УДК 004.9:654

Яковлєв А. А., Лис О. О.

СПЕЦІАЛЬНІ ТЕХНІЧНІ ЗАСОБИ НЕГЛАСНОГО ЗБОРУ ІНФОРМАЦІЇ

Запропоновано способи класифікації технічних засобів негласного збору інформації. У результаті проведення аналізу закладних пристроїв встановлено, що з усіх типів цих пристроїв найбільш широке розповсюдження в силу своїх переваг знайшли радіозакладні та мережеві закладні пристрої. Запропоновано комплекс заходів щодо протидії промисловому шпигунству, який засновано на поєднанні організаційно-правових та технічних методів і засобів захисту.

Ключові слова: *інформація, захист, класифікація, закладні пристрої, промислове шпигунство.*

Предложены способы классификации технических средств негласного съема информации. В результате проведения анализа закладных устройств установлено, что из всех типов этих устройств наиболее широкое распространение в силу своих преимуществ нашли радиозакладные и сетевые закладные устройства. Предложен комплекс мероприятий по противодействию промышленному шпионажу, который основан на сочетании организационно-правовых и технических методов и средств защиты.

Ключевые слова: *информация, защита, классификация, закладные устройства, промышленный шпионаж.*

Proposed ways of classification of technical means of secret information retrieval. As result of the analysis of embedded devices installed basic classifying signs for the memories, moreover of all types devices most widespread due to its advantages found radioembedded and networked embedded devices. The complex of measures on counteraction to industrial espionage, which is based on a combination of legal and technical methods and means for protection.

Key words: *information, safety, classification, embedded devices, industrial espionage.*

Постановка проблеми. На сучасному етапі, коли багато традиційних ресурсів людського прогресу втрачають своє першочергове значення, інформація як була, так і залишається одним із головних ресурсів науково-технічного і соціально-економічного розвитку світового співтовариства. Однак багато фахівців відзначають слабкість юриспруденції розвинених країн щодо захисту підприємств від промислового (комерційного) шпигунства [1; 2]. Викрадення промислових секретів важко довести, а неадекватність законів обмежують суди і дають мало шансів потерпілим у переслідуванні злочинців, які займаються промисловим шпигунством.

Таким чином, проблема захисту інформації та забезпечення її конфіденційності набуває актуальності для багатьох комерційних підприємств, чия діяльність перебуває поза сферою, де ці питання вирішують державні органи. І, звичайно, кожному хочеться для зміцнення своєї безпеки використовувати самі надійні сучасні методи і засоби, що враховують усі особливості прийомів несанкціонованого добування інформації.

Метою статті є класифікація засобів негласного збору інформації для вибору оптимальних способів здійснення інформаційної безпеки власників конфіденційної інформації.

Аналіз публікацій. Один з ефективних шляхів негласного збору інформації засновано на застосуванні так званих закладних пристроїв (ЗП), що таємно встановлюються в місцях можливого перебування об’єктів спостереження або підключаються до використовуваних ними каналів зв’язку [3], причому для опису таких пристроїв використовуються також терміни «радіомікрофони», «закладки», «жучки», «спецзасоби» [4; 5; 6]. На сьогодні створено величезну кількість типів таких пристроїв [7; 8], що відрізняються принципом функціонування, способом передачі інформації, дальністю дії, а також розміром і зовнішнім оформленням. Зазвичай ЗП таємно встановлюються на елементи конструкції будівель та інтер’єру, кріпляться під одягом або камуфлюються під особисті речі.

Основний матеріал досліджень. Для того, щоб систематизувати уявлення про закладні пристрої, доцільно ввести п’ять ознак їх класифікації (рис. 1).

