УДК 004.681

А.А. Завада,
кандидат технічних наук, старший науковий співробітник,
О.В. Самчишин,
кандидат технічних наук,
Р.В. Сухов

ПІДХІД ДО КЛАСИФІКАЦІЇ СИСТЕМ ТЕХНІЧНОЇ РОЗВІДКИ

Здійснено аналіз класифікацій пристроїв несанкціонованого знімання інформації та визначено їх недоліки. Запропоновано підхід до класифікації систем технічної розвідки, що базується на найбільш загальних для радіотехнічних систем поняттях. Застосування запропонованої класифікації дозволить більш чітко відокремлювати різні аспекти виявлення технічних каналів витоку інформації.

Ключові слова: *технічна розвідка, канали витоку інформації, інформаційно-телекомунікаційна система, закладні пристрої зняття інформації.*

Осуществлен анализ классификаций устройств несанкционированного съема информации и определены их недостатки. Предложен подход к классификации систем технической разведки, основанный на наиболее общих для радиотехнических систем понятиях. Применение предложенной классификации позволит более четко отделять различные аспекты выявления технических каналов утечки информации.

Ключевые слова: *техническая разведка, каналы утечки информации, информационно-телекоммуникационная система, закладные устройства снятия информации.*

The analysis classifications devices unauthorized removal of information and identified their shortcomings. An approach to the classification of technical intelligence systems based on the most common for radio systems concepts. Application of the proposed classification will more clearly separate the different aspects of technical detection channels of information leakage.

Keywords: *technical intelligence channels of information leakage, information and telecommunication systems, embedded devices interception.*

Події, які відбуваються у світі переконливо демонструють, що віднедавна критично важливим державним ресурсом, який забезпечує безпеку країни, стає інформація, яка циркулює в інформаційно-телекомунікаційних системах (ІТС) різного, у тому числі військового призначення. Зазначені системи є невід'ємною компонентою структури управління державою, економікою, фінансами та обороною. Можливість несанкціонованого впливу на них розглядається як пряма загроза національним інтересам країни. Інформація стала товаром та знаряддям, призначеним для отримання прибутку або досягнення політичних цілей. Бурхливий розвиток техніки, технології та інформатики викликав ще більш бурхливий розвиток пристроїв та систем технічної та зокрема радіоелектронної розвідки, у зв'язку із чим завдання захисту інформації набуває все більшої актуальності. Разом з тим, комплексний підхід до захисту інформації гальмується відсутністю чіткої та найбільш загальної класифікації систем радіоелектронної розвідки, зокрема систем технічного шпіонажу.

Постановка проблеми. Існуючі класифікації [1–6] мають обмежений характер саме через розгляд пристроїв (окремих технічних засобів) зняття інформації, а не систем, до складу яких вони входять. Найбільш поширеними є класифікації так званих "жучків" (закладних пристроїв зняття інформації), які базуються на окремих вирваних із загального контексту ознаках, таких як тип інформації, що знімається (аудіо, відео, електронна), метод передачі отриманої інформації (радіоканал, провідна лінія передачі і т.п.), доступність інформації, що передається (відкритий канал передачі, інформація шифрується), потужність передавача, періодичність роботи передавача, тип живлення (тимчасові, стаціонарні), форма переданої інформації (аналогова, цифрова) тощо.

Відсутність системного підходу до вирішення проблеми протидії технічній розвідці (а також витоку інформації за рахунок побічних випромінювань) диктує необхідність розгляду даного питання із врахуванням усіх факторів, що можливо діють у системах, за допомогою яких здійснюється технічна розвідка. Деякі аспекти такого підходу розглянуті у [7; 8], проте дані дослідження носять частковий характер. Таким чином, актуальним науковим завданням є створення розробка такої класифікації пристроїв знімання інформації, яка базуватиметься на найбільш загальних для радіотехнічних систем поняттях.

Виклад основного матеріалу. Класифікацію пристроїв знімання інформації необхідно базувати на розгляді систем технічної розвідки як радіотехнічних систем, в яких функціонують джерела інформації, споживачі цієї інформації, здійснюються електрофізичні перетворення, проводиться передача сигналів, що містять інформацію. Поширення випромінювань проходить у певному середовищі, в якому можуть існувати й інші випромінювання однієї природи із задіяними в системі або іншої природи, які певним чином можуть впливати на функціонування системи в цілому. Окрім цього, елементи системи можуть мати власні побічні випромінювання тощо.

До систем технічної розвідки віднесемо радіотехнічні системи, головною ознакою яких є "вилучення", тобто перехоплення або добування інформації, що циркулює у системах-носіях цієї інформації або є ознакою (одним з параметрів) цих систем, з подальшою передачею отриманої інформації споживачу.

