УДК 537.871.62

І.М. Коротєєв

ПЕРВИННІ ЗАХОДИ З ПОШУКУ ПРИСТРОЇВ ВИТОКУ ІНФОРМАЦІЇ[1]

У статті розглянуто основні заходи, які доцільно виконати перед початком проведення пошукових заходів з виявлення пристроїв витоку інформації.

Ключові слова: *технічні канали витоку інформації, негласний виток інформації, супротивник.*

В статье рассмотрены основные мероприятия, какие целесообразно выполнить перед началом проведения поисковых мероприятий по выявлению устройств утечки информации.

Ключевые слова: *технические каналы утечки информации, негласная утечка информации, противник.*

The article describes the main activities, which it is advisable to perform before the start of the search activities of the identification leak devices.

Keywords: *technical channels of information leakage, confidential data leakage, opponent.*

1.5. Вибір апаратури для проведення перевірки, розподіл сил і засобів.

Важливим елементом підготовки до перевірки приміщень є вибір технічних засобів, які забезпечують проведення планованих пошукових і дослідницьких робіт. До мінімального переліку апаратури, необхідної для перевірки приміщень на наявність джерел НВІ, повинні входити:

- засоби, що забезпечують ефективність візуального огляду елементів конструкції приміщення, предметів інтер'єру і важкодоступних місць;
- прилади для перевірки провідних комунікацій;
- апаратура для виявлення радіовипромінювальних засобів НВІ.

При проведенні комплексних спеціальних перевірок приміщень цей перелік зазвичай доповнюється металошукачем, приладом нелінійної радіолокації та переносним рентгенівським комплексом.

У випадках, коли попередній огляд виявив необхідність проведення спеціальних досліджень з метою виявлення й оцінки потенційних ТКВІ, за погодженням з керівництвом організації до переліку необхідного обладнання включається апаратура для проведення акустичних і віброакустичних вимірів, дослідження побічних електромагнітних випромінювань і ін. необхідні прилади.

Доцільно поєднувати проведення спеціальних перевірок з контролем радіаційного фону у приміщеннях. З цією метою у пошуковій бригаді необхідно мати дозиметр або індикатор радіоактивного випромінювання.

Для кожного з обраних типів приладів заздалегідь повинні бути прораховано необхідність та доцільність додаткових заходів щодо активації впроваджених джерел НВІ. У деяких випадках, навпаки, може знадобитися введення обмежень на функціонування або навіть розміщення будь-яких засобів на час роботи з обраним типом пошукової або дослідницької апаратури.

[1] Закінчення. Початок у № 4, 2012.

Це пов'язано з тим, що пошук інформативних сигналів у лініях силової та освітлювальної мережі вимагає попереднє вмикання (активації) всіх наявних у приміщенні споживачів електроенергії, а пошук інформативних ПЕМВ ПЕОМ, навпаки – вимкнення. Застосування приладу нелінійної радіолокації для перевірки елементів будівельних конструкцій вимагає попереднього видалення із зони дії бічних пелюсток його антени, обладнання та предметів, що містять радіоелектронні компоненти, у т.ч., ін. пошукової та дослідницької апаратури. У деяких випадках при перевірці невеликих за обсягом серверних або ін. приміщень зі стаціонарно встановленим радіоелектронним обладнанням, ефективне застосування нелінійного локатору може взагалі виявитися неможливим.

Комплексна спеціальна перевірка приміщень, зазвичай, проводиться в умовах гострого дефіциту часу, відведеного на пошукові та дослідницькі роботи. Легенда прикриття пошукових робіт та заходи щодо активації впроваджених джерел НВІ не можуть бути ефективними в продовж тривалого часу. У зв'язку з цим однією з проблем підготовчого етапу є правильний розподіл наявних сил та засобів з об'єктів перевірки за видами робіт. Під силами, у даному випадку, слід розуміти кількість фахівців, яких включають до складу пошукової бригади. Очевидно, що чим більше буде склад бригади, тим менше часу може зайняти безпосереднє проведення перевірки. Разом з тим, непомірне розширення складу пошукової бригади недоцільно з конспіративних міркувань. Тому чисельний склад пошукової бригади повинен визначатися з урахуванням усіх факторів.

