихованих радіозакладок – над широкосмугових і шумоподібних закладок, слід зазначити наступне: метод їх виявлення заснований на тому, що в ближній зоні відношення сигнал / шум буде вище нуля, тому збільшення рівня шуму в окремих діапазонах частот може свідчити про роботу таких радіопристроїв. Виходячи з цього можна сформулювати наступні вимоги до засобів автоматизованих програмних комплексів радіомоніторингу- для того, щоб відслідковувати зміну рівня шуму на тлі сильних легальних радіосигналів приймає сигнал пристрій повинен мати хорошу чутливість і широкий динамічний діапазон (не менше 80-90 дБ). Міркування про те, що динамічний діапазон в автоматизованих програмних комплексах радіомоніторингу не так важливий, зважаючи на то що радіозакладки в ближній зоні мають досить високу потужність сигналу і тому можна використовувати тільки атенюатор, неприйнятний в разі пошуку над широкосмугових і гумоподібних радіосигналів.

На сьогодні досить поширеною є ситуація, коли разом з цифровою радіозакладками в частотному діапазоні працює легальний засіб зв'язку, рівень сигналу якого перевищує рівень закладки на 70-90 дБ. Треба відзначити що уровень70-90 дБ – це дуже високий рівень сигналу, який здатний перевантажити приймальний тракт радіоприймального пристрою АПК. Якщо сигнал перевищує рівень динамічного діапазону приймального тракту, то на панорамі сигналів ми бачимо безліч помилкових побічних радіосигналів, нестабільних по частоті, амплітуді. А також в часі.

Аналіз представлених на ринку автоматизованих програмних комплексів радіомоніторингу, при формальній відповідності параметрів їх динамічного діапазону даними пошуковим вимогам, показав, що їх приймальні пристрої дуже легко перевантажуються від працюючого неподалік простого радіопередавача малої потужності, які продаються у вільному продажу і не потребують ліцензування. Слід зазначити що при наявності великої кількості різноманітних хибних сигналів говорити про надійний пошук закладних пристроїв в такому випадку не доводиться. Звідси випливає наступна вимога до АПК, для пошуку прихованих-закамуфльованих радіозакладок, які маскуються під частотний діапазон легальних радіосигналів і виходять в ефір в вузькополосному діапазоні на короткий період часу, або цифрових радіозакладок які постійно працюють в частотному діапазоні легальних сигналів, автоматизований комплекс радіомоніторингу повинен мати засоби детального дослідження спектрів сигналів з дозволом в одиниці Герц. Однак, досвід оператора та його інтуїція мають дуже важливе значення, але апаратура і програмне забезпечення комплексу повинні дозволити оператору виконувати саме такі завдання.

Наступне завдання які не вирішується традиційним методом радіомоніторингу це пошук закладних цифрових радіопристроїв, що використовують стандартні канали зв'язку, такі як

DECT, GSM, CDMA, Wi-Fi, BlueTooth, крім радіомоніторингу роботи цих пристроїв класичним методом-методом аналізу відповідних частотних діапазонів, автоматизований комплекс радіомоніторингу повинен мати засоби додаткового аналізу мереж, що дозволяють виявляти MAC адреси для локальних комп'ютерних мереж, визначати все MAC адреси і робити аналіз визначаючи MAC адреса які не належать до даної мережі-вказувати їх розташування тобто ідентифікувати сторонні пристрої. Якщо процес локалізації MAC адресу невідомого пристрою АПК скрутний необхідно мати додаткові пристрої або прилади, що дозволяють локалізувати цей пристрій. Аналогічно це стосується і мереж абонентської телефонного зв'язку DECT, тільки там ідентифікатором буде виступати не MAC адреса, а унікальну адресу RFPI.