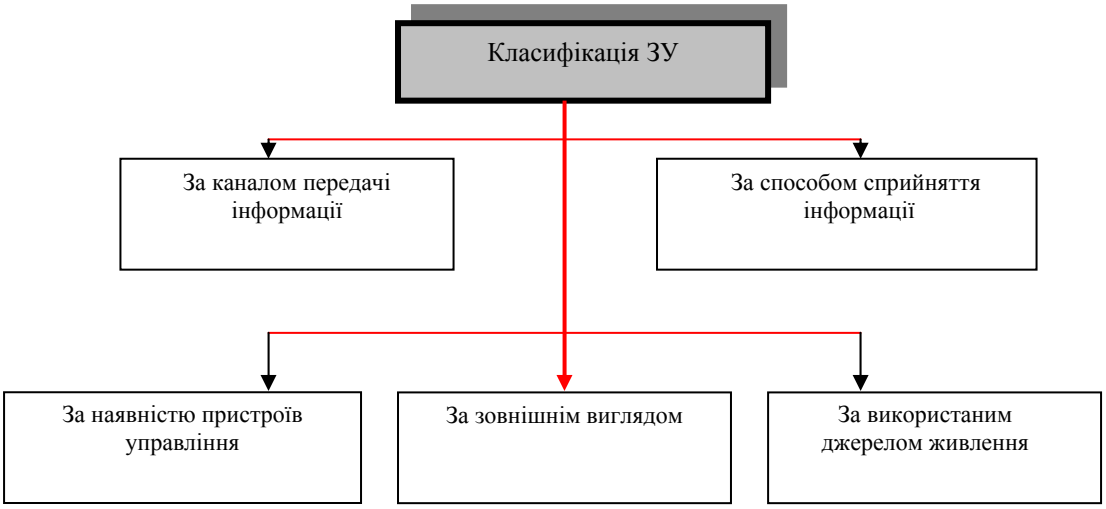

Рис. 1. Основні ознаки класифікації ЗП

Залежно від **каналу передачі інформації** розрізняють такі типи ЗП: радіозакладки; інфрачервоні закладки; закладки з передачею інформації струмопровідними лініями; закладки з записом на магнітофон.

У **радіозакладних пристроях (РЗП)** для передачі інформації використовується енергія електромагнітних хвиль, які не впливають на органи чуття людини і здатні поширюватися на значні відстані, долаючи природні та штучні перешкоди. Завдяки цим двом властивостям РЗП дозволяють за допомогою спеціальної приймальної апаратури вести таємне спостереження за цим об'єктом із досить віддаленої від нього точки.

В **інфрачервоних закладках (ІЧ)** для передачі інформації використовується енергія електромагнітних хвиль, але не радіодіапазону, а невидимої частини оптичної сфери спектру – інфрачервоного діапазону. Завдяки малій довжині такі хвилі розповсюджуються вузьким пучком у заданому напрямі, їх важко виявити навіть за допомогою спеціальної апаратури, однак висока прихованість таких пристроїв і незастосовність на мобільних об'єктах істотно ускладнює їх застосування.

Закладки з передачею інформації струмопровідними лініями використовують властивість електричних сигналів розповсюджуватися на значні відстані по провідниках і володіють такими суттєвими перевагами: висока прихованість передачі інформації, велика дальність дії, відсутність необхідності в додаткових джерелах живлення, унаслідок чого вони часто застосовуються недобросовісними конкурентами для отримання відомостей конфіденційного характеру.

У випадках, коли відсутня необхідність отримання оперативної інформації в реальному масштабі часу, а також є можливість прихованого вилучення та заміни касети або магнітної стрічки, **закладка може оснащуватися магнітофоном** замість пристрою передачі по одному з розглянутих каналів. Такий спосіб, як правило, застосовується тільки в тих випадках, коли є потенційна загроза виявлення об'єктом спостереження каналу передачі інформації (наприклад, за допомогою спеціальної апаратури контролю).

