УДК 621.96:004.056

С.Л. Ємельянов,
кандидат технічних наук, доцент

КОМП'ЮТЕРНА РОЗВІДКА ЯК ОСОБЛИВИЙ РІЗНОВИД ТЕХНІЧНОЇ РОЗВІДКИ

Розглянуто сутність, методи та особливості комп'ютерної розвідки як різновиду технічної розвідки.
Ключові слова: *технічна розвідка, комп'ютерна розвідка, технічні канали витоку інформації.*

Рассмотрены сущность, методы и средства компьютерной разведки как разновидности технической разведки.
Ключевые слова*: техническая разведка, компьютерная разведка, технические каналы утечки информации.*

Essence, methods and features of computer intelligence as a kind of technical intelligence are considered.
Keywords*: technical intelligence, computer intelligence, technical leakage paths of information.*

У сучасних комп'ютерних системах та мережах (КСМ) обробляється, накопичується та передається великий обсяг як відкритої інформації, так і інформації з обмеженим доступом (ІзОД).

У зв'язку з цим набула широкого розмаху й діяльність із гласного та негласного видобування інформації з відкритих і захищених КСМ, баз і банків даних, контролю за повідомленнями, які передаються в КСМ, отримання персональних даних користувачів КСМ і іншої цінної комп'ютерної інформації. Для характеристики подібної діяльності стали широко застосовуватися терміни: "комп'ютерне шпигунство", "комп'ютерна розвідка", "інформаційно-аналітична робота в Інтернет", "аналітична розвідка", "комп'ютерний моніторинг" і ін. [1–6].

Проте в нормативно-методичних документах і численних публікаціях з даної тематики дотепер немає єдиного термінологічного тлумачення сутності, завдань, методів і засобів комп'ютерної розвідки (КР) та її співвідношення з іншими видами розвідок, що й зумовлює **актуальність проблеми**, яка розглядається.

Ряд авторів, що спеціалізуються на теорії і практиці економічної розвідки (званої також конкурентною, діловою, комерційною і т.д.), визначають КР як аналітичну обробку величезного обсягу даних з різноманітних відкритих джерел інформації, передовсім із Інтернет. Сутність КР вони вбачають в пошуку і передачі інформації з відкритих джерел "всесвітньої павутини" з подальшою її верифікацією і аналітичною обробкою [1,2].

Термін "аналітична розвідка" вперше з'явився в нормативних документах МВС Росії в 1992 р. для позначення особливої форми діяльності оперативно-розшукових підрозділів [3]. Аналітична розвідка була визначена як розвідувальний пошук, технічна розвідка, комплексне вивчення матеріалів прихованого нагляду і оперативної установки, а також аналіз повідомлень, публікацій і виступів в засобах масової інформації, статистичних даних, відомостей автоматизованих банків даних. КР розглядалася при цьому як один із різновидів аналітичної розвідки, що цілеспрямовано використовується для моніторингу комп'ютерних систем.

Однак більшість авторів [4–6], спираючись на визначення технічної розвідки як несанкціонованого здобування закритої інформації за допомогою технічних засобів та її аналізу [7], небезпідставно відносять КР до одного з видів технічної розвідки (ТР). ТР є однією з найінформативніших, має багату історію та тенденцію до зростання значущості завдяки постійному та бурхливому розвитку науки і техніки, зокрема радіоелектроніки [8].

Відомо, що однією з основних (базових) класифікуючих ознак технічних засобів розвідки (ТЗР) є фізичний принцип побудови їх апаратури (Рис.1), який перекриває всі існуючі й потенційно можливі технічні канали витоку інформації (ТКВІ) з об'єкта розвідки [4–8].