Необхідно констатувати, що окремих універсальних приладів аналізу цифрових пакетів, щодо завдання пошуку і локалізації цифрових ЗНОІ зараз практично немає. Перша спроба створення програмних засобів (ПЗ) по демодуляції та аналізу цифрових засобів радіозв'язку можна вважати пакет цифрової обробки сигналів в програмному забезпеченні ПЗ DigiScan і в ПЗ «РадіоІнспекторСофт ТМ». ПЗ «РадіоІнспекторСофтТМ» знайшов своє подальше застосування в АПК «Кассандра», Пошуковий програмний автоматизований комплекс «Кассандра» з ПЗ RadioInspector надає оператору такі можливості: сталий довгостроковий контроль заданого частотного діапазону, збір, зберігання і відображення даних про стан радіочастотного спектру за весь час вимірювань (спектрограма або "водоспад"), використовувати базу даних частот - відображаю їх легальні сигнали на даному об'єкті, встановлювати лінію порога після перевищення якого радіосигнал записується в базу, записувати аудіо сигнал і демодулирувати цей аудіо сигнал, формувати завдання на запис демодульованого аудіо сигналу при перевищенні лінії порога. Управляти другим сканирующим приймачем як засобом аудіо контролю без зупинки сканування основним приймачем (настройка на частоту, прослуховування та запис демодульованого аудіо сигналу без зупинки сканування). Тобто другий приймач виконує класичну задачу пошуку цифрових радіозакладок. Можливість управління скануючим приймачем по мережі LAN, передача демодульованого аудіосигналу мережею у реальному масштабі часу. Контролювати всім пристрої бездротового зв'язку Wi-Fi по їх MAC адресами, моніторинг за пристроями Wi-Fi мереж діапазонів IEEE 802.11. до 5 ГГц з можливістю автономного, цілодобового збору інформації з подальшою передачею накопиченої інформації по мережі LAN. Робота в реальному масштабі часу. Аналізувати сигнали DECT по RFPI,GSM, Bluetooth, TETRA, IEEE 802.15.4 (ZigBee) UMTS (3G). Зовнішній вигляд апаратно пошукового комплексу «Кассандра» наведено на рис1.

Рис.1.Зовнішній вид пошукового АПК Кассандра з ВО «РадіоІнспекторСофт ТМ»

Як бачимо з наведеного вище опису комплекс з ПЗ «РадіоІнспекторСофт ТМ» дозволяє виконувати практично всі завдання пошуку цифрових радіозакладок, однак недоліком цього комплексу і ПЗ та його модульність яка не дозволяє виконувати пошук відразу в повному обсязі, необхідно опціональне докуповувати додаткові модулі такі як RadioInspectorWI-FI, Dtest (DigitalTest) та виконувати додаткові перемикання, оператору необхідно працювати в різних програмних середовищах, різних інтерфейсах-відсутнє так зване «єдине вікно» пошуку цифрових радіозакладок. Цього недоліку позбавлений АПК DeltaX, який є продовженням АПК з ПЗ DigiScan. Розробник удосконалив ПЗ DigiScan, доповнив його можливістю аналізувати сигнали, які працюють в частотних стандартах DECT, GSM, Bluetooth, Wi-Fi, виконувати демодуляцію і відображення відео аналогового телевізійного сигналу, в тому числі, з використанням методу інверсії синхроімпульсів, демодулировать аналогові AM і FM сигнали в смузі частот від десятків герц до декількох мегагерц. Розробник спробував виконати всі вищевикладені нами вимоги в повному обсязі вдосконалити комплекс. Результатом цих удосконалень став апаратно програмний комплекс з ПЗ «Delta2000 / 6Real-timeXAdvanced». [6] Зовнішній вигляд комплексу представлений на рис 2.

Рис.2. Зовнішній вид пошукового АПК з ПЗ «Delta 2000 / 6Real-timeXAdvanced»

На сьогодні автоматизованого пошуковий комплекс на базі ПО DeltaX, це самий передовий автоматизований програмний комплекс, він дозволяє виявляти і в більшості випадків локалізувати цифрові радіозакладки, демодулировать, аналізувати, ідентифікувати і визначати місця розташування базових станції як WI-FI, так і DECT, різні мобільні пристрої. Цей АПК дуже щільно наблизився до універсального навіть до оптимального, проте це ПЗ не використовує для пошуку векторний аналіз, в повному обсязі. Тобто не приділено належної уваги векторному аналізу і автоматичної пеленгації цифрових радізакладок.

Аналіз був би не повний їли не розглянути програмний комплекс АКОР.

