ЗАХИСТ ІНФОРМАЦІЇ

УДК 537.871.62

І.М. Коротєєв

ПЕРВИННІ ЗАХОДИ З ПОШУКУ ПРИСТРОЇВ ВИТОКУ ІНФОРМАЦІЇ

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

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

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

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

The paper 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.*

Розвиток у суспільстві ринкових відносин неминуче супроводжується загостренням конкурентної боротьби між виробниками товарів і послуг, зокрема за доступ до інформації. Для її добування використовуються найрізноманітніші методи. Особливе місце серед них займає знімання інформації за допомогою всановлення у приміщення, підключених до засобів обробки інформації або каналів зв'язку спеціальних технічних засобів негласного витоку інформації (далі – НВІ).

Одним з видів або елементом засобів (систем) НВІ є закладні пристрої, таємно впроваджені (закладаються або вносяться) у місця можливого зняття інформації. Номенклатура таких пристроїв нині надзвичайно велика.

Технічні канали витоку інформації (далі – ТКВІ), які за наявності певних умов та спеціальних технічних засобів розвідки можуть бути організовані зловмисниками, називають потенційними. У ході комплексних спеціальних перевірок приміщень повинні бути виявлені потенційні ТКВІ та вироблені рекомендації щодо їх закриття (ліквідації).

Комплексні спеціальні перевірки приміщень займають помітне місце у загальній системі заходів щодо захисту інформації.

1. Підготовчий етап проведення комплексних спеціальних перевірок приміщень

Зарубіжний та вітчизняний досвід проведення робіт із виявлення джерел НВІ вказує, що дії з підготовки й проведення комплексних спеціальних перевірок

приміщень доцільно умовно поділити на три етапи: підготовчий, етап безпосереднього проведення спеціальної перевірки приміщень і заключний етап.

Роботи підготовчого етапу.

1. Уточнення переліку відомостей, що охороняються, та ступеня важливості інформації.

2. Визначення ймовірного супротивника, оцінка його можливостей, тактики впровадження засобів НВІ та їх використання.

3. Розробка задуму проведення комплексної спеціальної перевірки приміщень:

3.1. Вироблення цільової постановки: стосовно якого супротивника слід провести пошукові заходи;

3.2. Визначення масштабу та місця проведення пошукових заходів;

3.3. Вибір часу проведення перевірки;

3.4. Розроблення легенди, під прикриттям якої буде проводитись спеціальна перевірка;

3.5. Вироблення задуму активації впроваджених джерел НВІ;

3.6. Розроблення варіантів дій у разі виявлення джерел НВІ.

4. Вивчення планів приміщень, схем технічних комунікацій, зв'язку, організації охорони, доступу та інших необхідних документів.

5. Попередній огляд приміщень.

6. Розробка переліку апаратури, необхідної для проведення спеціальної перевірки приміщень.

7. Розробка додаткових заходів щодо активізації впроваджених джерел НВІ на час проведення пошуку з різними типами апаратури.

8. Розподіл залучених сил та засобів на об'єкті та видів робіт.

9. Уточнення відповідності методик використання залученої апаратури до конкретних умов майбутньої перевірки.

10. Оформлення плану проведення комплексної спеціальної перевірки приміщень та затвердження його у керівника організації.

11. Підготовка апаратури для проведення пошукових та дослідницьких робіт.

12. Попередній збір даних та аналіз радіоелектронної обстановки в районі обстеження приміщень.

13. Підготовка документів прикриття робіт зі спеціальної перевірки приміщень відповідно до обраної легенди прикриття.

14. Підготовка бланків, схем, інших документів, необхідних для проведення робіт на подальших етапах.

Підготовчий етап є винятково важливим, оскільки якість попередніх робіт зумовлює надійність результатів перевірки. Частина робіт передбачає участь у них керівників організації, у якій має бути проведена перевірка приміщень. Тому від того, чи вдасться від самого початку досягти взаєморозуміння між керівництвом організації та фахівцями пошукових робіт, значною мірою залежить ефективність всіх пошукових заходів.