Відповідно до загальноприйнятої класифікації радіосистем, системи технічної розвідки можуть відноситись до різних функціональних класів, зокрема до систем передачі інформації та до систем добування інформації, а також мати змішаний характер.

З метою використання в подальшому, визначимось з певними категоріями:

джерело інформації – система, в якій циркулює інформація або параметр цієї системи, який є об'єктом технічної розвідки (буде „вилучатися");

споживач інформації – система, що реалізує інформацію тим чи іншим чином;

електрофізичний (фізичний) перетворювач інформації (прямий і зворотній) – пристрій для перетворення фізичного поля, яке є інформаційним сигналом, у поле іншої фізичної природи і навпаки;

кодуючий пристрій – пристрій для перетворення сигналу, що містить інформацію, у вид, необхідний для подальшої передачі цього сигналу;

передавач – пристрій, що служить для випромінювання у канал передачі кодованого сигналу, який містить інформацію;

приймач – пристрій, що служить для вилучення інформаційного випромінювання з каналу передачі;

декодер – пристрій для перетворення кодованого сигналу у вид, необхідний для його подальшого електрофізичного перетворення;

опромінювач – джерело активного опромінення;

інформаційний сигнал – сигнал (фізичне поле), що випромінюється джерелом інформації;

побічний сигнал – сигнал однакової із інформаційним сигналом природи, що випромінюється не джерелом інформації;

сигнал, що містить інформацію – сигнал, утворений з інформаційного сигналу після електрофізичного (фізичного) перетворення;

інформаційне випромінювання – випромінювання (фізичне поле), що містить інформацію та поширюється у каналі передачі;

невласне випромінювання – випромінювання однакової із інформаційним випромінюванням фізичної природи, що діє у каналі передачі;

зовнішнє опромінення – опромінення довільної фізичної природи, що різним чином впливає на складові частини системи;

побічне випромінювання – можливе випромінювання складових частин системи довільної фізичної природи;

побічне опромінення – опромінення фізичного перетворювача одного із активним опроміненням виду.

Класифікація систем технічної розвідки повинна базуватись на способі отримання інформації, незалежно від фізичних полів та каналів передачі, що задіюються чи використовуються для вилучення інформації.

В роботі пропонується системи технічної розвідки поділяти на системи з пасивним отриманням інформації, системи напівактивного типу та системи активного отримання інформації (рис. 1). Крім того, можливе застосування мішаних систем, які складаються із вищезазначених.

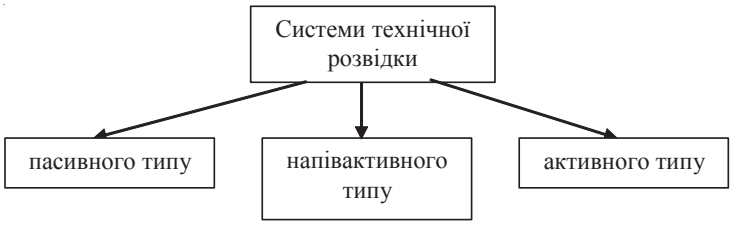

Рис. 1. Класифікація систем технічної розвідки

До систем пасивного вилучення інформації відносяться системи, призначені для пасивного приймання випромінювань, що містять ту чи іншу інформацію (рис. 2). Інформаційний сигнал або інформаційне випромінювання безпосередньо потрапляє у приймач, декодується, перетворюється та потрапляє до споживача.

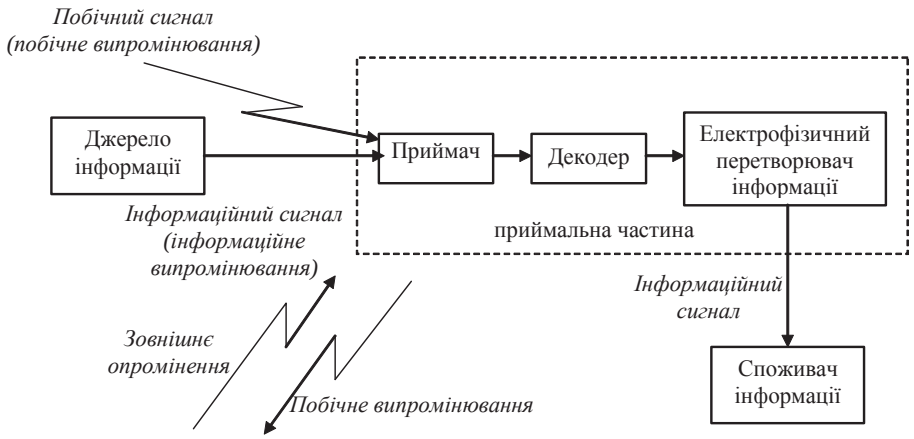

Рис. 2. Структурна схема пасивної системи технічної розвідки

До цього типу можна віднести системи радіоприйому (радіоперехоплень), системи безпосереднього відеоспостереження, направлені мікрофони, а також всі системи, що вилучають інформацію за рахунок побічних випромінювань (наприклад, система перехоплення зображень з екранів моніторів персональних електронно-обчислювальних машин).

