УДК 316.776:351.741

С. Л. ЄМЕЛЬЯНОВ,
кандидат технічних наук, доцент,
завідувач кафедри правової інформатики
Одеської національної юридичної академії,
член-кореспондент Академії зв'язку
В. В. НОСОВ,
кандидат технічних наук, доцент,
професор кафедри інформаційної безпеки
Харківський національний університет внутрішніх справ

ШЛЯХИ І КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ З ТИПОВОГО ОБ'ЄКТА ІНФОРМАТИЗАЦІЇ

Загальна кількість інформації, що зростає за експоненціальним законом [1], посилення вимог щодо її зберігання, пошуку й обробки, збільшення трафіку і швидкості передачі інформації зумовили появу інформаційних систем (далі – ІС) різних поколінь і призначення. ІС становить організаційно-технічну систему, що об'єднує обчислювальну систему як сукупність апаратно-програмних засобів, фізичне середовище, персонал та оброблювану інформацію. Сьогодні термін «інформаційна система» охоплює автоматизовані системи, комп'ютерні мережі, системи зв'язку [2], інформаційно-телекомунікаційні системи [3] тощо.

У певному розумінні, вказані вище поняття узагальнює *об'єкт інформатизації* - сукупність інформаційних ресурсів, засобів і систем обробки інформації, використовуваних відповідно до заданої інформаційної технології, засобів забезпечення об'єкта інформатизації, приміщень або об'єктів (будівель, споруд, технічних засобів), у яких вони встановлені, або приміщення й об'єкти, призначені для ведення конфіденційних переговорів [4].

Під інформаційною загрозою об'єкта інформатизації, що захищається, розуміють виникнення такого явища або події, в результаті яких можуть бути порушені одна (або декілька) базових властивостей інформації, що циркулює на ньому, – конфіденційність, цілісність, доступність. При цьому конфіденційність *(information confidentiality)* – суб'єктивно визначувана властивість інформації, що вказує на необхідність введення обмежень щодо кола суб'єктів, які мають доступ до неї.

Серед численних інформаційних загроз об'єкта інформатизації, за даними багатьох статистичних досліджень [5], домінують загрози конфіденційності інформації, під час реалізації яких інформація з обмеженим доступом (далі – ІзОД) стає відомою особам, що не мають права доступу до неї, тобто відбувається *витік інформації, що захищається, з об'єкта інформатизації.*

Проте в нормативно-методичних документах і численних публікаціях з даної тематики до сьогодні відсутнє єдине визначення можливих шляхів (способів) і каналів витоку інформації, що й обумовлює *актуальність даної проблеми.*

Мета статті - визначення і систематизація можливих шляхів і каналів витоку інформації стосовно типового об'єкта інформатизації.

Базовий термін «витік інформації» багато авторів трактують по-різному. Так, В. І. Ярочкін відзначає, що «*витік – це безконтрольний вихід конфіденційної інформації за межі організації або кола осіб, яким вона була довірена, і яка здійснюється різними технічними каналами*» [6], тобто розуміє витік як фізичний процес, що прив'язується до технічних каналів поширення інформаційних сигналів. У цій же роботі автор називає на три основні шляхи порушення конфіденційності інфо-

рмації: розголошування; власне витік інформації (технічні канали витоку); несанкціонований доступ.

За державними стандартами, витік інформації *(information leakage)* – це *неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання* [7; 8]. Тут до витоку також відносять ненавмисні (технічні) канали (unpremeditated (technical) channel of information leakage) та навмисні (технічні) канали витоку (premeditated (technical) channel of information leakage).

А. О. Торокін наводить більш загальне, на наш погляд, визначення витоку інформації – *несанкціоноване перенесення інформації від її джерела до зловмисника* [9]. Шлях такого несанкціонованого перенесення інформації автор називає каналом витоку і відзначає, що витік інформації можливий шляхом її розголошування, втрати носія і технічними каналами.

