УДК 316.776:351.741:34:650.0128

І.О. Громико

Харківський національний університет внутрішніх справ

ЗАГАЛЬНА ПАРАДИГМА ЗАХИСТУ ІНФОРМАЦІЇ: ВИЗНАЧЕННЯ ТЕРМІНІВ ВІД НОСІЇВ ДО КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

У данный статты визначений новий підхід до рішення проблем, що існують в теорії та практиці захисту інформації.

парадигма, захист інформації, інформаційна безпека, канали витоку інформації

Вступ

В рамках державної політики забезпечення безпеки інформаційних ресурсів вкрай потрібне створення і розвиток сучасної методології ефективного забезпечення безпеки інформації [1]. На сьогоднішній день, найбільш структурованою є теорія захисту інформації в комп'ютерних (автоматизованих) системах. У цій теорії сформульовано цілу низку аксіом і тверджень (теорем), що розкривають методологію створення й функціонування захищених комп'ютерних систем. Узагальнення цієї теорії, 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 [2 – 4]:

Інформація вважається захищеною, якщо при її переміщенні дотримується режимна адекватність комунікабельних носіїв інформації.

Зрозуміло, що необхідний новий, прогресивний підхід до рішення питань захисту інформації. Подальші дослідження, проведені автором в даному напрямі, показали, що в теорії захисту інформації вимагають коректування ряд положень та визначень термінів. Це торкнулося і "середовища поширення...", і проблем з несанкціонованим доступом до інформації, де, наприклад, деякі автори наукових робіт стали нехтувати терміном "канал витоку інформації" (й ін.), відмовляючись від рутинних філософських міркувань.

Наука, в якій келійно-ідеалістичною єдиноначальністю намагаються компенсувати незнання основ діалектичного матеріалізму, приводить до утворення командно-бюрократичної системи захисту інформації. Цей порок уразив більшість країн світу і породив негативні наслідки. В США це ряд моментів від терористичних атак і до продажу документації з секретної зброї "на сторону"; в Англії це виток секретної інформації з планом евакуації жителів Лондона, продаж комп'ютерів з військового підводного човна, які містили секретну інформацію; в Україні це виявлений і перекритий канал доступу сторонніх осіб до бази даних Державтоінспекції; в Росії це масове безперешкодне просочування закритої інформації в космічні дослідницькі центри Китаю; і багато що інше. Порушення інформаційної безпеки найймовірніше там, де панує корупція, постійні приниження і знущання чиновників над викладачами і науковцями, нехтування світовим досвідом та відсутність фундаментальних досліджень [5].

З метою подальшого докладного викладу наукових статей, матеріал запропонований у вигляді послідовних загальних віх "від носіїв до каналів витоку інформації". Деякі терміни і визначення, наприклад – "інформація", довелося формулювати наново, оскільки вони визначалися через самих себе [2].

1. Інформація

Закон України "Про інформацію" визначає інформацію, як "документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі" [1].

Крім того існує ще понад 400 визначень цього терміну. Наприклад:

– інформація – це зафіксоване на носії уявлення про предмети, процеси, події, природні явища тощо [2 – 4];

– інформація – відомості про суб'єкти, об'єкти, явища та процеси [6];

– інформація – відомості про об'єкти та явища навколишнього середовища, їхні параметри, властивості й стани, які зменшують наявну про них ступінь невизначеності, неповноти знань [7] й т.ін.

Існує багато ознак поділення інформації на класи, види та т.п. Наприклад, Закон України "Про інформацію" поділяє інформацію на такі види, як статистична інформація; адміністративна інформація (дані); масова інформація; інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування; правова інформація; інформація про особу; інформація довідково-енциклопедичного характеру; соціологічна інформація [1].

Розрізняють також відкриту інформацію та інформацію з обмеженим доступом. Обмеження передбаченого правовими нормами одержання, використання, поширення і зберігання інформації може

викликати необхідність нанесення на її носії (носії інформації) спеціальних позначок. Наприклад, позначка грифу секретності є реквізитом матеріального носія секретної інформації. Вона засвідчує ступінь секретності даної інформації [8].

2. Носії 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 [6].

До носіїв інформації відносяться матеріальні об'єкти, які забезпечують запис, зберігання і передавання інформації у просторі і часі [7].

Визначено, що забезпечення належного стану матеріальних носіїв є суттєвою складовою поняття "зберігання інформації" [1].

Необхідно підкреслити, що словосполучення "носій без інформації" як і "чистий аркуш паперу" настільки реально і допустимо, наскільки недопустимі словосполучення "інформація без носія" або "інформація не на носії".