Залежно від **способу сприймання інформації** розрізняють три типи ЗП: мікрофонного типу; вібраційного типу; із підключенням до комунікаційних ліній. Принцип дії ЗП ***мікрофонного типу*** заснований на перетворенні акустичних атмосферних коливань в електричні сигнали і передачі їх споживачу одним із вищеперелічених способів. ЗП ***вібраційного типу*** (стетоскопи) перехоплюють акустичні коливання твердих середовищ (вібрації), що виникають унаслідок тиску на них атмосферних акустичних хвиль. ЗП із ***підключенням до комунікаційних ліній*** призначені для негласного перехоплення інформації, що циркулює в телефонних або волоконно-оптичних лініях.

За **наявністю пристрою управління** ЗП умовно можна розділити на три групи: із безперервним випромінюванням; із дистанційним управлінням; із автоматичним включенням при появі сигналу. ЗП із ***безперервним випромінюванням*** найбільш прості у виготовленні, дешеві і призначені для отримання інформації протягом обмеженого проміжку часу, проте недоліком таких пристроїв є можливість їх виявлення за випромінюванням.

Суттєво збільшити час безперервної роботи ЗП з автономним живленням і підвищити прихованість дозволяє застосування ***дистанційного управління*** ЗП. Воно дозволяє переводити пристрій у режим випромінювання тільки в тих випадках, коли об'єкт спостереження веде переговори або передає інформацію по каналах зв'язку.

Іншим способом збільшення часу роботи ЗП є використання пристроїв ***автоматичного включення***

передавача при появі сигналу (акустичного або електричного в лінії). Пристрої включення від голосу називають акустоматами, а також системами VAS або VOX. При появі сигналу з початком розмови об'єкта спостереження з ким-небудь подається напруга на передавач, і той переходить у режим випромінювання. Застосування акустомата дозволяє в кілька разів збільшити час роботи ЗП, але призводить до його подорожчання і втрати перших слів при кожному включенні.

За **використовуваним джерелом живлення** ЗП поділяються на два види: із власним (автономним) джерелом; із живленням від зовнішнього джерела. Причому, до другого виду відносяться ЗП із передачею інформації струмоведучими лініями і з безпосереднім підключенням до комунікаційних ліній.

За **зовнішнім виглядом** ЗП можуть бути у звичайному виконанні (у металевому корпусі і мають форму паралелепіпеда) або в закамуфльованому вигляді (вбудовані в предмети інтер'єру або особисті речі).

Класифікація, принципи дії та основні характеристики радіозакладних пристроїв (РЗП). Найбільш широке застосування в практиці промислового шпигунства знаходять пристрої з радіоканалом передачі перехопленої інформації, які називаються радіозакладками (РЗП) або радіомікрофонами (РМ). Підвищений інтерес до використання РЗП пов'язаний з їх винятковими можливостями віддаленого спостереження за об'єктами, у тому числі мобільними, незалежно від часу доби і погодних умов.

Для класифікації РЗП може бути використано такі **ознаки**: принцип формування сигналу; спосіб закриття переданої інформації і дальність дії. Відповідно до **принципу формування сигналу** РЗП можуть бути активні, пасивні та напівактивні. У пасивних і напівактивних РЗП використовується підсвічування (випромінювання) додаткового джерела сигналу. Однак, володіючи високою прихованістю (вони не випромінюють, якщо їх не опромінює потужне джерело сигналу), пасивні та напівактивні РЗП досить громіздкі, дорогі, а тому не знайшли широкого практичного застосування.

Найпростіші РМ, стуктурну схему яких наведено на рис. 2, містять кілька основних елементів, що визначають їх технічні характеристики та можливості застосування: мікрофон із низькочастотним підсилювачем (НЧП); радіопередавач (РП); джерело живлення (ДЖ), від якого залежить тривалість роботи РМ; антена; блок накопичення і стиснення інформації (БНС); пристрій управління (ПУ), у ролі якого може використовуватися приймач дистанційного управління (ПДУ), що дозволяє переводити РМ у режим випромінювання тільки за кодованими радіосигналами «ініціації»; та приймальна апаратура (ПРА). Стрілками на рис. 2 показано можливі вразливі елементи як самого РМ, так і утвореного ним технічного каналу витоку інформації, вплив на які дозволяє блокувати цей спосіб інформаційної загрози.

