УДК 316.776:351.741:34:650.0128

І.О. Громико

Харківський національний університет внутрішніх справ, Харків

ВИЗНАЧЕННЯ СЕРЕДОВИЩА ПОШИРЕННЯ ІНФОРМАЦІЇ ТА ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ

На підґрунті Загальної парадигми інформації визначений новий підхід у системі технічного захисту інформації до таких базових понять, як середовище поширення інформації та технічні канали витоку інформації. Середовищу поширення інформації відведена роль середовища впливу своїми чинниками на зміну параметрів та характеристик носіїв інформації, а технічний канал витоку інформації, у такому разі, перетворився на паразитний ланцюжок носіїв інформації, що закінчується правопорушником або його розвідувальною апаратурою.

Ключові слова: *інформація, носії інформації, захист інформації, канали витоку, середовище поширення.*

Вступ

Узагальнення теорії захисту інформації в комп'ютерних (автоматизованих) системах, що увібрала світовий досвід боротьби з правопорушеннями в інформаційній сфері, і поширення її на загальну інформаційну сферу дозволило сформулювати загальну парадигму захисту інформації у наступному вигляді [1 – 3]: «**Інформація вважається захищеною, якщо при її переміщенні дотримується режимна адекватність комунікабельних носіїв інформації».**

Дослідження властивостей інформації показують, що інформація завжди існує на носії інформації. Носій інформації це матеріальний об'єкт, що містить інформацію, яка підлягає захисту від загроз: витоку, можливості блокування або порушення цілісності [4].

Основний матеріал

Реально, інформація поширюється не у якомусь загальному середовищі, а поступово переходить з одного носія інформації в інший. Тому й швидкість поширення інформації від джерела до отримувача визначає тій носій, який переносить інформацію повільніше.

Прийнято вважати, що середовищем поширення носіїв інформації можуть бути лінії зв'язку, сигналізації, управління, енергетичні мережі, устаткування, інженерні комунікації і споруди, що захищають будівельні конструкції, а також світлопроникні елементи будівель і споруди (отвори), повітря, водне середовище, ґрунт, рослинність і т.п. [5, 6].

Загальна парадигма захисту інформації конкретизує абстрактне уявлення про середовище поширення:

"Інформація, у вигляді сигналів поширюється по ланцюжку (послідовному, послідовно-паралельному та ін.) носіїв інформації від джерела до одержувача. Середовищу (навколишньому середовищу) відводиться тільки роль впливу на параметри носіїв інформації".

Під дією чинників середовища (що оточує) змінюються ті або інші параметри носія інформації аж до видозміни самого носія (приклад фазового переходу).

Навколишнє середовище включає природне середовище і штучне (техногенне) середовище [6]. З врахуванням того, що людина офіційно розглядається як носій інформації [7, 8], найбільш коректним варіантом визначення терміну „середовище” є варіант [7]:

“**середовище** це:

1. Речовина і/чи поле, що оточують розглянутий об'єкт (у нашому випадку – носій інформації. – *І. Громико*).

2. Природні тіла і явища, з якими організм людини знаходиться в прямих чи непрямих взаєминах.

3. Сукупність фізичних (природних), природно-антропогенних і соціальних факторів життя людини”.

Це дозволяє сформулювати визначення каналу витоку інформації і охарактеризувати процес утворення каналу витоку інформації.

У багатьох ведучих авторських роботах під "каналом витоку інформації", а також “технічним каналом витоку інформації” розуміється наступне [9 – 15]:

1. Канал витоку інформації – **потенційні напрями** несанкціонованого доступу до інформації, обумовлені архітектурою, технологічними схемами функціонування засобів електронно-обчислювальної техніки, а також невиконанням організаційно-режимних заходів [9].

2. Канал витоку інформації (технічний) – сукупність джерела небезпечного сигналу, **середовища поширення носія небезпечного сигналу** і засобу розвідки [10].

3. Під технічним каналом витоку інформації розуміють сукупність об'єкту розвідки, технічного засобу розвідки, за допомогою якого здобувається інформація про цей об'єкт, і фізичного **середовища, в якому поширюється інформаційний сигнал** [11, 12].