Вимушена (через дефіцит часу) необхідність паралельного ведення різних робіт в тих самих приміщеннях призводить до того, що частина досліджень доведеться виконувати в умовах обмежень, накладених ін. роботами. Слід заздалегідь продумати вплив зазначених обмежень на порядок роботи з апаратурою та приладами. У ряді випадків доведеться внести коригування до (конкретних) методик застосування приладів. Обрана легенда прикриття та необхідність прихованого проведення робіт також можуть змусити змінити звичайний порядок дій з деякими видами пошукової техніки.

Відомо, наприклад, що пошук радіовипромінювальних або пристроїв НВІ встановлених на проводові комунікації, помітно спрощується та прискорюється при використанні системи акустичного зворотного зв'язку, наявної в багатьох пошукових приладах. У той же час, характерний звук роботи цієї системи дозволяє супротивнику легко встановити факт виявлення впровадженого ним пристрою. З цієї причини необхідно заздалегідь відмовитися від застосування системи акустичного зворотного зв'язку, незважаючи на те, що це викличе деяке збільшення тривалості пошукових робіт.

Правильний розподіл сил і засобів неможливо без попередньої оцінки витрат часу, необхідних для виконання кожної із запланованих робіт. Очікувані витрати часу можуть бути визначені методом експертних оцінок фахівцями пошукової бригади з урахуванням накопиченого досвіду роботи в ході аналогічних перевірок, обсягу та інших характеристик приміщень, запланованих для проведення перевірки.

Розподіл наявних сил та засобів з об'єктів перевірки та видами робіт повинно проводитися з метою максимального скорочення загального часу їх проведення. Для оптимізації такого розподілу доцільно скористатися відомою методикою мережевого планування робіт. Ретельно продуманий мережевий графік дозволить узгодити в рамках єдиної структури процес проведення всіх необхідних пошукових і дослідницьких робіт з урахуванням їх обсягу та спільних обмежень.

Враховуючи викладене вище можливий наступний порядок дій:

• Визначаються орієнтовні витрати часу для виконання кожної із запланованих робіт, в тому числі, очікувана тривалість дій з кожним із видів пошукової та дослідницької апаратури.

• Серед робіт визначаються такі, при проведені яких не можливе, одночасне їх проведення через їх взаємний плив або інших міркувань.

• Шляхом додавання визначаються витрати часу, необхідні для послідовного виконання робіт, одночасне проведення яких неможливо.

• Відзначаються витрати часу на найбільш трудомістку з числа робіт, що залишилися.

• Визначається мінімально можлива тривалість безпосереднього проведення спеціальної перевірки, як найбільша за витратою часу, визначених у двох попередніх пунктах.

• В межах мінімально можливої тривалості безпосереднього проведення спеціальної перевірки розподіляються всі заплановані роботи таким чином, щоб мінімізувати кількість одночасно (паралельно) виконуваних робіт.

Отримане в результаті цих маніпуляцій найбільше число робіт, що паралельно виконуються, вкаже на мінімально необхідний кількісний склад пошукової бригади, який забезпечить проведення спеціальної перевірки приміщень за мінімально можливий час.

1.6. Складання плану проведення спеціальної перевірки.

План проведення комплексної спеціальної перевірки приміщень є головним документом, що визначає масштаб, зміст та методику проведення. У випадку, коли всі викладені у попередніх розділах роботи підготовчого етапу ретельно виконані, складання та оформлення цього плану не викликає будь-яких труднощів.

Структура типового плану проведення комплексної спеціальної перевірки приміщень може виглядати наступним чином.

План проведення комплексної спеціальної перевірки приміщень

1. Висновки з оцінки супротивника.

1.1. Задум проведення спеціальної перевірки приміщень:

1.1.1. Мета (мотив) проведення перевірки.

1.1.2. Перелік та стисла характеристика приміщення.

1.1.3. Перелік запланованих пошукових робіт і досліджень.

1.1.4. Час проведення перевірки.

1.1.5. Легенда, під прикриттям якої проводитиметься перевірка.