До систем напівактивного вилучення інформації відносяться системи, в яких отримання інформації відбувається пасивно з подальшою активною ретрансляцією отриманої інформації (рис. 3). При цьому інформаційний сигнал потрапляє на (в) електрофізичний перетворювач, кодується та передається. У приймальній частині сигнал декодується, змінюється в електрофізичному перетворювачі та потрапляє до споживача.

До систем даного виду належать радіомікрофони, системи відеоконтролю із передачею зображень на відстань, пристрої зняття інформації на основі RFID технологій (в цьому випадку живлення ретранслятора здійснюється ВЧ-накачкою) тощо.

В системах активного вилучення інформації (рис. 4) використовується активне (за допомогою певного технічного засобу) або псевдоактивне (природними або такими, що не створюються даною системою, фізичними полями необхідної природи) опромінення певного фізичного перетворювача, який тим чи іншим чином модулює це випромінювання при дії на перетворювач інформаційного сигналу, та (або) перевипромінює (відбиває) випромінювання, яке вже несе інформацію (є інформаційним). В приймальній частині відбувається виділення інформаційного сигналу, який потрапляє до споживача.

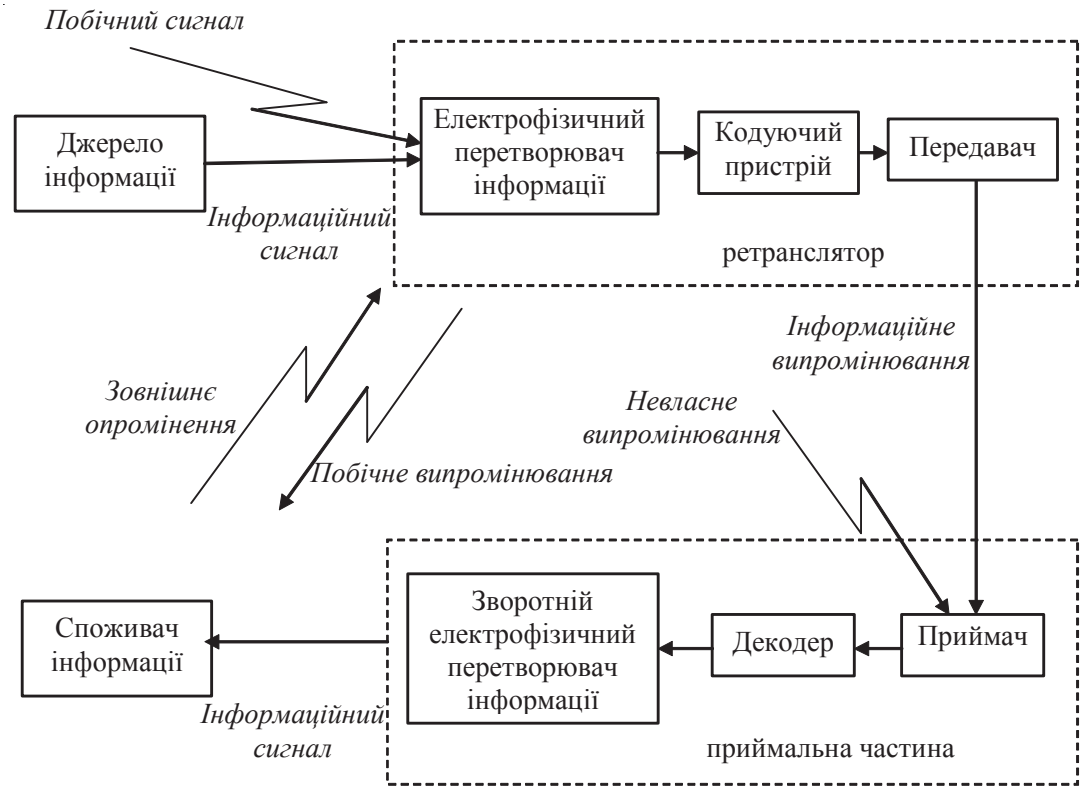

Рис. 3. Структурна схема напівактивної системи технічної розвідки

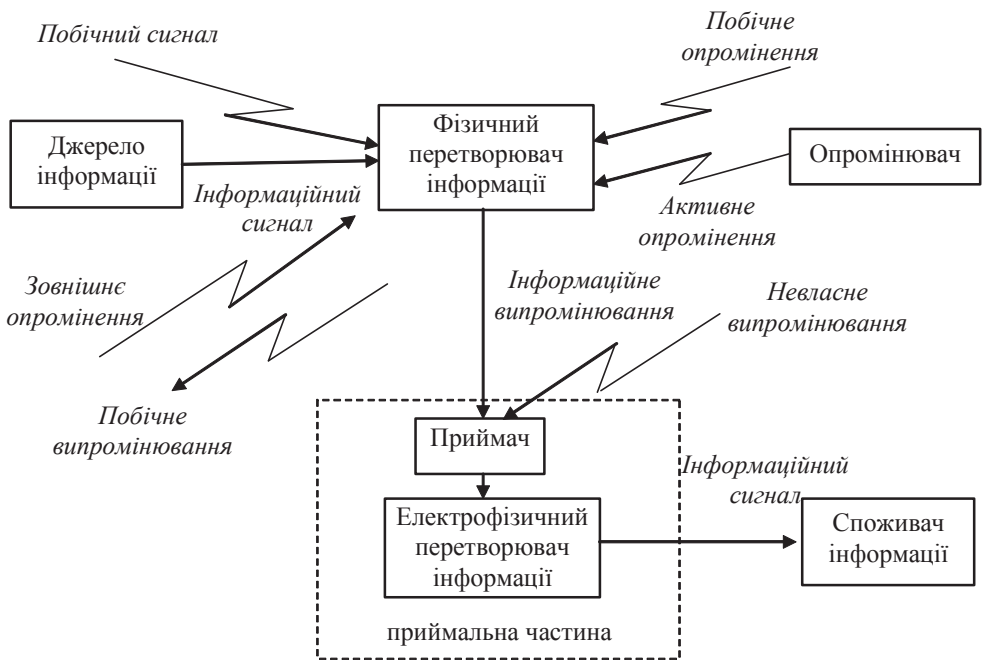

Рис. 4. Структурна схема активної системи технічної розвідки

До таких систем відносяться широко відомі системи лазерного дистанційного аудіоконтролю приміщень та розроблені Терменом системи аудіоконтролю на ендовібраторах (ВЧ-нав'язування) [9, 10].

Очевидно, що в кожному з розглянутих типів систем технічної розвідки необхідно розглядати не лише наведені чинники, а й канали передачі, в яких поширюються ті чи інші випромінювання. Так для інформаційного сигналу, який є акустичним, можливе поширення акустичного коливання у газоподібному, рідинному або твердому середовищі. Поширення електромагнітної хвилі можливе у вільному середовищі або по відповідній лінії передачі (коаксіальна лінія, хвилевід, оптоволоконна лінія та інше).