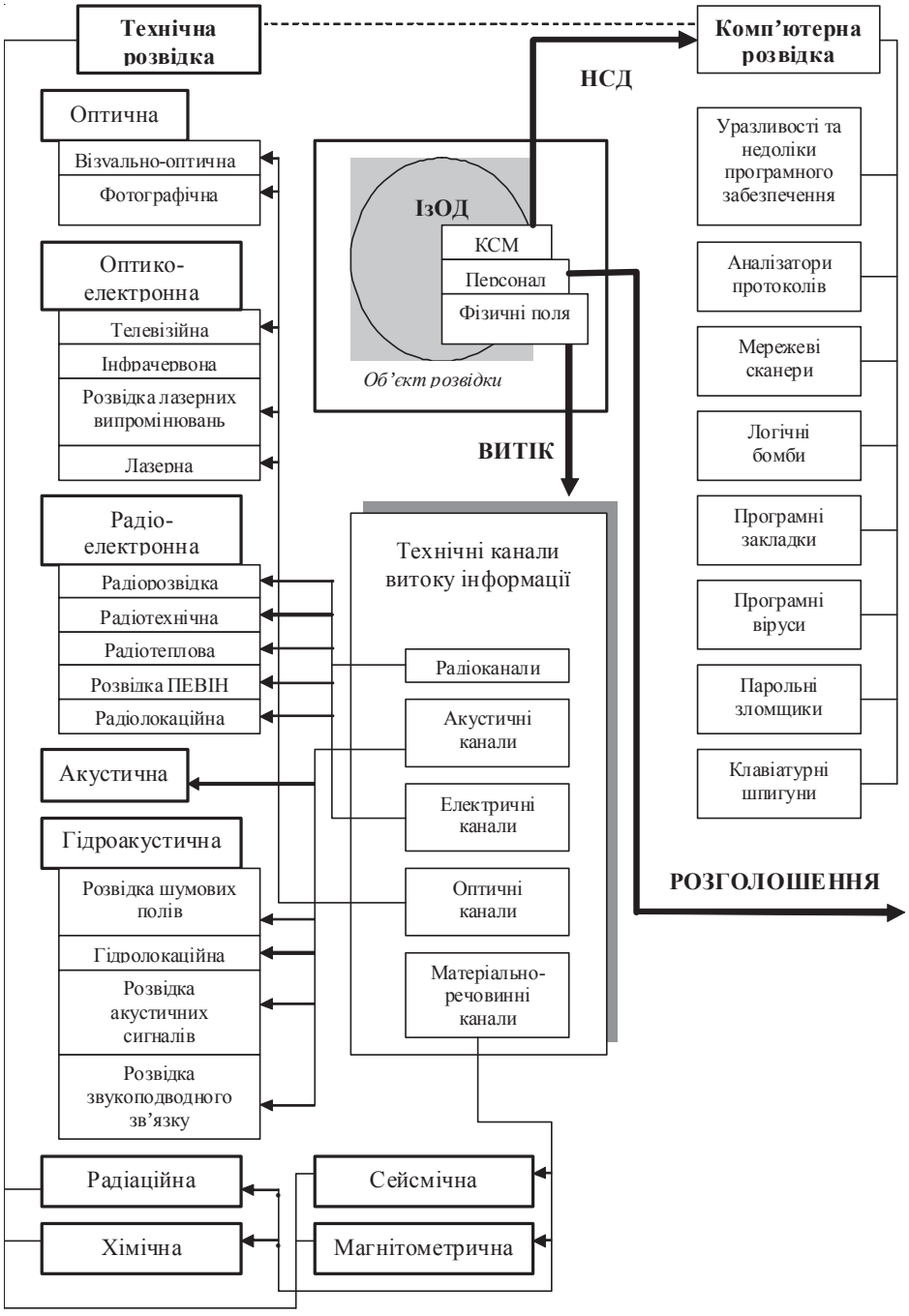

Рис.1. Роль та місце КР у системі добування інформації з типового об'єкта розвідки

Вочевидь, ці фізичні принципи обумовлені методом видобування інформації з різних за фізичною природою джерел інформації, до яких відносять [4, с. 13]:

– будь-які фізичні поля, що виникають або супутні функціонуванню об'єкта розвідки, у тому числі, електромагнітні, акустичні, гідроакустичні та ін.;

– хімічні викиди функціонуючих об'єктів розвідки в довкілля (повітря, ґрунт, рослинність);

– конструктивні особливості і зовнішній вигляд об'єктів розвідки і їх елементів та ін.

Основні ТКВІ також класифікують за фізичними полями, за допомогою яких може поширюватися інформація, що захищається: радіоканали, акустичні, електричні, оптичні і матеріально-речовинні канали, які достатньо добре відомі, систематизовані і вивчені [8].

Оскільки ТЗР, за визначенням, є кінцевим елементом ТКВІ, то розглянуті класифікації ТЗР і ТКВІ за фізичними принципами, що лежать в їх основі, є жорстко корельованими [9]. Інакше кажучи, кожному виду ТР відповідає один або декілька ТКВІ, і навпаки (Рис. 1). Наприклад, радіоелектронна розвідка може видобувати інформацію по радіоканалу і електричному каналу витоку інформації. Акустичний канал витоку інформації використовується акустичною і гідроакустичною розвідками і так далі.

Таким чином, можна припустити, що КР повинна мати власний (окремий) ТКВІ. Тому, наприклад, в роботі [6] автор трактує КР як метод видобування інформації шляхом перехоплення й аналізу побічних електромагнітних випромінювань і наведень (ПЕМВН) засобів ЕОТ, тобто розглядає її як різновид радіоелектронної розвідки, яка, у свою чергу, є одним з видів ТР.