1.1.6. Заходи щодо активації ймовірних джерел НВІ.

1.1.7. Дії у випадку виявлення джерел НВІ.

2. Сили та засоби, їх розподіл за об'єктами та видами робіт

2.1. Склад пошукової бригади.

2.2. Перелік технічних засобів, які залучаються для проведення перевірки та основні особливості їх застосування, що визначається умовами перевірки.

2.3. Розподіл сил і засобів за об'єктами та видами робіт.

2.4. Додаткові заходи щодо активації ймовірних джерел НВІ.

3. Перелік підготовлених за результатами перевірки підсумкових та звітних документів і термін їх подання для затвердження.

У розділі "Висновки з оцінки супротивника", доцільно вказати:

• категорію осіб, до яких може належати суб'єкт, обраний вірогідним противником для впровадження засобів НВІ та зняття інформації;

• можливий рівень знань, навичок та кваліфікації суб'єкта, що здійснює впровадження засобів НВІ;

• можливі види засобів НВІ, очікувана ступінь відповідності їх характеристик найбільш технологічним зразкам аналогічних засобів;

• можливі способи і час встановлення (впровадження) засобів НВІ та дій щодо отримання інформації;

• ймовірні дії у випадках встановлення намірів провести спеціальну перевірку приміщень, факту проведення такої перевірки та факту виявлення встановлених джерел НВІ.

Переважна більшість даних, які необхідні для включення до розділу плану, вже були отримані на етапі робіт з виявлення ймовірного противника та складання моделі його дій.

У розділ "Задум проведення спеціальної перевірки приміщень" доцільно включити:

• мета (мотив) проведення спеціальної перевірки приміщень;

• оформлений у вигляді таблиці або перелік приміщень (що перевіряються) з короткою характеристикою кожного приміщення: призначення, площа і об'єм, особливості конструкції, основні види обстановки, встановленого обладнання і відсоток займаної ними загальної площі (обсягу) приміщення, види провідних технологічних комунікацій;

• перелік запланованих для кожного приміщення пошукових робіт і супутніх досліджень (включаючи роботи, запланованих до проведення в суміжних приміщеннях і на зовнішніх поверхнях огороджувальних будівельних конструкцій) із зазначенням їх очікуваної трудомісткості;

• час проведення спеціальної перевірки приміщень: дата, початок, кінець і загальна тривалість безпосереднього проведення перевірки;

• зміст і час дії легенди або кількох легенд, під прикриттям яких будуть проводитися роботи з спеціальної перевірці приміщень, способи і початок доведення легенд до персоналу підприємства, перелік обладнання та документів, необхідних для підтвердження легенд;

• заходи з активації ймовірних джерел НВІ, способи та початок їх виконання;

• дії пошукової бригади у разі виявлення джерел НВІ.

Більшість даних, необхідних для розробки цього розділу плану, також було отримано на попередніх етапах підготовчих робіт.

У розділ "Залучені сили та засоби, їх розподіл за об'єктами та видами робіт", необхідно включити:

• кількісний та персональний склад пошукової бригади;

• перелік спеціального обладнання та технічних засобів, що залучаються для проведення спеціальної перевірки приміщень з зазначенням основних особливостей їх застосування в рамках обраних легенд прикриття та інших обмежень, що накладаються умовами перевірки;

• мережевий графік виконання запланованих пошукових та дослідницьких робіт або таблицю розподілу фахівців пошукової бригади, устаткування і технічних засобів за видами робіт та об'єктам спеціальної перевірки;

• текстову частину з викладенням додаткових заходів щодо активізації впроваджених джерел НВІ у процесі застосування конкретних типів пошукової апаратури.

Заключний етап перевірки приміщень повинен містити перелік підготовлених за результатами попередніх етапів перевірки підсумкових та звітних документів і термін їх подання для затвердження. До цього переліку можуть входити акт проведення комплексної спеціальної перевірки приміщень, опис проведених робіт і досліджень, протоколи вимірювань, рекомендації з підвищення надійності захисту інформації від її можливого витоку технічними каналами та інші документи.