Слід переконати керівника максимально обмежити коло осіб, які залучаються до підготовки перевірки, щоб забезпечити приховане проведення всіх підготовчих робіт. Необхідно пам'ятати, що в інтересах супротивника може працювати хтось із працівників. Випадковий витік інформації про заплановану перевірку може звести її результативність нанівець. Причиною може бути не тільки можливе вилучення або вимкнення засобів НВІ на період перевірки, але й висока

ймовірність встановлення таких джерел одразу після закінчення перевірки, коли керівництво та служба безпеки організації заспокояться та будуть вважати приміщення "чистими". Тому всі узгодження питань майбутньої перевірки доцільно проводити поза стінами організації.

1.1. Уточнення переліку відомостей, які охороняються, та ступінь важливості інформації, що захищається

Очевидно, що інформація, яка захищається, має різний характер, а її витік може призвести до різних наслідків. Тому необхідно знати не тільки, що і навіщо треба захищати, а й наскільки слід захистити конкретний вид відомостей, які охороняються. Це дозволить диференціювати заходи щодо забезпечення безпеки інформації та скоротити тим самим витрати на їх проведення.

Ступінь захисту інформації обмеженого доступу визначає її власник. Відповідальність за виконання заходів захисту, встановлених власником інформації, закон покладає не тільки на власника, а й на користувачів цієї інформації. Тому важливо чітко усвідомлювати, що інформація обмеженого доступу, власником якої ви можете не бути, використовується на підприємстві, бо ця інформація повинна бути захищена незалежно від вашого бажання.

Доцільний наступний порядок дій із визначення видів, обсягу та ступеня важливості інформації, яку ви повинні захищати від можливого витоку та інших загроз.

Уточнюється перелік відомостей, які необхідно захищати відповідно до законодавства. До них належать відомості, що становлять державну таємницю, а також інші відомості, які віднесені їх власниками до категорії конфіденційних. Ви можете бути користувачем або навіть власником цих відомостей, але зобов'язані забезпечити такий ступінь їх захисту, який вимагає від вас законодавство.

Складається перелік відомостей, що є власністю організації, які доцільно віднести до категорії захищених. Зазвичай у цей перелік включають:

– відомості, що становлять результати творчої діяльності й складові інтелектуальної власності організації: неопубліковані науково-технічні результати, технічні рішення, методи, способи використання технологічних процесів та пристроїв, не забезпечені патентним захистом; відомості про використання програмних продуктів, матеріалів, елементної бази, комплектуючих виробів та способи виробництва нової продукції, стан та особливості перспективних розробок; зміст комерційних, методичних та організаційно-управлінських ідей і рішень: планів реорганізації, розвитку та модернізації виробництва, розширення ринків збуту товарів і послуг, задумів чергових рекламних компаній та ін.; результати маркетингових досліджень, аналізу кон'юнктури ринку, ефективності реклами, відомості про найбільш вигідні форми використання фінансових джерел, цінних паперів, акцій тощо;

– відомості, що становлять ділову інформацію щодо діяльності організації, партнерів;

– відомості про систему безпеки організації: системи охорони, сигналізації, контролю лояльності співробітників, способи застосовування та технічні засоби захисту інформації та ін.

Для кожного з пунктів переліку захищених відомостей визначається можливий економічний збиток від їх витоку, що характеризує собою цінність інформації. Для оцінки можливого збитку можуть бути використані математичні

методи або методи експертних оцінок, при цьому повинні бути враховані як безпосередні, так і непрямі втрати.

Здійснюється сортування пунктів переліку захищених відомостей за цінністю, що захищається, еквіваленту можливого збитку від витоку інформації. У результаті цієї операції пункти переліку повинні бути розподілені за кількома різними групами (категоріями), що включають відомості приблизно однакової цінності.

Обрана кількість таких груп (категорій) визначить число градацій ступеня захисту інформації в системі захисту інформації, яка вами створюється. Цінність відомостей, включених до конкретної групи (категорії), дозволить обґрунтовано обмежити номенклатуру захисних заходів та засобів захисту для кожної групи відомостей, диференціюючи і скоротивши тим самим загальні витрати на захист інформації.

1.2. Визначення ймовірного супротивника та тактики його дій

Найважливіше місце серед робіт підготовчого етапу комплексної спеціальної перевірки приміщень займає виявлення або уточнення ймовірного супротивника, який здійснює перехоплення інформації за допомогою засобів НВІ.