В. О. Хорошко й А. А. Чекатков також говорять про існування на логічному рівні різних каналів витоку інформації, що істотно відрізняються за типом використовуваного джерела інформації, шляхами (трактами) її передачі (розповсюдження), особливостями задіяних способів і засобів прийому інформації тощо [10].

У російському стандарті [11] виділено три основні напрями захисту інформації від її витоку за рахунок: розголошування; несанкціонованого доступу (далі – НСД); отримання іноземною технічною розвідкою (ІТР).

При цьому слід зазначити, що єдине розуміння можливих шляхів НСД також відсутнє. За В. І. Ярочкіним, несанкціонований доступ - це протиправне навмисне отримання конфіденційної інформації особою, що не має права доступу до секретів, що охороняються, яке може реалізовуватися різними способами: співпраця, вивідування, підслуховування, спостереження, розкрадання, копіювання, підробка, перехоплення, фотографування тощо.

В українських стандартах [7; 8] визначаються інші шляхи НСД: підключення до апаратури і ліній зв'язку, маскування під зареєстрованого користувача, подолання засобів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв і програм та впровадження комп'ютерних вірусів.

На наш погляд, *під витоком інформації слід розуміти неконтрольоване розповсюдження інформації, яке може призвести до її несанкціонованого отримання*. Наявність каналів витоку інформації є необхідною, але недостатньою умовою витоку інформації. Таким чином, витік інформації слід розуміти не тільки як фізичний процес її поширення, але і як конкретний результат такого поширення. Наприклад, за відсутності джерела та / або одержувача інформації (порушника, зловмисника тощо) чи за відсутності у останнього адекватних методів і засобів добування інформації витоку інформації може і не відбутися.

Розглянемо з цих позицій класичний інформаційний канал: **джерело → фізичне середовище → одержувач**.

Багато сучасних об'єктів інформатизації мають у своєму складі технічні засоби прийому, обробки, зберігання і передачі інформації (ТЗПІ), які безпосередньо обробляють інформацію, що захищається (ЕОМ та їх мережі, АТС для ведення секретних переговорів, системи оперативно-командного і гучномовному зв'язку, системи звукопідсилення тощо) [12; 13].

Окрім вищезгаданих основних ТЗПІ, на об'єкті інформатизації можуть також знаходитися ТЗПІ, що не беруть участі безпосередньо в процесі обробки ІзОД, але знаходяться з ними в одному приміщенні, – так звані ДТСЗ - допоміжні технічні системи і засоби. До них належать: технічні засоби відкритого телефонного, гучномовного зв'язку, системи пожежної й охоронної сигналізації, радіотрансляції, електропобутові прилади тощо, а також самі приміщення, призначені для обробки ІзОД.

Структура типового (базового) об'єкта інформатизації в узагальненому вигляді показана на рис.1.

На об'єкті інформатизації, що захища-

ється, де циркулює ІзОД, є виділене приміщення (ВП), в якому можуть проводитися секретні переговори (наради), встановлені як основні (ОТСЗ), так і допоміжні (ДТСЗ) ТЗПІ. Окремо виділена обчислювальна система (ОС), що включає апаратне (АЗ) і програмне (ПЗ) забезпечення, які безпосередньо обробляють ІзОД, а також персонал, що має доступ у ВП (наприклад, той, який експлуатує ТСПІ). Також на об'єкті інформатизації створюються й обробляються різні документи (як у паперовому, так і в електронному вигляді) і є відходи виробничої діяльності (відпрацьовані мобільні носії, чернетки документів, списане устаткування тощо). Навколо об'єкта інформатизації знаходиться контрольована зона (далі – КЗ) - територія (будівля, група будівель, приміщення), де виключене неконтрольоване перебування сторонніх осіб і транспортних засобів.

Вочевидь, що *джерелами інформації* на такому об'єкті потенційно можуть бути усі розглянуті елементи: люди (персонал), документи, ТЗПІ (ОТСЗ і ДТСЗ), апаратно-програмне забезпечення ОС, технічні засоби забезпечення виробничої і трудової діяльності, продукція і відходи виробництва та ін.