Якщо виходити з класичного визначення каналу витоку як каналу передачі інформації у вигляді: **джерело→фізичне середовище→одержувач** [4, 5, 8], то технічний канал витоку комп'ютерної інформації формально може розглядатися як самостійний канал витоку, оскільки він має усі вказані елементи. Джерело інформації тут КСМ, середовище (тракт) розповсюдження – телекомунікаційні лінії зв'язку (нижній фізичний рівень у моделі відкритих систем OSI [10]), одержувач інформації – інші держави, окремі юридичні або фізичні особи, що видобувають ІзОД із об'єкта розвідки.

Проте існує й інша думка [8, с. 227] про недоцільність виокремлення явищ, що призводять до витоку інформації з КСМ, в окрему групу, створюючи самостійний технічний канал витоку інформації, оскільки багато з них при більш детальному розгляді можуть бути приведені до одного з описаних ТКВІ, наприклад, електромагнітного або матеріально-речовинного.

На наш погляд, **сутність КР** полягає у видобуванні [11]:

– комп'ютерної інформації, яка оброблюється, зберігається та передається в КСМ;

– даних і відомостей про характеристики (параметри) програмних, апаратних і програмно-апаратних комплексів, вживаних в КСМ;

– даних і відомостей про вживані в КСМ методи, способи і механізми захисту інформації;

– персональної інформації про користувачів КСМ.

Виходячи із сутності КР, випливає, що вона не прив'язується до фізичних полів і сигналів (не є видовою або сигнальною), на відміну від інших способів ведення технічної розвідки.

Предметом дослідження КР є не побічні (небажані) ефекти, що неминуче супроводжують функціонування технічних засобів КСМ і лежать в основі утворення ненавмисних ТКВІ, а різні види комп'ютерної інформації, що є результатом якраз штатного функціонування КСМ і реалізації її основного призначення – збору, аналізу, обробки, зберігання, передачі інформації і ін.

Основним **методом** ведення КР є несанкціонований доступ (НСД) до комп'ютерної інформації, що циркулює в КСМ. Проте в термінах комп'ютерної безпеки [12] йдеться не про технічну (комп'ютерну) розвідку і про канали витоку інформації, а, відповідно, про загрози конфіденційності комп'ютерної інформації і про приховані (таємні) канали проникнення в КСМ, які можуть виявлятися як на фізичному (фізичний доступ до елементів КСМ, розкрадання носіїв інформації і т.д.), так і на логічному рівні (відключення або обхід системи захисту, захоплення привілеїв, помилкова маршрутизація потоків даних та ін.).

Способи безконтактного НСД в комп'ютерні системи й мережі ґрунтуються (Рис.1) на використанні недоліків мов програмування, наявності уразливостей ("люків", "дір" і т.д.) у штатному програмному забезпеченні КСМ і застосуванні так званого атакуючого спеціального програмного забезпечення [13, 14]. Його застосування, як правило, передбачає роботу на більш високих рівнях згаданої моделі OSI (канальному, транспортному, мережевому, сеансовому, представницькому і прикладному).

У роботі [4, с. 31] зазначено, що "*...к компьютерной разведке нельзя относить средства активного воздействия на информационные системы противника: почтовые и логические бомбы, электронные черви, SYN-наводнения, атаки типа "Салями", большинство вирусов*".

Проте в КР, як і в технічній розвідці взагалі, можуть застосовуватися *пасивні* і *активні* методи добування інформації. Наприклад, радіолокаційний або лазерний види технічної розвідки, які ґрунтуються на активній локації об'єктів розвідки (або їх елементів) за допомогою випромінювання спеціальних зондуючих сигналів і прийому відбитих відкликів. Інші види ТЗР використовують власне випромінювання об'єктів розвідки в різних частотних діапазонах. Аналогічно при добуванні інформації через ТКВІ можуть застосовуватися як активні (ВЧ-нав'язування, опромінювання лазерним променем поверхні скла, використовування апаратних закладок, радіомікрофонів та ін.), так і пасивні методи перехоплення інформаційних сигналів (ПЕМВН, акустики приміщень і ін.).

Тому і в КР можливе як пасивне перехоплення інформації (прийом і аналіз мережевого трафіку, сканування портів ПК і ін.), так і активні методи добування комп'ютерної інформації за допомогою, наприклад, упровадження в КСМ вірусів, троянців, логічних бомб, що спрацьовують при настанні певних умов або ініціюються сигналами ззовні, програм–клавіатурних шпигунів тощо [13, 14].