Низка організаційно-методичних документів із захисту інформації від несанкціонованого доступу та технічної розвідки рекомендують у якості супротивника або порушника розглядати суб'єкт, що має доступ до роботи в організації, який є фахівцем вищої кваліфікації і знає все про функціонування системи безпеки, включаючи повні відомості про систему та засоби захисту інформації.

Доцільним є диференційований підхід із визначення ймовірного супротивника. Різноманіття вихідних ситуацій для прогнозування противника, що здійснює зняття інформації з використанням засобів НВІ, може бути, зведено до основних трьох категорій.

Перша. Прагнення застрахувати себе від витоку цілком конкретних відомостей, які становлять для вас найбільшу цінність. У цій ситуації слід, за можливості, найбільш повно уявити собі у вигляді переліку, які організації та приватні особи можуть бути зацікавлені в отриманні такої інформації. Відтак слід проаналізувати складений список та спробувати виділити в ньому організації й структури, які володіють найбільшими фінансовими і технічними можливостями. На зазначені організації слід орієнтуватися при складанні моделі дій ймовірного супротивника.

Друга. Витік інформації, яка захищається, вже завдав шкоди вашій організації або фізичним особам, і ви бажаєте його припинити. У цій ситуації коло організацій та фізичних осіб, яких ви віднесли до ймовірних супротивників, може бути гранично звужене. Перш за все, необхідно проаналізувати, коли, в якому обсязі та в якій формі міг відбутися витік інформації, ким і яким чином вона була використана. Це той самий випадок, коли повною мірою може використовуватися юридична формула, висхідна до римського права: зробив той, кому вигідно.

Третя. Проведення профілактичної спеціальної перевірки приміщень, щоб виключити можливість витоку через засоби НВІ. Цей випадок можна вважати найбільш складним, оскільки він припускає як ймовірного супротивника не тільки конкуруючі підприємства, різного роду кримінальні елементи та структури, а й нерозбірливих у засобах представників органів масової інформації, структур, що займаються збором компромату на замовлення зацікавлених осіб.

Противником можуть виявитись організації, що підтримують з вами ділові, окремі особи. При визначенні кола ймовірних супротивників слід пам'ятати, що вони можуть мати найрізноманітніші спонукальні мотиви для встановлення у організації джерел НВІ.

У переважній більшості випадків визначення ймовірного супротивника – прерогатива керівника підприємства, оскільки він краще за інших уявляє собі стратегічні завдання підприємства, має необмежений доступ до інформації щодо партнерів, клієнтів, конкурентів і співробітників та може організувати добування інформації, якої бракує, як відкритим, так і прихованим шляхом. У оцінці оперативних та технічних можливостей ймовірного супротивника із використання джерел НВІ й прогнозування тактики його дій повинні допомогти технічні фахівці служби безпеки.

1.3 Розробка задуму проведення спеціальної перевірки приміщень

Розробку задуму проведення спеціальної перевірки приміщень можна вважати найбільш важливим елементом робіт підготовчого етапу.

У задумі визначено:

- цільове призначення: для протидії якому супротивнику слід провести пошукові заходи;
- масштаб та місце проведення пошукових заходів;
- час проведення перевірки;
- легенда, під прикриттям якої має бути проведена спеціальна перевірка;
- задум активації впроваджених джерел НВІ;
- варіанти дій у разі виявлення джерел НВІ.

Цільове призначення безпосередньо випливає з результатів роботи (з уточнення або виявлення ймовірного противника). Результати оцінки, оперативних та технічних можливостей супротивника зумовлюють масштаб проведення пошукових заходів.

Вибір часу проведення перевірки (у робочий чи вихідний день, вдень або вночі, у робочий час, до початку робочого часу або відразу після закінчення робочого дня) безпосередньо пов'язаний з розробкою легенди, під прикриттям якої буде працювати пошукова бригада.

Одним з основоположних принципів проведення комплексних спеціальних перевірок приміщень є скритність виконання основних робіт. З цього випливає необхідність розробки для персоналу підприємства і відвідувачів, у тому числі осіб, що ймовірно працюють на супротивника, правдоподібної версії (легенди прикриття) появи на підприємстві фахівців, що займаються проведенням вимірювальних та пошукових робіт з використанням складного та досить специфічного обладнання.