Другим поколінням АПК АКОР став програмний комплекс АКОР-2ПК, АКОР-2ПК (рис. 3), це друге покоління універсальних професійних пошуково-вимірювальних комплексів призначених для пошуку і локалізації ЗНОІ, для цього комплексу характерні наступні особливості:

комплекс використовує в якості повної обробки радіосигналів тобто в якості обчислювача сучасні ПК, що дозволяє удосконалювати програмне забезпечення комплексу і розширювати його функціональні можливості по радіомоніторингу незалежно від джерела вхідного сигналу, наступною особливістю вважаю за необхідне зазначити – виявлення малопотужних цифрових пристроїв, виявлення технічних каналів витоку інформації від всіх електронних пристроїв і приладів по побічним електромагнітним випромінювання (ПЕМВ), наявність звукового корелятора для виявлення побічної модуляції ПЕМВ аудіосигналом сигналом;

наявність набору фільтрів з шириною смуги до1Гц, дозволяє вимірювати сигнали, що лежать нижче рівня шумів; універсальність, так як поєднує в собі функції двох комплексів: пошукового-для радіомоніторингу і пошуку радіо заставних пристроїв і вимірювального-для виявлення і вимірювання ПЕМВ.

Рис.3. Зовнішній вид пошукового АПК АКОР-2ПК

Це єдиний на сьогоднішній день комплекс дозволяє проводити такі види робіт, простота управління і перемикання з пошукового режиму роботи комплексу вимірювальний і назад. Цей АПК перевершує вищеописані комплекси по виявленню технічних каналів витоку інформації по ПЕМВ, однак поступається їм по спектральному аналізу та локалізації цифрових радіозакладок.

Виходячи з вищевикладеного, можна сформулювати вимоги до сучасного і перспективного автоматизованого програмного комплексу радіомоніторингу:

1. Сучасний комплекс АПК повинен володіти високочутливими каналами аналогової і цифрової обробки сигналу, щоб присутність потужних сторонніх сигналів-шумів не заважало йому виявляти і перевіряти широкосмугові і шумоподібні радіосигнали. У тактико-технічних характеристиках радіоприймальних пристроїв – це характеристики чутливості і динамічний діапазон. Зрозуміло, що з розвитком технологій вимірювальної техніки дані характеристики будуть тільки поліпшуватися. Будемо приймати на сьогоднішній день за точку відліку характеристики сучасних вимірювальних пристроїв з чутливістю - не менше -160дБт (1 Гц) і динамічним діапазоном не менше 85 дБ на частоті 1 ГГц.

2.Комплекс, що задовольняє сучасним вимогам по пошуку і локалізації цифрових ЗНОІ повинен мати високоякісне і багатофункціональне програмне забезпечення, яке повинно мати по можливості один інтерфейс для всіх модулів ПО і має дозволяти, виконувати наступні функції:

виконувати цілодобовий радіомоніторинг заданих діапазонів частот і зберігати всі результати вимірювань для подальшого їх аналізу;

забезпечувати аналіз амплітуди, частоти і тривалості цифрових радіосигналів і результатів радіомоніторингу в режимі реального часу і в режимі аналізу бази накопичених радіосигналів;

дозволяє виконувати детальний аналіз спектрів сигналів з дозволом в одиниці Герц;

додаткової досліджувати випромінювання стандартних, відкритих каналів зв'язку Wi-Fi на MAC адрес котрі належать до даної мережі, а також і ідентифікаторів абонентських телефонних станцій даного об'єкта;

виконувати аналіз сигналів по векторний діаграмі-векторний аналіз в повному обсязі;

здійснювати пеленгацію невідомих джерел радіосигналів.