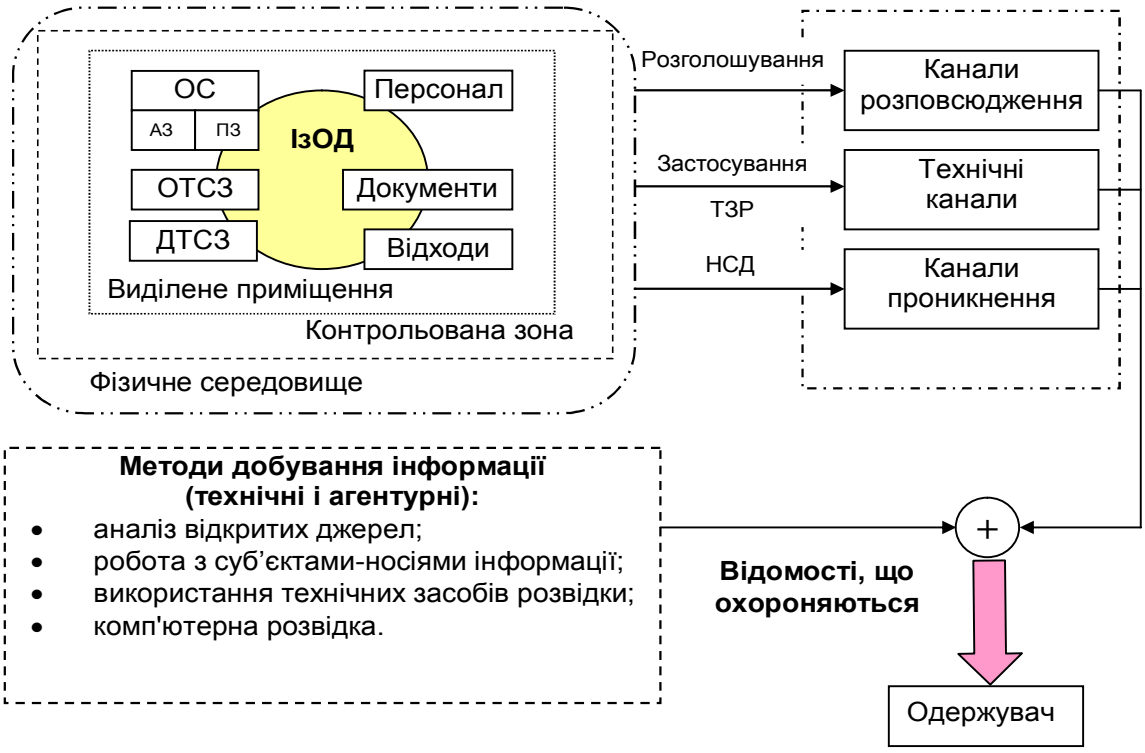

Рис. 1. Шляхи і канали витоку інформації з об'єкта інформатизації

Окрім них, носієм інформації можуть бути фізичні поля, що виникають при циркуляції інформації. Ці поля існують і поширюються в різних за природою фізичних середовищах. Середовищами поширення інформаційних сигналів, що породжуються фізичними полями, можуть бути лінії зв'язку, сигналізації, управління, енергетичні мережі, інженерні комунікації і споруди, світлопроникні елементи будівель і споруд, повітряне, водне та інші середовища, а також ґрунт, рослинність тощо.

Під *каналом витоку інформації* розумітимемо фізичний шлях несанкціонованого поширення інформації. Для даного об'єкта захисту поширення (перенесення) інформації за межі КЗ можливо шляхом:

– розголошування;

– застосування технічних засобів розвідки (ТЗР);

– несанкціонованого доступу до дже-

рел інформації (НСД).

Таким чином, можна говорити про три можливі види каналів витоку інформації, що відповідають вказаним шляхам:

– канали поширення;

– технічні канали;

– канали проникнення.

Розголошування - це навмисні або необережні дії персоналу з носіями інформації, які можуть призвести до ознайомлення з інформацією суб'єктів, що не мають прав доступу. Воно може виражатися в повідомленні, переданні, пересиланні, копіюванні, розкраданні, публікації та інших формах. Реалізується розголошування за формальними і неформальними каналами поширення (комунікативними каналами) (рис. 2). Основним, але не єдиним носієм інформації (далі – НІ) в такому каналі витоку є фізична особа (людина).