Розроблена легенда прикриття має узгоджуватись з діяльністю підприємства й мати мінімальний деструктивний вплив на його повсякденний розпорядок. Досить імовірно, що доведеться розробляти не одну, а відразу кілька легенд прикриття, у тому числі для появи на підприємстві одного або кількох членів пошукової бригади, які мають завдання провести попередній огляд приміщень. Для кожної з легенд повинні бути розроблені способи та визначено час їх доведення до персоналу підприємства, складений перелік необхідних для підтвердження легенди обладнання, приладів і документів. Загальними вимогами до

легенд прикриття є їх правдивість, природність, надійність та відповідність створюваної ситуації змісту робіт членів пошукової бригади.

Як легенди прикриття пошукових робіт можна рекомендувати:

• перевірку фахівцями стану телефонних ліній та устаткування;

• перевірку стану опалювальної системи, водопровідних та інших інженерно-технічних комунікацій, проведення на них ремонтних робіт;

• планову перевірку функціонування систем охоронної та пожежної сигналізації;

• проведення регламентних робіт на елементах системи внутрішнього зв'язку підприємства;

• перевірку системи заземлення, стану електроізоляції проводів системи освітлення, елементів системи електроживлення;

• пошук іскріння контактів прихованої електропроводки для усунення перешкод ПЕОМ;

• санітарну перевірку робочих місць (освітленість, рівень радіації й електромагнітних випромінювань, склад повітря тощо);

• підготовку та проведення ремонту приміщень.

Під час вибору часу проведення перевірки слід враховувати, що в неробочий час дистанційно керовані засоби НВІ можуть виявитися вимкненими. Це помітно знизить ймовірність їх виявлення пошуковою апаратурою, для цього необхідно заздалегідь продумати заходи з активації джерел НВІ. Можна, наприклад, заздалегідь поширити серед працівників підприємства інформацію про нібито намічену на обраний для перевірки час важливу нараду із запрошенням осіб зі інших організацій. Ще краще, якщо керівництво організації проведе фіктивну, але "правдиву" нараду, яка здатна настільки зацікавити супротивника, що він активує всі дистанційно керовані засоби НВІ. Очевидно, що обраний сценарій заходів щодо активації впроваджених джерел НВІ не повинен суперечити легенді прикриття пошукових заходів.

Важливість усіх цих питань для успіху перевірки, їх тісний взаємозв'язок, вплив на звичайний порядок роботи підприємства й необхідність опрацювання в єдиному пакеті вимагають рішень, приймати які повинен керівник підприємства.

Зазвичай, керівник підприємства буде прагнути перекласти вирішення питань задуму на керівника служби безпеки. Водночас саме керівник підприємства розуміє, звідки може надходити загроза його секретам, яка легенда прикриття робіт з перевірки приміщень найбільш органічна до діяльності підприємства, що, не суперечить сценарію заходів з активації засобів НВІ.

Однак необхідно зазначити, що сказане вище стосується головним чином керівника не дуже великої організації, що має можливість самостійно вникати в усі нюанси її роботи. У великій організації, де кожен великий відділ, служба звичайно розробляють власні плани захисту інформації, задум проведення спеціальної перевірки приміщень відділу або служби може бути розроблений керівником цього підрозділу.

У будь-якому випадку фахівці служби безпеки повинні допомогти керівнику організації прийняти доцільні рішення з питань задуму спеціальної перевірки приміщень. У ході обговорення питань, що відносяться до задуму, фахівці повинні допомогти керівнику усвідомити тісний взаємозв'язок вибору часу проведення

перевірки, легенди прикриття відповідних робіт і заходів з активації впроваджених джерел НВІ. Слід переконати керівника у доцільності вибору такої легенди прикриття, яка дозволяла б використовувати при перевірці приміщень, за можливості, весь арсенал пошукових засобів.

Припустимо, що легендою прикриття пошукових робіт приміщень обрана перевірка функціонування пожежної та охоронної сигналізації підприємства. Ця легенда допускає використання пошуковою бригадою досить широкого спектру спеціальної техніки. Водночас поява співробітника із приладом нелінійної локації, який обстежує стіни та стелі приміщень, не вписується у зміст легенди. Така легенда, якщо вона обрана як єдина, швидше за все, змусить відмовитися від використання приладу нелінійної локації, а його відсутність, хоча б частково, компенсувати більш ретельним візуальним оглядом і наполегливою рекомендацією керівнику підприємства встановити у приміщенні систему активного захисту інформації.