4. Канал витоку інформації [Covert channel] – канал комунікації, що дозволяє процесу передавати інформацію шляхом, що порушує безпеку системи [13]. Технічний канал витоку інформації [technical channel of information loss] - сукупність носія інформації, **середовища поширення або речовин** і реального (або можливого) засобу розвідки, яка привела (може привести) до витоку інформації [24].

5. Витік інформації – несанкціоноване перенесення інформації від її джерела до зловмисника [25]. Канал витоку інформації – фізичний шлях несанкціонованого поширення носія з інформацією, що захищається, від її джерела до зловмисника. Якщо поширення інформації відбувається за допомогою технічних засобів, то відповідний канал називається технічним каналом витоку інформації (рис. 1) [14].

6. Під каналом витоку інформації розумітимемо фізичний шлях від джерела конфіденційної інформації до зловмисника [15]. Відносно сигналу цей шлях містить послідовний ланцюг з елементів: "джерело - джерело сигналу – **середовище** – приймач - зловмисник"[15].

Таким чином, можна побачити загальну тенденцію. Автори при визначенні **каналу витоку інформації** застосовують поняття **напрямів** та **шляхів -** взагалі, але якщо виникає потреба надати конкретний образ цьому шляху та напряму (наприклад, при визначенні технічного каналу витоку інформації), автори вводять поняття **середовища, по якому поширюються сигнали**. Як правило, схеми технічних каналів витоку інформації зводять до варіантів рис. 1.

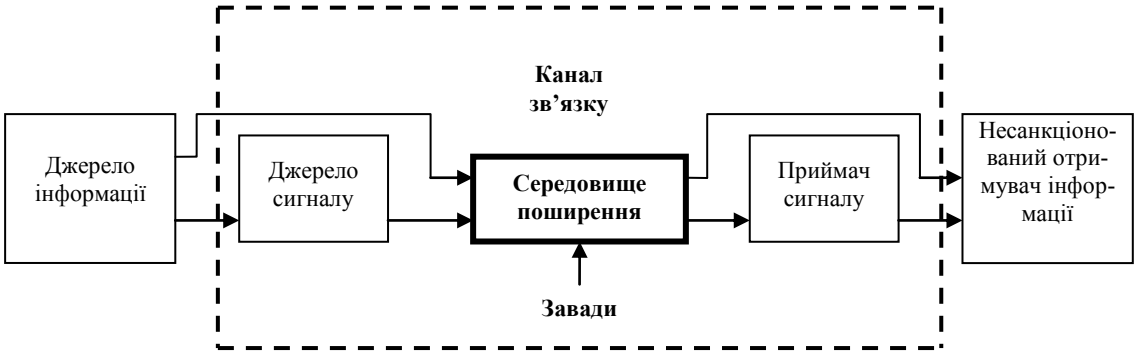

Рис. 1. Структура технічного каналу витоку інформації [14].

Враховуючи, положення Загальної парадигми захисту інформації про те, що "під дією чинників середовища, що оточує носії інформації, змінюються їх параметри, які, в свою чергу, впливають на процес поширення сигналу", узагальнена структурна схема каналу витоку інформації виглядає таким чином (рис. 2). Тоді структурна схема (варіант) технічного каналу витоку інформації буде (рис. 3).

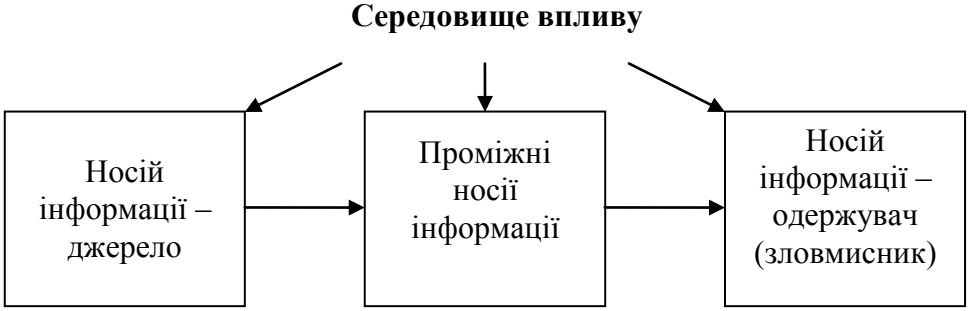

Рис. 2. Узагальнена структурна схема каналу витоку інформації

Одинарними і подвійними стрілками показані напрями поширення сигналів. Подвійні стрілки - напрями поширення сигналів після перетворення. Товстими стрілками показано вплив чинників середовища на значення параметрів носіїв інформації.