Рис. 2. Витік інформації через комунікативні канали

Якщо поширення (перенесення) інформації або її носіїв проводиться за допомогою технічних засобів, то такий канал називають технічним каналом витоку інформації (далі – ТКВІ). Основними НІ в ТКВІ є фізичні поля, в яких інформація знаходить своє відображення у вигляді інформаційних (небезпечних) сигналів. На логічному рівні можна записати:

ТКВІ = НІ+СЕРЕДОВИЩЕ+ТЗР

Узагальнена структура типового технічного каналу витоку інформації наведена на рис. 3.

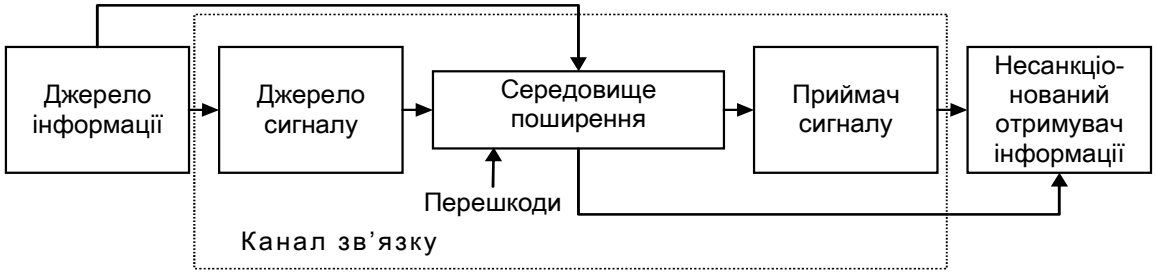

Рис. 3. Структура типового технічного каналу витоку інформації

Звідси бачимо, що в процесі розповсюдження інформація може міститися як на носіях-джерелах інформації, так і на носіях-переносниках інформації. У широкому сенсі носій інформації – це фізична особа або матеріальний об'єкт, зокрема, фізичне поле, в яких інформація знаходить своє відображення у вигляді символів, образів, сигналів, технічних рішень і процесів [4].

Слід зазначити, що ненавмисні (випадкові) ТКВІ досить добре систематизовані, класифіковані і описані. Наприклад, залежно від фізичної природи виникнення інформаційних сигналів ТКВІ поділяють на:

– радіоканали (електромагнітні випромінювання радіодіапазону);

– акустичні канали (поширення звукових коливань в будь-якому звукопровідному матеріалі);

– електричні канали (небезпечна напруга і струми в струмопровідних комунікаціях);

– оптичні канали (електромагнітні випромінювання в інфрачервоній, видимій, ультрафіолетовій частинах спектру);

– матеріально-речові канали (папір, фото, магнітні носії, відходи тощо) [10].

Менш дослідженими є навмисні (організовані) ТКВІ, які утворені апаратними закладками, що працюють за різними фізичними принципами. Мабуть, цим можна пояснити той факт, що деякі автори взагалі описують такі ТКВІ як методи і засоби несанкціонованого отримання інформації технічними каналами, тобто як шляхи і канали НСД [10].

Трактування НСД як протиправного навмисного отримання інформації, що захищається, зацікавленим суб'єктом із порушенням установлених правовими документами або власником інформації прав чи правил доступу до інформації, що захищається, є, на наш погляд, дуже «розмитим» і має юридичну спрямованість, що і обумовлює дуже широкий спектр можливих способів НСД (рис. 4) [14]. Усі раніше розглянуті шляхи і канали витоку інформації також підпадають під таке визначення, оскільки в них здійснюється несанкціоноване перенесення інформації до суб'єкта-одержувача.