Цілком у компетенції керівника організації перебуває також визначення варіантів подальших дій. Зазвичай, обирається один з варіантів:

• вилучення джерел;

• нейтралізація джерел НВІ без його видалення з місця установки;

• збереження джерел НВІ в робочому стані на місці виявлення для подальшого його використання з метою дезінформації супротивника.

При виборі варіанту дій необхідно пам'ятати, що вилучення НВІ може спонукати супротивника до впровадження інших джерел НВІ, для виявлення якого доведеться знову проводити пошукові заходи.

Нейтралізація джерел НВІ полягає у модифікації його роботи, при якій більшість функцій засобу зберігаються, крім найголовнішого: воно перестає передавати інформацію. Наприклад, нейтралізація радіомікрофона може бути здійснена шляхом заклеювання липкою стрічкою або закладення шматочком пластиліну отворів (для вбудованого мікрофона).

1.4. Вивчення та попередній огляд об'єктів перевірки

Вивчення та попередній огляд об'єктів перевірки є достатніми умовами правильного визначення обсягу майбутніх робіт та вибору необхідного устаткування. Вивчення об'єкта перевірки включає в себе:

• знайомство з профілем підприємства, особливостями його функціонування, призначенням використання приміщення (що підлягає перевірці);

• вивчення наявних планів території підприємства, навколишньої забудови, розміщення на території підприємства будівель та споруд, розміщення в будівлях приміщень, що підлягають перевірці, у т.ч. суміжних;

• вивчення наявних в організації планів і будівельних креслень приміщень, що підлягають перевірці, іншої будівельної та ремонтної документації на ці приміщення;

• знайомство з організацією охорони території, будівель й приміщень, вивчення порядку і системи контролю доступу на територію організації (які підлягають перевірці) та суміжні з ними приміщення;

• вивчення схем інженерно-технічних комунікацій, енергопостачання, зв'язку, охоронної, пожежної сигналізації, інших документів щодо робіт з прокладання, ремонту й демонтажу проводових і інженерно-технічних комунікацій;

• знайомство із організацією системи захисту інформації, засобами ТЗІ та заходами, які застосовують для запобігання витоку інформації з приміщень, що підлягають перевірці.

Вивчення об'єкта перевірки здійснюється шляхом його відвідування, бесід з керівником організації, керівником служби безпеки, іншими компетентними особами, а також вивчення наявної на підприємстві документації. У ряді випадків, особливо коли в організації немає необхідної проектної та експлуатаційної документації, вона застаріла або її якість не задовольняє завданням перевірки й може виникнути необхідність залучити до співбесіди технічних фахівців з експлуатації будівель та технічних систем: енергосистем, систем центрального опалення, систем зв'язку, радіотрансляції.

Слід пам'ятати, що всі консультації з компетентними особами повинні проводитися в рамках обраних заздалегідь легенд прикриття (наприклад, про майбутній ремонт приміщень або встановлення у них нового обладнання), щоб не викликати у співрозмовників підозр стосовно підготовки до проведення спеціальної перевірки приміщень.

У результаті співбесід та вивчення документів у фахівців пошукової бригади має скластись чітке уявлення щодо характеру навколишньої забудови та прилеглої місцевості, конструктивних та інших особливостей будівлі, розміщеного в ній обладнання, проводових та інженерно-технічних комунікацій, доступності приміщень для відвідувачів та персоналу підприємства, системи охорони, контролю доступу й захисту інформації. Цієї інформації повинно бути достатньо для складання переліку пошукових та дослідницьких робіт, переліку необхідної для цих робіт апаратури, орієнтовної оцінки очікуваних трудовитрат на їх виконання.

Для скорочення та прискорення подальших робіт доцільно вже на цьому етапі скласти схему прилеглої до об'єктів перевірки місцевості з зазначенням особливостей сусідніх будівель, планів поверхів будівлі, в якій розташоване приміщення, що потребує перевірки.