Звідси, **процесом утворення каналу витоку інформації** називається утворення паразитної (небажаної) послідовності (ланцюжка) носіїв інформації, один (або декілька) з яких може бути правопорушником або його спеціальною апаратурою.

Канал витоку інформації – паразитний ланцюжок носіїв інформації, один (або декілька) з яких може бути правопорушником або його спеціальною апаратурою.

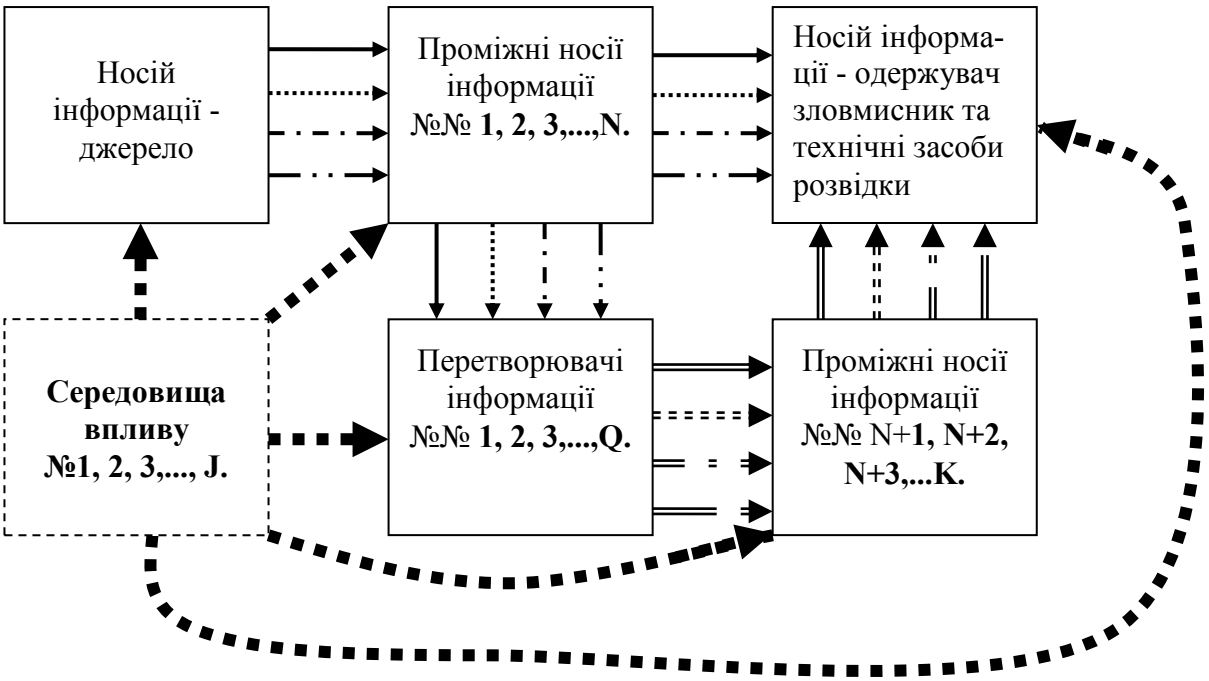

Рис. 3. Структурна схема технічного каналу витоку інформації

2. Запропоновано розглядати навколишнє середовище як таке, що бере участь в процесі поширення сигналів тільки шляхом впливу (дії) її чинників на параметри носіїв інформації.

3. З визначення каналів витоку інформації виключено поняття "середовище поширення сигналу", оскільки тут сигнал поширюється по ланцюжку носіїв інформації „від носія-джерела – по проміжним (допоміжним) носіям – до носія-одержувача, що не має санкції на доступ до інформації". Слід зазначити, що паразитний ланцюжок каналу витоку інформації може починатись як від джерела, так й від інших носіїв. Але ж закінчується цей ланцюжок правопорушником або його спеціальною апаратурою.