Розроблений план затверджується керівником організації. У ряді випадків, особливо в умовах дефіциту часу при необхідності термінового проведення позапланової спеціальної перевірки, за домовленістю з керівником організації може готуватися скорочений варіант плану. Іноді з тієї ж причини і з міркувань конспірації допускається усна форма представлення плану.

1.7. Попередній аналіз радіоелектронної обстановки.

Збір попередніх даних та аналіз радіоелектронної обстановки в районі розташування приміщень не обов'язкова, але вельми бажана фаза підготовчих робіт. Вона дозволяє помітно прискорити подальші роботи з радіомоніторингу приміщень, що перевіряються і підвищити надійність виявлення радіовипромінювань засобів НВІ.

Попередній збір даних та аналіз радіоелектронної обстановки полягає у пошуку та виявленні радіовипромінювань в районі розміщення приміщень, що перевіряються, визначенні джерел (приналежності) виявлених радіовипромінювань та їх попередньої сортування для подальшого спеціального тестування та аналізу на приналежність до джерел НВІ і ПЕМВ засобів оргтехніки з приміщень, що перевіряються. За погодженням з керівництвом організації додатковими завданнями аналізу радіоелектронної обстановки на цьому етапі можуть бути контроль дотримання співробітниками підприємства встановлених його керівництвом обмежень на використання відкритих каналів радіозв'язку, контроль та оцінка ефективності використання технічних засобів захисту інформації та ін. завдання.

Проведення зазначених робіт в умовах звичайного режиму діяльності організації дозволяє скласти карту зайнятості радіоефіру, базу даних виявлених сигналів та виключити з подальшого аналізу відомі радіовипромінювання, істотно скоротивши час, необхідний для проведення радіомоніторингу у процесі безпосередньої перевірки приміщень.

Методика попереднього збору даних радіоелектронної обстановки та їх аналізу багато в чому визначається типами апаратури.

Мінімально необхідний комплект устаткування повинен включати широкодіапазонну антену; радіоприймач сканування або радіоприймач, що можна переналаштувати вручну; аналізатор спектра прийнятих сигналів. Приймач повинен мати безперервний діапазон, і як мінімум, охоплювати області ОВЧ (VHF), УВЧ (UHF) та початок СВЧ (SHF). Робота з таким комплектом апаратури вельми трудомістка, вимагає високої кваліфікації та значного досвіду оператора.

У більшості випадків для ведення радіоконтролю та виявлення радіовипромінювань засобів НВІ застосовуються автоматизовані програмно-апаратні комплекси, виконані на базі ПЕОМ та радіоприймача з можливістю сканування радіоефіру (у кращому випадку використовувати аналізатор спектра). Такий комплекс зазвичай дозволяє в автоматичному режимі зняти (відобразити) панораму завантаження радіодіапазону, з мінімальною участю оператора ідентифікувати прийняті випромінювання з сигналами відомих джерел (наприклад, радіомовних станцій, систем телефонного стільникового або пейджингового зв'язку), провести ручний аналіз

ін. сигналів за їх спектральними та ін. характеристиками, скласти перелік частот ідентифікованих випромінювань і частот "підозрілих" сигналів.

Якщо служба безпеки організації не має власних постів радіомоніторингу, то необхідно з керівником цієї організації узгодити місце й час розгортання тимчасового пункту радіоконтролю, з комплектом необхідної апаратури радіомоніторингу та аналізу. З метою конспірації бажано, щоб це місце знаходилося десь за територією організації, але у безпосередній близькості від запланованих до перевірки приміщень. У якості такого пункту може бути використаний, звичайний легковий автомобіль з розгорнутим у ньому комплексом виявлення засобів радіовипромінювань та радіомоніторингу. У разі появи поблизу організації тимчасового пункту радіоконтролю слід передбачити спеціальну легенду прикриття.

Підсумком діяльності пункту радіоконтролю на цьому етапі робіт повинна бути карта завантаженості радіоефіру в умовах звичайного режиму роботи організації, база даних ідентифікованих радіосигналів, а також база даних підозрілих радіовипромінювань, що потребують додаткового дослідження.