При цьому однозначно не можна забувати, що програмне забезпечення має підтримувати методи пошуку, що стали вже «класичними» і широко використовуваними усіма пошуковими системами на практиці:

метод рознесених антен-для порівняння сигналів і локалізації радіозакладок;

метод порівняння з файлом зразка-для скорочення часу перевірки та виявлення сигналів, що перевищують по амплітуді сигнал від файлу зразка;

використання виборної лінії порога і формування переліку сигналів, які перевищили лінію порога-зі збереженням сигналу в базі для подальшого аналізу;

детальний аналіз характеристик спектрів прийнятих сигналів до 6 ГГц;

автоматичний запис модульованого аудіо радіосигналу. Функціональні можливості, ергономічні характеристики і розробка програмного забезпечення всіх комплексів пошуку ЗНОІ є найбільш актуальними на сьогодні, тому що, безумовно, пошук сучасних радіо закладок – це інтелектуальна боротьба розробника таких засобів і оператора, що виконує пошук закладок. Програмне забезпечення – це інструмент пошукача, і від того, наскільки воно функціонально і зручно, в чималому ступені визначає результат робіт по виявленню, локалізації та блокування засобів негласного знімання інформації.

Висновки й перспективи подальших досліджень

1. Проведено аналіз універсальних приладів і програмних комплексів пошуку засобів негласного отримання інформації, який показав відсутність на ринку автоматизованих програмних комплексів, комплексів які дозволяють вирішувати завдання автоматизованого пошуку цифрових радіозакладок в повному обсязі, в усіх частотних діапазонах.

2. Враховано особливості сучасних розробок засобів негласного отримання інформації, надано повний методичній набір вимог що до проектування та створення сучасних автоматизованих пошукових комплексів які відповідають процесу сучасного автоматизованого пошуку цифрових радіозакладок в повному обсязі. Дані вимоги можуть використовуватися як технічне завдання при проектуванні автоматизованих програмних комплексів пошуку цифрових радіозакладок. Подальші дослідження доцільно спрямувати на удосконалення ПО для АПК, вивчення позитивних сторін і поліпшення методики їх використання.

Література

1. Хорев А.А.Техническая защита информации: учебное пособие для студентов вузов. В 3 т. Т. 1./ Технические каналы утечки информации. - М: «НПЦ Аналитика», 2008. - 436 с. **2.Ананский Е.В.** Что такое радиозакладки и как их обнаружить? (часть2)/журнал «Служба безопасности» [Электронный ресурс] режим доступ: http://www.kvirin.com/articles/267/ **3. А.В.Кривцун** Использование новых возможностей комплекса радиомониторинга и цифрового анализа сигналов «Кассандра-М» для обнаружения современных специальных технических средств с передачей информации по радиоканалу [Электронный ресурс] /А.В. Кривцун А.В.Захаров режим доступа: http://www.inspectorsoft.ru/article.php?id=388 (24.05.2019) **4. Захаров А.В.** Требования к перспективному анализатору сетей Wi-Fi [Електронний ресурс] - Режим доступу: http://www.analitika.info/stati3.php (25.05.2019). **5. Власов А.** Беспроводные офисная связь: DECT и Wi-Fi. [Электронный ресурс]. — Режим доступа: http://www.dect.ru/dect.html (05.05.2016) **6.** Поисковые комплексы . [Электронный ресурс]. https://www.das-ua.com/documents/catalog/search-appliances/search-complexes/page-01.php (03.05.2019)

АНАЛИЗ И ТЕНДЕНЦИИ РАЗВИТИЯ СПОСОБОВ ПОИСКА ЦИФРОВЫХ РАДИОЗАКЛАДОК

***Александр Анатольевич Лаптев** (кандидат технических наук, с. н. с.)[1]*
***Роман Иванович Грозовский**[2]*

[1]Государственный университет телекоммуникаций.Киев,Украина
[2]Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье рассмотрен вопрос утечки или утраты информации, что может повлечь за собой материальный ущерб или привести к катастрофическим последствиям в управление - производством, транспорте и военном деле. Современная военная наука утверждает, что полное лишение средств связи сводит боеспособность армии к нулю. Нами проведен анализ различных по принципу работы, поисковых приборов, и методов поиска средств негласного съема информации. Проведенный анализ позволяет сделать вывод, что на современном этапе развития общества процесс поиска средств негласного съема информации выходит качественно на другой уровень. Поэтому методы поиска и оборудование используемые для этого требуют усовершенствования, а проблема анализа средств поиска цифровых радиозакладок с целью выявления тенденции развития и разработки современных требований к ним становится очень актуальной. Рассмотрены методы сокрытия работы радиозакладок, применяемые при разработке цифровіх радиозакладок. Отмечено, что в настоящее время гораздо легче сделать цифровой передатчик, используя современную элементную базу стандартных средств связи, чем конструировать и налаживать «аналоговую» закладку на транзисторе с положительной обратной связью. Поэтому современные и перспективные технологии качественно влияют на возможности изготовления современных средств негласного съема информации. Современные радиозакладки могут использовать различные методы сокрытия канала передачи данных, что очень усложняет процесс их поиска. Особенно если они используют комбинированные методы сокрытия канала передачи данных.