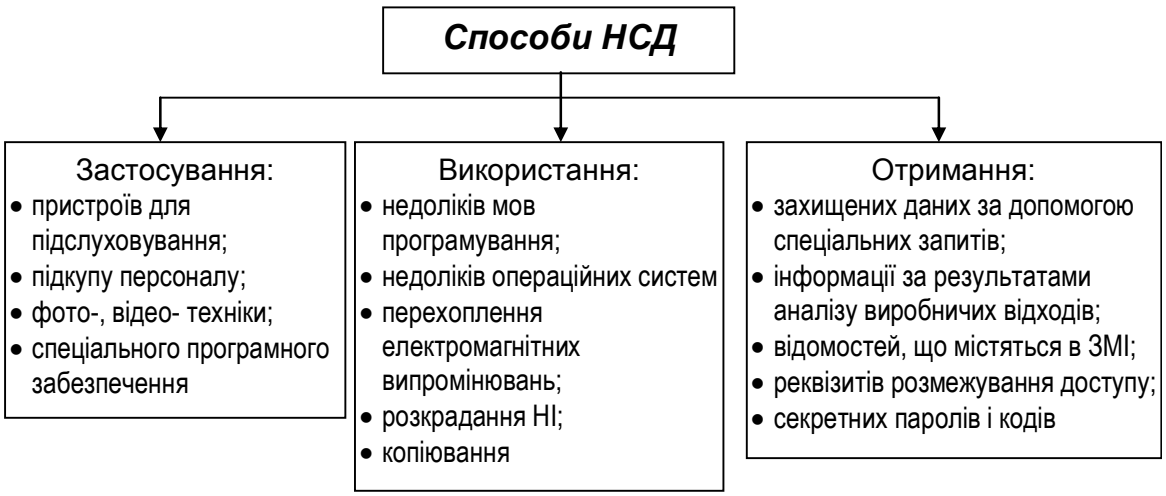

Рис. 4. Можливі способи НСД

Очевидно, що тільки звуження предметної сфери щодо об'єкта, що захищається, дозволить конкретизувати поняття НСД і його можливих способів. Наприклад, якщо розглядати як об'єкт, що захищається, інформаційно-обчислювальні системи і мережі, то в термінах комп'ютерної безпеки загроза порушення конфіденційності означає, що порушник (користувач) дістає можливість протиправного (в обхід встановлених правил розмежування доступу) отримання закритої інформації, яка зберігається або передається в комп'ютерній системі (мережі) [15]. Реалізація НСД (unauthorized access to information) або організація каналів проникнення в цьому випадку можлива як за рахунок штатних засобів системи (використання вразливостей штатного ПЗ), так і за рахунок спеціального ПЗ: програмних закладок, клавіатурних «шпигунів», парольних «зломників», комп'ютерних вірусів, мережевих

сканерів, аналізаторів протоколів тощо [18; 19].

Слід зазначити, що в теорії інформатики інформація трактується як динамічний продукт взаємодії даних (зареєстрованих сигналів) і методів доступу та обробки даних у контексті цієї взаємодії [20]. Тому доцільно розглядати канали витоку інформації в контексті можливих методів і засобів отримання інформації, показаних на рис. 1. При цьому слід враховувати, що пропонований багатьма авторами [6; 9; 10] розподіл методів розвідки на агентурні і технічні є достатньо умовним, оскільки отримання інформації (відомостей, що охороняються) агентурними методами часто супроводжується використанням портативних ТЗР, а технічна розвідка, особливо аналіз її результатів, проводиться людьми.

Вищезазначене дозволяє зробити такі **висновки:**

1. Предметна сфера поняття «витік інформації» є дещо звуженою.

2. Як канали витоку інформації, окрім технічних каналів, що традиційно розглядаються в цьому контексті, доцільно аналізувати також канали поширення інформації (за рахунок розголошування) і канали проникнення (за рахунок НСД) до комп'ютерних систем і мереж. Саме за допомогою цих каналів на типовому об'єкті інформатизації сьогодні реалізуються численні загрози конфіденційності інформації.

3. Навпаки, предметна область поняття «НСД» дуже розпливчата і потребує конкретизації, як це зроблено, наприклад, стосовно інформаційно-обчислювальних систем і мереж.