1. Запропоновані варіанти термінів і визначень дозволяють провести корекцію і доповнення деяких Законів України з подальшим уточненням інших документів.

Список літератури

1. Общая парадигма защиты информации / П. Орлов, И. Громыко, В. Носов, Н. Логвиненко, Е. Громыко // Збірник "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – К.: НТУУ "КПІ", 2002. – № 5. – С. 84-86.

2. Общая парадигма защиты информации / П.И. Орлов, И.А. Громыко, В.В. Носов, Н.Ф. Логвиненко, Е.И. Громыко // Конфидент. – 2003. – № 1 (49). – С. 14-26.

3. Загальна парадигма захисту інформації / П.І Орлов та ін. // Інформація та інформатизація: Науково-практичний посібник. – 2-е видання, доп. й перероб. – Х.: НУВС, 2003. – 234 с.

4. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. – К.: Держспоживстандарт України, 1997. – 47 с.

5. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації Основні положення. – К.: Держспоживстандарт України, 1996. – 64 с.

6. Новый энциклопедический словарь. – М.: Большая Российская энциклопедия, РИПОЛ КЛАССИК, 2004. – 1456 с.

7. Моніторинг надзвичайних ситуацій: підручник / Ю.О. Абрамов, Є.М. Грінченко, О.Ю. Кірочкін, П.А. Коротинський, С.М. Миронець, В.О. Росоха, В.В. Тютюник, В.М. Чучковський, Р.І. Невченко. – Х.: АЦЗУ, 2005. – 530 с.

8. НД ТЗИ 1.1-002-99. Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. Нормативний документ ДСТЗІ СБ України. – К., 1999.

9. Специальная техника и информационная безопасность. Т. 1: учебник / Под ред. В.И. Кирина. – М.: Академия управления МВД России, 2000. – 784 с.

10. Технические методы и средства защиты информации / Ю.Н. Максимов, В.Г. Сонников, В.Г. Петров и др. – СПб.: ООО "Издательство Полигон", 2000. – 320 с.

11. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации: учебное пособие / А.А. Хорев. – М.: Гостехкомиссия России, 1998. – 320 с.

12. Хорев А.А. Способы и средства защиты информации / А.А. Хорев. – М.: МО РФ, 2000. – 316 с.

13. Домарев В.В. Безпека інформаційних технологій. Системний підхід / В.В. Домарев. – К.: ТОВ "ТВДДС", 2004. – 992 с.

14. Торокин А.А. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.

15. Ярочкин В.И. Информационная безопасность: учебное пособие. для студентов непрофильных вузов / В.И. Ярочкин. – М.: Междунар. отношения, 2000. – 400 с.

Надійшла до редколегії 13.02.2009

Рецензент: канд. техн. наук, доцент С.В. Кавун, Харківський національний економічний університет, Харків.

ОПРЕДЕЛЕНИЕ СРЕДЫ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ И ТЕХНИЧЕСКИХ КАНАЛОВ ИСТОКА

И.А. Громыко

На основе общей парадигмы информации определен новый подход в системе технической защиты информации к таким базовым понятиям, как среда распространения информации и технические каналы утечки информации. Среде распространения информации отведенная роль среды влияния своими факторами на смену параметров и характеристик носителей информации, а технический канал утечки информации, в таком случае, превратился на паразитную цепочку носителей информации, которая заканчивается правонарушителем или его разведывательной аппаратурой.

Ключевые слова: *информация, носитель информации, защита информации, каналы истока, среда распространения.*

THE DETERMINATION OF THE AMBIENCE OF THE SPREADING TO INFORMATION AND TECHNICAL CHANNEL OF THE HEADWATERS

I.A. Gromiko

On base of the general paradigm to information is determined new approach in system of technical protection to information to such base notion, as ambience of the spreading to information and technical channels seepage. The Ambience of the spreading to information conducted role of the ambience of the influence their own factor on change parameter and naturesстик carriers to information, but technical channel seepage, in such event, changed on stray chain of the carriers to information, which ends the offender or his(its) reconnaissance equipment.

Keywords: *information, carrier to information, protection to information, channels of the headwaters, ambience spread-thread.*