Учитывая особенности современных разработок средств негласного съема информации, нами предоставлен полный методической набор требований к проектированию и созданию современных автоматизированных поисковых комплексов. Комплексов которые удовлетворяют современному уровню автоматизированного поиска цифровых радиозакладок в полном объеме. Данные требования могут использоваться как техническое задание при проектировании автоматизированных программных комплексов поиска цифровых радиозакладок.

***Ключевые слова**: радиозакладка, поиск, радиоканал, радиомониторинг, автоматизированный программный комплекс.*

ANALYSIS AND TREND IN THE DEVELOPMENT OF DIGITAL RADIO TAG SEARCH TOOL

***Alexander Laptev** (Candidate of Technical Sciences, Senior researcher)* [1]
Roman Hrozovskyi [2]

[1]*State University of Telecommunications. Kyiv, Ukraine*
[2]*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

The article deals with issues of leakage or loss of information that could cause material damage or could lead to catastrophic consequences in the object of management - production, transport and military affairs. Modern military science argues that the total deprivation of communications reduces the combat capability of the army to zero. The analysis of various on the principle of work, search engines, and methods of searching for tacit information. The analysis allows us to conclude that at the present stage of the development of society, the process of seeking the means of secret information obtains qualitatively to another level. Therefore, the search methods and equipment used for this need improvement, and the problem of analyzing digital radio tag search tools in order to identify trends in the development and development of modern requirements for them will become relevant. The methods of hiding the work of radio tabs that are used in the development of radio tabs are considered. It is noted that at present it is much easier to make a digital transmitter using a modern elemental base of standard communication devices than to construct and debug an "analog" bookmark on a positive feedback transistor. Therefore, modern and promising technologies stem from the possibility of modern means of secretly obtaining information. Modern radio tabs can use different methods of concealing the data transmission channel, which greatly complicates the process of their search. Especially as they use combined methods of concealing the data transmission channel.

Taking into account the peculiarities of modern developments of secret means of obtaining information, a complete methodical set of requirements for the design and creation of modern automated search systems that meet the process of modern automated search of digital radio bookmarks in full is provided. These requirements can be used as a technical task when designing automated software solutions for digital radio tabs.

***Keywords:** radio tab, search, radio channel, radio monitoring, automated software complex.*

References

1. Horev A.A. Technicheskaya protection of information: a manual for students of high schools. In 3 t. T. 1. / Technical channels of leakage of information. - M: "NPC Analyst", 2008. - 436 pp. 2**.Anansky E.V.**chto such radio tabs and how to find them? (part2) / Journal "Security Service" [Electronic resource] access mode: http://www.kvirin.com/articles/267/. **3. AV Krivtsun** The use of new possibilities of the radio monitoring and digital analysis complex of "Kassandra-M" signals for the detection of modern special technical means with the transmission of information over the radio channel [Electron resource] /A.V. Krivtsun AV Zakharov access mode: http://www.inspectorsoft.ru/article.php?id=388 (05/22/2019) **4. Zakharov AV** Requirements for a prospective analyzer of Wi-Fi networks [Electronic resource] - Access mode: http://www.analitika.info/stati3.php?page=1&full=block_article241 (25.05.2019). **5. Vlasov A.** Wireless office communication: DECT and Wi-Fi. [Electronic resource]. - Access mode: http://www.dect.ru/dect.html (05.05.2016)
6. Search complexes. [Electronic resource]. https://www.das-ua.com/documents/catalog/search-appliances/search-complexes/page-01.php (05.03.2019).