На наш погляд, не відносяться до КР:

– вивідування відомостей через персонал КСМ, оскільки це самостійний канал витоку інформації через суб'єкти–носії інформації (***розголошення***);

– аналіз і обробка, у тому числі з використанням комп'ютерних систем, відкритих текстів ЗМІ, Інтернет;

– використання апаратних закладок в засобах ЕОТ;

– передача розвідданих за допомогою КСМ;

– перехоплення та аналіз ПЕВМН засобів ЕОТ;

– фізичне проникнення до елементів КСМ, нагляд за їх роботою, копіювання інформації або розкрадання її носіїв, оскільки це інші методи НСД.

Слід зазначити, що викладений підхід до визначення сутності і методів комп'ютерної розвідки не суперечить чинним нормативно-методичним докумен-

там щодо захисту інформації, а лише доповнює їх, зберігаючи базовий підхід до можливих шляхів (каналів) витоку інформації з об'єкта інформатизації за рахунок [15]: розголошення інформації персоналом; використання технічних засобів розвідки (технічними каналами витоку інформації); НСД до джерел інформації, що захищається.

Висновки

1. Комп'ютерна розвідка є відносно новим і самостійним видом технічної розвідки.

2. З формальної точки зору можуть розглядатися канали витоку комп'ютерної інформації як самостійні технічні канали розповсюдження ІзОД з об'єкта інформатизації, проте вони потребують подальшого дослідження.

3. Сутність комп'ютерної розвідки полягає в добуванні:

– комп'ютерної інформації, яка оброблюється, накопичується та передається в КСМ;

– даних і відомостей про характеристики (параметри) програмних, апаратних і програмно-апаратних комплексів, застосовуваних в КСМ;

– даних і відомостей про застосовувані в КСМ методи, способи і механізми захисту інформації;

– персональної інформації про користувачів КСМ.

4. Основним методом ведення комп'ютерної розвідки є несанкціонований безконтактний доступ до комп'ютерної інформації, що циркулює в КСМ.

5. Комп'ютерна розвідка може вестися за допомогою як активних, так і пасивних методів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Доронин А.И.* Бизнес-разведка / А.А. Доронин.– М. : "Ось-89", 2003.–384 с.

2. Мисюк С. Компьютерная разведка : взгляд на сайт компании из недр Интернета [Електронний ресурс]. – Режим доступу : http : // www.daily.sec.ru/dailypblshow.cfm?rid= 17&pid=8872.

3. *Скрыль С.В.* Аналитическая разведка в оценке угроз информационной безопасности / С.В. Скрыль, В.В. Киселев // Системы безопасности. – 2003.– № 6(48). – С. 96–97.

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

5. *Халяпин Д.Б.* Защита информации. Вас подслушивают? Защищайтесь! / Д.Б. Халяпин. – М. : НОУ ШО "Баярд", 2004. – 432 с.

6. *Ржавский В.К.* Информационная безопасность : практическая защита информационных технологий и телекоммуникационных систем : Учебное пособие / В.К. Ржавский .– Волгоград : ВолГУ, 2002. – 122 с.

7. Захист інформації. Технічний захист інформації. Терміни і визначення. ДСТУ 3396.2-97. – [Дійсний від 01.07.1997 р.]. – Національний стандарт України.

8. *Хорошко В.А.* Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – Юниор, 2003. – 504 с.

9. *Емельянов С.Л.* Техническая разведка и технические каналы утечки информации / С.Л. Емельянов // Системи обробки інформації. – 2010. – Вип. 3(84). Інформаційна та економічна безпека : Харківський університет Повітряних Сил ім. І. Кожедуба. – С. 20–23.

10. Протоколы информационно-вычислительных сетей : Справочник / Под общ. ред. И.А. Мизина, А.П. Кулешова.– М. : Радио и связь,1990. – 504 с.

11. *Ємельянов С.Л.* Сутність та методи комп'ютерної розвідки / С.Л. Ємельянов // Право і безпека. – 2010.–№4 (36). – С. 262–266.

12. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу : Затв. наказом ДСТСЗІ від 28 квітня 1999 р. / [Електронний ресурс]. – Режим доступу : http : // www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id= 40396&cat_id=38835.

13. *Анин Б.Ю.* Защита компьютерной информации / Б.Ю. Анин. – СПб. : БХВ-Петербург, 2000. – 384 с.

14. *Красноступ Н.* Шпионские программы и новейшие методы защиты от них / Н. Красноступ, Д. Кудин // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : Науково-технічний збірник. – НТУУ "КПІ", ДСТС ЗІ СБУ. –2004. – Вып. 9. – С. 67–75.

15. *Ємельянов С.Л.* Шляхи і канали витоку інформації з типового об'єкту інформатизації / С.Л. Ємельянов, В.В. Носов // Право і безпека. – Науковий журнал. – 2009. –№ 1. – С. 273–279.

Отримано 13.03.2012