УДК 621.396:004.056

ВИЯВЛЕННЯ ЗАКЛАДНИХ ПРИСТРОЇВ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Духанін Г.А.
Науковий керівник – к.т.н., проф. Олейніков А.М.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ,
м. Харків, Україна
тел. +38(050) 325-75-00, e-mail: hlib.dukhanin@nure.ua.

This work is devoted to the detection of embedded devices at the objects of information activities.Embedded devices are detected in the course of complex special checks at the objects of information activity. Comprehensive special checks are divided into three main stages. The first stage of the verification will be the preparatory stage. At the second stage, a direct check is carried out at the facility. The end of the test is the final stage.

Для добування інформації використовуються різні методи, що включають розкрадання носіїв інформації, її копіювання, підслуховування, перехоплення інформаційних ПЕМВН, перехоплення інформації, що передається за системами зв'язку, та ін. Значну роль серед них займає знімання інформації за допомогою підключених до засобів обробки інформації або каналів зв'язку закладних пристроїв (далі – ЗП).

Займатися нейтралізацією впроваджених ЗП – є одним з найважливіших напрямів ТЗІ на будь-якому підприємстві. Завданням проведення комплексу спеціалізованих дій з перевірки об'єктів інформаційної діяльності (далі – ОІД) – є припинення отримання зловмисником інформації, що охороняється на ОІД за допомогою використання ЗП. Такі дії направлені на запобігання збиткам власника інформації. Але варто звернути увагу на те, що проведення перевірок на ОІД не дозволяє захистити повною мірою конфіденційні відомості від усіх видів загроз. Всесвітній досвід у захисті інформації вказує на те, що найефективнішим і надійнішим може бути лише комплексний захист, який поєднує в собі правове, організаційне та технічне спрямування. Враховуючи вищезазначене, такі перевірки приміщень можна розглядати лише як один з етапів підсистеми захисту інформації від витоку технічних каналів у складі цілого комплексу захисту інформації на ОІД.

Світовий досвід з виявлення ЗП дає зрозуміти, що при підготовці до проведення перевірок ОІД дії доцільно розділити на три умовні етапи, а саме: підготовчий; безпосереднього проведення перевірки ОІД; заключний.

Для забезпечення надійності результатів перевірки слід серйозно поставитися до виконання підготовчого етапу. Одним із аспектів робіт на даному етапі – є участь у них керівника підприємства, на якому проводиться перевірка. Отже рівень взаєморозуміння між керівництвом підприємства та

виконавцем робіт безпосередньо позначиться на ефективності всіх робіт із виявлення ЗП.

Безпосереднє проведення на ОІД запланованих пошукових заходів та досліджень є змістом другого етапу робіт з комплексної спеціальної перевірки приміщень. Насамперед, ще до початку прямого виконання пошукових робіт, рекомендовано обстежити прилеглі до підприємства вулиці, а також прилеглу територію. Існує ймовірність, що противник міг розгорнути пости прийому інформації з приміщень, що підлягають перевірці. Під час перевірки приміщення радиться закрити двері, вікна, жалюзі та штори для запобігання зоровому контакту з боку вулиці або сусідніх приміщень. З метою приховати шум, що супроводжує ведення пошуку, доречно включити звуковідтворюючу апаратуру. Розгортання пошукової та дослідницької апаратури та ведення запланованих робіт має здійснюватися безшумно, з виконанням демонстраційних дій, передбачених легендою прикриття робіт.

Завершальний етап перевірки охоплює роботи, які, зазвичай, виконуються в офісі організації, яка проводила перевірку. Заключні роботи кінцевого етапу включають роботу з оформлення підсумкових та звітних документів, планування заключної зустрічі з керівництвом підприємства і надання керівнику фірми створених за результатами перевірки документів для узгодження.

У доповіді також розглянуто питання класифікації засобів виявлення, локалізації і нейтралізації ЗП, особливості технічних характеристик радіоакустичних ЗП, знакова структура радіоакустичних ЗП, основні вимоги до структури і параметрів засобів радіомоніторингу та особливості застосування апаратно-програмного комплексу "VOSTOK" для виявлення ЗП.

Метою даної роботи є – звернення уваги на важливість ретельного підходу до організаційних та методичних питань виконання складних спеціальних перевірок приміщень.

Список використаних джерел:

1. Болдырев А.И. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОИСКУ И НЕЙТРАЛИЗАЦИИ СРЕДСТВ НЕГЛАСНОГО СЪЕМА ИНФОРМАЦИИ / А.И. Болдырев, И.В. Василевский, С.Е. Сталенков. – Москва, 2001. – 138 с. – (ЗАО НПЦ Фирма «НЕЛК»).

2. Олейніков А.М. «Методи та засоби захисту інформації» Навчальний посібник для студентів вищих навчальних закладів (з гріфом МОН України)// Харків: НТМТ , 2014. – 298с ;

3. І.Є. Антіпов, А.М. Олейніков, Ю.В. Ликов, В.Д. Кукуш, І.О. Милютченко. Засоби та системи технічного захисту інформації: Навчальний посібник для студентів ЗВО / Харків: ХНУРЕ, 2019. – 216 с.