За **способом закриття інформації** РЗП бувають: без закриття інформації; із використанням складних видів модуляції; із кодуванням інформації.

Залежно від **потужності передавача** РЗП діляться на три види – малої, середньої і великої дальності дії.

Деякі дані за характеристиками РЗП, які серійно випускаються, наведено в таблиці 1.

Таблиця 1

Залежність дальності дії РЗП від потужності передавача та експлуатаційних умов

$P_{вих, мВт}$ (Потужність РП)	ДАЛЬНІСТЬ передачі інформації, м		
	У залізозобетонному приміщенні	Із приміщення на вулицю	Пряма видимість
1	20…30	50…100	100…200
10	30…60	150…200	200…500
100	50…100	300…400	800…1000
500	100…200	400…600	1000…2000

Мережеві закладні пристрої (МЗП) та їх характеристики.

МЗП, які призначено для негласного збору акустичної (мовної) інформації з передачею її електромережею, володіють рядом переваг, порівняно з іншими типами ЗП: необмежений час безперервної роботи, так як живлення ЗП здійснюється від тієї ж електромережі; підвищена прихованість роботи, зумовлена видом модуляції і середовищем поширення інформаційних сигналів ЗП; складність точного виявлення місця установки приймального обладнання, на відміну, наприклад, від провідних мікрофонів, які використовують власні провідники для передачі сигналів; відсутність візуальних демаскуючих ознак, так як мережеві ЗП установлюються у звичайних побутових електроприладах. Ці переваги, поряд із відносно низькою вартістю, зумовлюють високу ймовірність застосування мережевих ЗП у системах тривалого контролю акустичних сигналів у виділених приміщеннях.

Основні характеристики деяких мережевих ЗП, які серійно випускаються, наведено в таблиці 2.

Таблиця 2

Основні характеристики МЗП

Тип МЗП	Робочий діапазон частот, кГц	Вид модуляції	Потужність, мВт	Дальність дії, м	Ціна, у. о.
Електромережа-КС	60...300	WFM	7...10	100	200
Електромережа-КМ	60...450	WFM	100...250	300	300
Подовжувач	600...650	WFM	100	250	250
HKG-2221	100...150	FM	10...25	150	220
PK-1295-S	60...200	NFM	10	100	200
SEL-M220-01	200...500	FM	25	200	180
Мережевий модуль	200...800	WFM	150...350	500	320

Заходи щодо захисту інформації від впливу промислового шпигунства. У разі витоку інформації, яка складає комерційну таємницю (КТ), особи, які незаконними методами отримали її, а також особи, що розголосили КТ, зобов'язані відшкодувати власникові КТ заподіяні цими діями збитки. Це означає, що якщо власник не вживав заходів для захисту інформації або інформація не становить комерційної цінності для нього, то в разі її розголошення або використання третіми особами такий володар не має права в судовому порядку вимагати відшкодування завданих йому збитків. Вважається, що основною метою віднесення інформації до КТ є необхідність захисту її від несанкціонованого використання третіми особами, промислового шпигунства, незаконної передачі та поширення, або, інакше кажучи, від недобросовісної конкуренції.

Однією з основних ознак відомостей, що становлять комерційну таємницю, є те, що стосовно цих відомостей вжито заходів щодо забезпечення конфіденційності. Тільки за дотримання цих умов може наступити передбачена законодавством дисциплінарна, матеріальна, адміністративна та кримінальна відповідальність.

Вдаватися до правового режиму КТ слід у випадках недоцільності або неможливості використання норм авторського або патентного права. Уже сьогодні можна й необхідно створювати на підприємствах організаційно-правовий захист інформації, у тому числі КТ, спираючись на норми цивільного законодавства. Заходи забезпечення збереження КТ на підприємстві можуть бути різними, залежно від масштабів підприємства, кількості охоронюваних секретів, їх значущості і т. п. Слід виходити з принципу економічної доцільності, тримаючись золотої середини, так як і надмірне засекречування, і недбале ставлення до секретів здатне викликати втрату прибутків і призвести до збитків.

