ЗАСТОСУВАННЯ СПЕЦІАЛЬНОЇ ТЕХНІКИ ДЛЯ БОРОТЬБИ ІЗ НЕСАНКЦІОНОВАНИМ ОТРИМАННЯМ МОВНОЇ ІНФОРМАЦІЇ

Цибуляк Богдан Зіновійович, доцент кафедри управління інформаційною безпекою, канд. фіз.-мат. наук;
Захарків Тетяна Іванівна, студент;
Величко Ольга Василівна, студент;
Львівський державний університет безпеки життєдіяльності

В умовах запеклої конкурентної боротьби на міжнародному та внутрішньому ринках різко зросли масштаби промислового шпигунства, при якому використовуються як легальні, так і нелегальні методи і засоби відбору інформації. Все частіше для добування важкодоступної інформації використовуються електронні пристрої перехоплення мовної інформації (закладні пристрої), що впроваджуються у службові приміщення. Тому виявлення електронних пристроїв перехоплення інформації є одним з важливих напрямків діяльності ОВС для забезпечення інформаційної безпеки підприємств, установ і організацій, незалежно від форми їх власності та боротьби із організованою злочинністю.

Для правильного вибору складу апаратури при виявленні закладних пристроїв необхідно знати принципи їх роботи та основні характеристики. На сьогоднішній день існує величезна кількість різних видів підслуховуючих пристроїв (ПП). Найпоширенішими видами пристроїв несанкціонованого здобуття інформації є:

- акустичні підслуховуючі пристрої;
- вібраційні підслуховуючі пристрої;
- інфрачервоні підслуховуючі пристрої;
- мережеві підслуховуючі пристрої;
- телефонні підслуховуючі пристрої;
- лазерні підслуховуючі пристрої.

Це далеко не повний перелік підслуховуючих пристроїв, адже практично щороку з'являється все новий вид аналогічних спецпристроїв.

Акустичні ПП складаються з трьох основних компонентів, які визначають їх технічні можливості. Це – мікрофон, що визначає зону акустичної чутливості приладу, радіопередавач, що визначає дальність його дії і скритність роботи, і джерело електроживлення, що визначає тривалість роботи пристрою.

Такі закладки, працюють як звичайний передавач. Як джерело електроживлення, як правило, використовуються малогабаритні акумулятори. Термін роботи пристроїв, що працюють від власного джерела живлення, визначається ємністю акумулятора. При безперервній роботі і передачі інформації – це 1-2 доби. Другий варіант електроживлення - підключення прослуховування до ліній електроживлення або телефонного зв'язку. Термін дії таких ПП практично не обмежений.

Вібраційні підслуховуючі пристрої - це пристрої, що перехоплюють акустичні коливання (вібрації), які поширюються у твердих конструкціях. Це можуть бути практично будь-які елементи будівлі і офісу – підлога, стеля, стіни, труби опалювання, системи водопостачання, каналізації. Такі підслуховуючі пристрої називаються радіостетоскопами. Оскільки звукова хвиля викликає коливання в твердих елементах конструкції, радіостетоскопи здатні уловлювати звукові коливання через бетонні стіни завтовшки до півметра, а також через будь-які види дверей і віконних конструкцій.

Інфрачервоні підслуховуючі пристрої – це пристрої, які передають інформацію по оптичному каналу в інфрачервоному (невидимому) діапазоні спектра. Такі ПП ще називають інфрачервоними закладками. Інфрачервоний передавач перетворює акустичні коливання в світлові та передає інформацію на спеціальний приймаючий пристрій – приймач оптичного випромінювання. Дальність дії (відстань передачі інформації) такої закладки складає декілька сотень метрів. Отримання відомостей за допомогою інфрачервоних закладок є альтернативою до ведення прослуховування звичайними акустичними заставними пристроями. Це пов'язано з тим, що

акустичні ПП можна легко виявити спеціальними пристроями, які уловлюють радіовипромінювання.

Мережеві підслуховуючі пристрої – ПП, які для передачі отриманої інформації використовують лінії електроживлення мережі 220 В. ПП можуть бути встановлені в електричні розетки, подовжувачі, побутову апаратуру що живиться від мережі змінного струму, або вмонтовані безпосередньо в силову лінію. Основною перевагою таких закладок можна вважати необмежений час роботи, високу надійність і складність виявлення. Для прийому переданої мережевими підслуховуючими пристроями інформації використовуються спеціальні приймачі, що підключаються в електромережу в межах будівлі. Як антену мережеві ПП використовують силовий дріт з передачею інформації по частотах від 40 до 600 кГц.

Телефонні підслуховуючі пристрої призначені для перехоплення мовної інформації із ліній телефонного зв'язку і подальшої передачі отриманого сигналу по радіоканалу. Такий ПП може встановлюватися як в розрив лінії, так і в телефонній розетці.

Лазерний підслуховуючий пристрій по суті не є повною мірою ПП, оскільки сам пристрій не знаходиться безпосередньо на місці знімання інформації. Лазерний мікрофон складається із системи, яка дозволяє на достатній відстані (до 300м) зчитувати вібрацію шибок і перетворювати її в акустичну інформацію (чутну мову). Лазерні спецзасоби поділяються за принципом роботи. Бюджетні поширеніші моделі вимагають для роботи (здобуття інформації) нанесення на скло плями спеціальною фарбою, що відбиває лазерний промінь в місце випромінювання для прийняття фотоприймальним пристроєм. Другий тип лазерних підслуховуючих пристроїв, не потребують спецпокриття скла, але вони дорогі і складні в експлуатації. Такі пристрої можуть дозволити собі лише спецслужби або організації з чималим бюджетом.

Для забезпечення захисту приміщення для переговорів можна використати наступні прилади захисту:

1. УКХ-приймач – для виявлення ПП в даному приміщенні.
2. Генератор "Window-1" – для захисту вікон від передачі інформації, яка здійснюється в оптичному (інфрачервоному) діапазоні.
3. Система безпеки "Теле-2" – для придушення підслуховуючих пристроїв, несанкціоновано підключених до телефонної лінії.
4. Генератор шуму "GS-200" для захисту акустичної інформації.

ВИСНОВКИ

У зв'язку з переходом від промислового до інформаційного суспільства різко зросли масштаби промислового шпигунства, при якому використовуються всі доступні методи і засоби отримання інформації. Проведено огляд та класифікацію існуючих пристроїв відбору мовної інформації та запропоновано заходи та устаткування, яке дозволяє виявляти підслуховуючи пристрої у приміщенні та захиститися від несанкціонованого відбору інформації.

ЛІТЕРАТУРА

1. Домарьов В.О. Організація захисту інформації. – М.: Вид-во "А-Стиль", 2004. – 896 с.
2. Івченко О. Промислове (економічне) шпигунство: конкурентна розвідка й контррозвідка // Юридичний журнал. – 2003, № 7.
3. Конохович Г.Ф. Защита информации в телекомуникационных системах. – К.: МК Прес Киев, 2005. – 288 с.