Можливий наступний порядок роботи пункту радіоконтролю:

• за погодженням з керівництвом організації визначається час початку, режим (цілодобовий або періодичний) та тривалість роботи тимчасового пункту радіоконтролю, місце його розгортання, перелік завдань і легенда прикриття роботи;

• відповідно до обсягу та номенклатури завдань визначається склад комплекту апаратури і операторів пункту радіоконтролю;

• з використанням наявних довідкових даних (місцевих радіостанцій, рекламних публікацій та ін. джерел) здійснюється збір та систематизація відомостей про розподіл та зайнятості частот у регіоні й безпосередньо в районі розміщення приміщень(що перевіряються);

• складання діаграми (карти) завантаженості радіоефіру у вигляді частотної осі, на якій зазначаються межі та відомча приналежність окремих ділянок (діапазонів); така нарізка загальної смуги частот на окремі ділянки дозволяє здійснювати послідовний аналіз їх завантаження й полегшує визначення приналежності випромінювань в межах кожної ділянки;

• готується таблиця зайнятості частот з числом рядків, рівним очікуваній кількості частот радіосигналів, і стовпцями, в яких будуть вказані частота випромінювання, приналежність та відмінні особливості сигналів (вид модуляції, займана смуга частот, відносний рівень, регулярність появи, час початку та тривалість передачі та т. п.);

• заповнюється таблиця зайнятості частот відомостями про сигнали відомих джерел радіовипромінювання;

• проводиться необхідна підготовка, бланків та документів для розгортання та роботи тимчасового пункту радіоконтролю;

• в запланований час тимчасовий пункт радіоконтролю розгортається та приступає до роботи;

• за результатами використанням апаратури моніторингу здійснюється послідовний перегляд реальної зайнятості окремих ділянок діапазону з виявленням та аналізом особливостей сигналів для визначення їх приналежності й ідентифікації з відомими джерелами випромінювань; відомості про параметри та особливості кожного випромінювання заносяться в таблицю зайнятості частот;

• частоти сигналів, приналежність яких з'ясувати не вдалося, або які ідентифікуються з сигналами джерел НВІ, заносяться до окремого списку для подальшого спостереження за ними та додаткового аналізу;

• періодично (один–два рази на годину) проводиться повторний перегляд завантаження діапазонів для виявлення й аналізу нових випромінювань;

• в проміжках між повторними переглядами завантаження діапазонів, здійснюється постійний або періодичний контроль занесених до цього списку "підозрілих" частот із записом на апаратурі реєстрації (часу початку та закінчення роботи джерела випромінювання, модуляцію, особливості спектру та ін.);

• після закінчення часу, відведеного для попереднього збору даних та аналізу радіоелектронної обстановки, тимчасовий пункт радіоконтролю згортається;

• у зручному місці, але не на очах співробітників організації, оператори тимчасового пункту радіоконтролю за результатами роботи проводять додатковий аналіз накопичених даних, до оформлюють таблицю зайнятості частот, уточнюють список "підозрілих" частот, обсяг та методику майбутньої роботи в ході безпосереднього проведення спеціальної перевірки приміщень.

Для виявлення можливого зв'язку появи у радіоефірі випромінювань з початком роботи організації доцільно приступати до контролю радіодіапазону за декілька години до початку робочого дня на підприємстві. З цих же міркувань завершувати роботу пункту радіоконтролю доцільно не раніше, як через декілька години після закінчення робочого дня та вибуття керівництва.

Слід мати на увазі, що для виявлення радіовипромінювань засобів НВІ, які здійснюють накопичення інформації та її передачу за розкладом, командою або радіозапитом, необхідний цілодобовий радіомоніторинг радіоелектронної обстановки в районі приміщень, що перевіряються. Організація цілодобового функціонування пункту радіоконтролю вимагає особливих заходів конспірації, ретельної підготовки апаратури та більшої кількості операторів, внаслідок необхідності їх цілодобової роботи. Разом з цим, вказані джерела НВІ зустрічаються досить рідко через їх високу вартість. Тому в деяких випадках, якщо за вашою оцінкою фінансово-технічних можливостей супротивника є не достатньо для використання сучасної техніки "нападу", можна відмовитися від ведення радіоконтролю у нічний час.