На кожне приміщення, що перевіряється, повинна бути складена його характеристика, яка включає відомості про його призначення, розміри, особливості конструкцій огородження, меблювання й ін. предмети обстановки, види встановленого обладнання, проводові та інженерно-технічні комунікації та ін. необхідні відомості. Аналогічні дані доцільно підготувати на суміжних приміщення.

Документальне вивчення об'єктів перевірки має обов'язково доповнюватися проведенням їх огляду фахівцями пошукових робіт. Виключати попередній огляд об'єктів перевірки з робіт попереднього етапу недоцільно навіть в тих випадках, коли в організації є повний комплект планів приміщень та схем, що дозволяє скласти об'єктивну картину майбутньої перевірки. З якою б старанністю не були складені й вивчені наявні у організації плани приміщень, схеми комунікацій та ін. документи, вони не можуть замінити інформацію, що одержує фахівцем з пошуку при візуальному огляді приміщень.

У ході попереднього огляду особливу увагу необхідно звернути на:

• вплив місцевості та навколишньої забудови на проходження радіохвиль ультракороткохвильового діапазону й оптичного випромінювання ІЧ-діапазону для визначення можливих місць розміщення супротивником пунктів прийому радіосигналів або ІЧ-випромінювань джерел НВІ, а також пунктів перехоплення ПЕМВ засобів оргтехніки з приміщень, що перевіряються;

• можливість доступу сторонніх осіб до зони електромагнітної доступності ПЕМВ засобів оргтехніки та випромінювань джерел НВІ;

• можливість розміщення джерел витоку віброакустичних сигналів на зовнішніх поверхнях конструкцій, що обгороджено приміщення (які підлягають перевірці);

• конструктивні особливості приміщень (які перевіряються) та інженерно-технічні комунікації, що не відображені у попередньо вивчених документах (підшивні або підвісні стелі, гіпсокартонні стіни, фальшпідлога, наявність підпільних каналів, плінтусів, знімних панелей, зовнішніх і прихованих кабельних каналів, трубопроводів, захисних екранів та ін.);

• місця можливого доступу сторонніх осіб до елементів конструкцій огородження приміщень, технологічних й провідних комунікацій, які проходять через приміщення;

• сліди нещодавно проведеного ремонту, реконструкції або вторгнення до елементів конструкцій огородження, інженерно-технічних та проводових комунікацій;

• особливості прокладки проводових комунікацій, наявність транзитних ліній, які проходять через приміщення;

• особливості внутрішнього оздоблення та обстановки приміщень (характер оздоблення стін, наявність підлогових покриттів, кількість меблів, кількість і складність складових інтер'єру тощо).

У ході огляду слід мати на увазі, що в умовах нещільної міської забудови відстань прийому сигналів радіозакладного пристрою потужністю 20 мВт, що працює в найбільш зручній з точки зору максимальної дальності поширення сигналів позиції у діапазоні 200 .. 500 МГц, зазвичай не перевищує 300... 400 м. В умовах суцільної забудови при підвищенні робочої частоти радіозакладного пристрою, відстань прийому її сигналів істотно знижується. Натомість в умовах прямої видимості між радіозакладним пристроєм та антеною радіоприймального пункту відстань прийому її сигналів зростає в два-три рази. Відстань перехоплення ПЕМВ дисплеїв (ЕП) ПЕОМ в умовах прямої видимості із застосуванням гостроспрямованих антен, теоретично може досягати 400 м для дисплеїв з металевим кожухом і 1200 м для дисплеїв з пластмасовим кожухом, проте зазвичай вона майже не перевищує 10 ... 30 метрів.

Значним підґрунтям у ході подальших робіт можуть стати фотографії, які можна зробити під час попереднього огляду. Бажано зробити фотографії вікон і зовнішніх стін приміщень (що підлягають перевірці) та у кожному з них зробити кілька знімків їх загального вигляду з різних точок зйомки, а також фотографії, які фіксують розміщення меблів та інших предметів інтер'єру в приміщенні, предметів на столах, полицях і в шафах. Не завадять й знімки елементів будівельних конструкцій та комунікацій, які Вас зацікавили своєю незвичністю. Результати попереднього огляду та вивчення зроблених фотографій можуть помітно вплинути на вибір пошукової та дослідницької апаратури, номенклатури, зміст і тактику пошукових робіт*.

Отримано 17.12.2012

* Продовження у наступному номері.