Однак для того, щоб ті чи інші відомості можна було виділити в загальному потоці інформації та ідентифікувати як комерційну таємницю, власнику інформації, яка складає комерційну таємницю, необхідно виконати таку процедуру: розробити і затвердити Перелік відомостей, що становлять комерційну таємницю, стосовно специфіки організації. Також необхідно затвердити Положення про захист комерційної таємниці, яке б регламентувало діловодство з документами, що містять відомості подібного роду, критерії та порядок віднесення відомостей до інформації, яка складає комерційну таємницю, режим комерційної таємниці та ряд інших питань. Проходження цієї процедури є юридичним фактом, коли інформація законодавчо набуває правового статусу комерційної таємниці і відповідний режим та захист.

Правова система захисту КТ вимагає встановлення на підприємстві відповідних правил роботи з інформацією. Зокрема, у місцях проведення нарад, ділових переговорів поряд із організацією пропускного режиму має бути встановлено відповідну апаратуру, здатну виявляти і блокувати роботу негласних засобів збору інформації, або така апаратура і фахівці з пошуку закладних пристроїв повинні періодично залучатися зі сторони (з організацій, які мають відповідні ліцензії).

Висновки. Таким чином, у результаті проведення аналізу закладних пристроїв встановлено, що основними класифікуючими ознаками для ЗП є: канал передачі і спосіб сприйняття інформації, наявність пристрою управління, зовнішній вигляд і використовуване джерело живлення, причому з усіх типів ЗП найбільш широке розповсюдження в силу своїх переваг знайшли радіозакладні та мережеві закладні пристрої. Запропоновано комплекс заходів щодо протидії промисловому шпигунству, який засновано на поєднанні організаційно-правових та технічних методів і засобів захисту.

ЛІТЕРАТУРА

1. Лопатин В. В. Правовые аспекты информационной безопасности / В. В. Лопатин // Системы безопасности связи и телекоммуникаций. 1998. – № 21. – С. 8–10.
2. Лысов А. В. Промышленный шпионаж в России : методы и средства / А. В. Лысов, А. Н. Остапенко. – СПб. : Лаборатория ППШ, 1994. – 71 с.
3. Хорев А. А. Способы и средства защиты информации / А. А. Хорев. – М. : МО РФ, 1998. – 316 с.
4. Халяпин Д. Б. Основы защиты промышленной и коммерческой информации / Д. Б. Халяпин, В. И. Ярочкин. – М. : ИПКИР, 1994. – 70 с.
5. Технические средства разведки / [под ред. В. И. Мухина]. – М. : РВСН, 1992. – 394 с.

6. Андрианов В. И. Шпионские штучки и устройства для защиты объектов и информации / В. И. Андрианов [и др.]. – СПб. : Лань, 1995. – 272 с.
7. Специальная техника. Системы безопасности и защиты. – М. : Knowledge Express Inc., 1994. – 30 с.
8. Атакуюча спецтехніка «RV» української фірми «ВІЧЕ» // Захист інформації. – 1994. – № 2. – С. 62–76.

 Дата надходження статті до редколегії 25.09.2013 р.

ЯКОВЛЄВ Андрій Альбертович – директор Департаменту охорони державної таємниці, технічного та криптографічного захисту інформації Міністерства доходів і зборів України, м. Київ.
***Коло наукових інтересів*:** техніка, що базується на комп'ютерних системах.

ЛИС Олександр Олександрович – головний спеціаліст Департаменту охорони державної таємниці, технічного та криптографічного захисту інформації Міністерства доходів і зборів України, м. Київ.
***Коло наукових інтересів*:** техніка, що базується на комп'ютерних системах.