4. Розгляд та аналіз потенційних каналів витоку інформації доцільно пов'язувати з можливими методами отримання інформації в контексті їх взаємодії у процесі отримання відомостей, що охороняються.

Література

1. Гаврилов О. А. Курс правовой информатики : учеб. для вузов / Гаврилов О. А. – М. : Издательство НОРМА (Изд. группа НОРМА–ИНФРА–М), 2002.– 432 с.
2. Про затвердження положення про технічний захист інформації в Україні : Указ Президента України від 27 верес. 1999 р. № 1229 // Офіційний вісник України. – 1999. – № 39. – Ст. 1934 (зі змінами та доповненнями на 06.10.2000 р.).
3. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05 лип. 1994 р. // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286 (зі змінами та доповненнями на 31 трав. 2005 р.).
4. ГОСТ Р 51275–99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
5. Скиба В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. – СПб. : Питер, 2008. – 320 с.
6. Ярочкин В. И. Информационная безопасность / Ярочкин В. И. – М. : Международные отношения, 2000. – 400 с.
7. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.1996 р. № 423.
8. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.1997 р. № 200.
9. Торокин А. А. Инженерно–техническая защита информации : учеб. пособ. для студ., обуч. по спец. в обл. информ. безопасности. – М. : Гелиос АРВ, 2005. – 960 с.
10. Хорошко В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. – М. : Юниор, 2003. – 504 с.
11. ГОСТ Р – 50922-96. Защита информации. Основные термины и определения.
12. Хорев А. А. Защита информации от утечки по техническим каналам. – Ч. 1. Технические каналы утечки информации [Електронний ресурс] / А. А. Хорев. – Режим доступу : http://www.analitika.info/kanalutechki.
13. Бузов Г. А. Защита от утечки информации по техническим каналам : учеб. пособ. / Бузов Г. А., Калинин С. В., Кондратьев А. В.– М. : Горячая линия – Телеком, 2005. – 416 с.

14. Соколов А. В. Защита от компьютерного терроризма : справоч. пособ. / А. В. Соколов, О. М. Степанюк. – СПб. : БХВ – Петербург; Арлит 2002. – 496 с.

15. Романец Ю. В. Защита информации в компьютерных системах и сетях / [под ред. В. Ф. Шаньгина]. – М. : Радио и связь, 1999. – 328 с.

16. ГОСТ Р – 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа. Общие технические требования.

17. НД ТЗИ 1.1-003-99.Терминология в области защиты информации в компьютерных системах от несанкционированного доступа.

18. Красноступ Н. Шпионские программы и новейшие методы защиты от них / Н. Красноступ, Д. Кудин // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науч.-техн. зб. – 2004. – Вип. 9. – С. 67–75.

19. Емельянов С. Л. Некоторые аспекты защиты от несанкционированного доступа в информационных сетях // Електромашинобудування та електрообладнання : міжвідомчий наук.-техн. зб. – 2008. – Вип. 70. – С. 156–159.

20. Информатика для юристов и экономистов / Симонович С. В. и др. – СПб. : Питер, 2001. – 688 с.

Надійшла до редколегії 14.01.2009

Анотації

У статті зазначена відсутність єдиного термінологічного тлумачення можливих шляхів і каналів витоку інформації. Зроблено системний аналіз можливих шляхів і каналів витоку інформації стосовно типового об’єкта інформації. Наведено висновки та рекомендації щодо визначення та трактування термінів «шляхи і канали витоку інформації».

В статье отмечено отсутствие единого терминологического толкования возможных путей и каналов утечки информации. Проведен системный анализ возможных путей и каналов утечки информации относительно типового объекта информатизации. Приведены выводы и рекомендации относительно определения и трактовки терминов «пути и каналы утечки информации с типового объекта информации».

Absence of single terminology interpretation of possible ways and channels of information leakage is marked. The analysis of possible ways and channels of information leakage is conducted on the standard object of informatization. Conclusions and recommendations are resulted in relation to determination and interpretation of terms: ways and channels of information leakage from the standard object of informatization.