Таблицю зайнятості частот найбільш зручно складати та вести в електронному вигляді з використанням ПЕОМ.

У процесі аналізу сигналів слід мати на увазі, що частина з них може виявитися побічними або позасмуговими випромінюваннями розташованих неподалік потужних радіопередавачів, випромінюваннями промислового чи ін. видів обладнання. Іденти-фікація таких сигналів з відомими джерелами представляє певні труднощі, але може бути здійснена шляхом зіставлення їх частот, часу появи та ін. особливостей. Сигнали на виході радіоприймача можуть бути також наслідком недосконалості самої апаратури радіоконтролю, наприклад, через наявність побічних каналів приймання або перехресної модуляції сигналів у вхідних ланцюгах. Тому оператор повинен мати повне уявлення про недоліки апаратури, що використовує.

Визначення належності випромінювань полегшується, якщо техніка яка використовується має високу роздільну здатність та дозволяє аналізувати, документувати та складати максимальну кількість параметрів прийнятих сигналів. Допомогою для оператора може стати "бібліотека" спектрів, осцилограм і фонограм характерних джерел радіовипромінювань: радіорелейних ліній зв'язку, організаційних каналів мереж стільникового зв'язку тощо. Порівняння виявлених випромінювань із зразками сигналів відомих джерел дає можливість з високим ступенем достовірності в ідентифікації значної кількість невідомих сигналів.

Відомо, що радіовипромінювання джерел НВІ в спектрі свого випромінювання зазвичай мають велику кількість гармонік основної (несівної) частоти. Тому

рекомендується перевіряти "підозрілі" сигнали на наявність гармонік виявленої частоти та проводити оцінку їх відносних рівнів. У випадках, коли джерела випромінювань мають високий рівень гармонік основної частоти, а час їх роботи та проходження по ним інформації збігається з часом роботи організації, можна зробити висновок про можливу приналежність виявлених випромінювань до сигналів, які періодично включаються (джерело НВІ або побічним випромінюванням засобів оргтехніки, що працюють в цієї організації). Сигнали на цих частотах повинні бути проаналізовані та протестовані особливо ретельно при радіомоніторингу приміщення під час проведення спеціальної перевірки.

1.8. Завершальні роботи підготовчого етапу.

Роботи підготовчого етапу, зазвичай, завершуються розробкою документів, що підтверджують легенду прикриття при проведенні різних видів пошукових і дослідних робіт, а також спеціальних бланків та заготовок документів, які прискорюють реєстрацію проміжних результатів запланованих робіт.

Серед документів, що підтверджують вибрані легенди прикриття, можуть використовуватися:

- наряд, наряд-замовлення або копія договору на проведення робіт;
- допуск до робіт на обладнанні у визначеному приміщені;
- рахунок-фактура на виконання робіт;
- технологічні карти для виконання окремих видів робіт;
- накладні на встановлення обладнання та апаратури;
- формуляри, бланки протоколів вимірювань і звітних документів, технічна та методична література, що підтверджує обрану легенду прикриття.

Документи повинні бути виготовлені в необхідній кількості примірників і належним чином оформлені, в тому числі, затверджені необхідними підписами посадових осіб.

Для скорочення непродуктивних витрат часу в ході безпосереднього проведення спеціальної перевірки приміщень доцільно заздалегідь підготувати: схеми комунікацій та плани приміщень (що перевіряються), на які будуть наноситись відмітки місць виявлених джерел НВІ та підозрілих місць; бланки протоколів майбутніх вимірювань; журнали реєстрації заводських та інвентарних номерів перевіреного обладнання; журнали реєстрації місць встановлення пломб та прихованих міток, що сприяють прискоренню робіт при проведенні наступних спеціальних перевірок; карту завантажено радіоефіру; базу даних виявлених та ідентифікованих радіосигналів; перелік частот "підозрілих" радіовипромінювань.

Слід пам'ятати, що на відміну від документів, що підтверджують легенди прикриття, всі документи, які підготовлені для робіт з безпосереднього проведення перевірки, відносяться до категорії конфіденційних та не підлягають розголошенню серед співробітників організації.

Отримано 22.03.2013