Висновки. Застосування запропонованої класифікації, із врахуванням фізичних полів, що діють у системах, та каналів передачі, які використовуються в цих системах, дозволить у подальшому виділити та розглянути окремі аспекти захисту інформації, зокрема такі як шляхи виявлення технічного витоку інформації, забезпечення безпеки передачі інформації, протидія засобам технічної розвідки тощо, а також створювати нові перспективні системи технічної розвідки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин – М. : ДМК Пресс, 2010. – 544 с.

2. Методы и средства защиты информации. В 2-х томах / С.В. Ленков, Д.А. Перегудов, В.О. Хорошко; Под ред. В.А. Хорошко. – К. : Арий, 2008. – Том II. Информационная безопасность. – 344 с.

3. Информационная безопасность [Электронный ресурс]. – Режим доступа : http : // www.data.com/lab_tests/intrusion.html.

4. *Конахович Г.Ф.* Защита информации в телекоммуникационных системах. – К. : МК Прес Киев, 2005. – 288 с.

5. Разновидности жучков [Электронный ресурс]. – Режим доступа : http : // www.slezhke.net/03_rz.php.

6. Поиск жучков. Виды прослушивающих устройств [Электронный ресурс]. – Режим доступа : http : // www.intehoffice.ru/security/spy/types.html.

7. *Меньшаков Ю.К.* Защита объектов и информации от технических средств разведки.– М. : Российск. гос. гуманит. ун-т, 2002. – 399 с.

8. *Мельников В.П., Клейменов С.А., Петраков А.М.* Информационная безопасность и защита информации / Под. ред. С.А. Клейменова. – М. : Издательский центр "Академия", 2008. – 336 с.

9. Технические каналы утечки акустической (речевой) информации. [Электронный ресурс]. – Режим доступа : http : // www.analitika.info/stati2.php?page=1&full= block_article150.

10. *Хорев А.А.* Техническая защита информации : учеб. пособие для студентов вузов. В 3 т. – Т. 1. Технические каналы утечки информации. – М. : НПЦ "Аналитика", 2008. – 436 с.