Примітка 1. Фахівцям системи технічного захисту інформації (ТЗІ) слід пам'ятати, що з технічної точки зору носій інформації завжди містить інформацію, яка потрібна вузькому кругу фахівців. Так, новенький комп'ютерний жорсткий диск, що зійшов з конвеєра, або новенька звичайна дискета містять багато параметрів, якими цікавляться як фахівці - виробники продукції, так і користувачі. Якщо ж відформатовані носії інформації коли-небудь містили інформацію, то інтерес до них проявляють і фахівці іншого профілю [9].

Носії інформації матеріальні. Вони знаходяться в просторі і в часі у вигляді поля, речовини або їх сукупності. Оскільки за допомогою матеріальних засобів можна захищати тільки матеріальний об'єкт, то при захисту інформації об'єктами захисту становляться саме **матеріальні** носії інформації [7].

З причини важливості *самої* ***матеріальності носія*** і для припинення помилкових варіантів тлумачення терміну "носій інформації" в документах багато разів застосовується термін "матеріальний носій інформації" [8].

Примітка 2. У деяких документах і навіть законах зустрічається об'єднання в єдиний ряд інформації і їх носіїв з послідовним переліком типу: "інформація, носій інформації" і т.д. Ця не зовсім коректна дія дозволяє припустити, що інформація здатна існувати без носія. Особливо, це негативно впливає на думки людей, що тільки починають пізнавати ази елементів теорії захисту інформації. Так, у статті 6 Закону України "Про державну таємницю" сказано: "Якщо **власник** ***секретної інформації або її матеріальних носіїв*** відмовляється від укладення договору чи порушує його, за рішенням суду ***ця інформація або її матеріальні носії*** можуть бути ... (далі по тексту) [8]". Подібні неточності містяться і в другому абзаці статті 27 цього закону, що вимагає його професійного доопрацювання і доповнення. Для порівняння слід зазначити, що подібного роду погрішності у базовому Законі України "Про інформацію" відсутні.

При класифікації носіїв інформації звертають увагу як на ступінь обмеженості доступу до інформації, що міститься на цих носіях, так і на їхню роль у процесі інформаційних відносин.

Загальна парадигма захисту інформації встановлює, що залежно від напрямку переміщення інформації у процесі інформаційних відносин носії можуть бути: носіями-джерелами (джерелами), проміжними носіями, носіями-одержувачами (одержувачами).

Джерелами інформації визначено передбачені або встановлені законом носії інформації: документи або інші носії інформації, які являють собою матеріальні об'єкти, що зберігають інформацію [1].

Необхідність виділення окремої проміжної групи носіїв інформації, що є переносниками інформації, підтримується й в інших роботах сучасних вчених [7].

У якості проміжних носіїв інформації може бути тільки матерія:

– речовина (повітря, вода, каміння, метал, перетворювачі й інші об'єкти живої та неживої природи);

– поле (електромагнітне, гравітаційне, та ін.), що оточує і пронизує речовину.

Відомо, що одержувачі сприймають інформацію через сенсор (датчик, вимірювальний перетворювач) [2 – 4]. Процес сприйняття доволі складний, і складається з процесів приймання і перетворення інформації, котрі забезпечують відбиття об'єктивної реальності й орієнтування в навколишньому світі. Сприйняття може містити в собі: виявлення об'єкта у полі сприйняття, розрізнення окремих ознак у об'єкті, виділення в ньому адекватного меті дії інформативного змісту, формування образу сприйняття.

3. Змінювання параметрів носіїв інформації

Під впливом природних або штучних чинників параметри носіїв інформації можуть бути кількісно або якісно змінені.

Ця зміна може існувати на носії певний проміжок часу, міняючи свої координати. Наприклад, друкарська фарба дифундує в товщу паперу або в повітря; магнітна сигналограма зміщується (спотворюється) із-за взаємної зміни розмірів і, відповідно, координат магнітних доменів; звукові пружні хвилі стиснення і розрідження поширюються в повітрі, рідині або твердому тілі; під дією ЕДС носії зарядів впорядковують рух, породжуючи магнітне поле або сукупність (що породжує одне одного) магнітного і

електричного полів, які поширюються від джерела із швидкістю близькою до швидкості світла і т.д.

Кількісні зміни параметрів носіїв інформації найбільш поширені, досить добре вивчені, систематизовані і відомі, зокрема, під технічним терміном "модуляція носіїв інформації" [10].

Не зупиняючись на "модуляції" (термін, який часто застосовується у фізиці для опису роботи перетворювачів, бо про них піде мова нижче), приведемо деякі приклади кількісної зміни носіїв інформації:

– збільшення або зменшення хаотичного руху молекул, атомів і вільних носіїв зарядів при підвищенні або пониженні температури провідника;

– виникнення або припинення впорядкованого руху носіїв електричних зарядів, збільшення або зменшення електричного струму, що протікає в електричному колі під дією різниці потенціалів;

– випромінювання або припинення випромінювання електромагнітного поля, збільшення або зменшення потужності радіопередавача;

– сканування по азимуту і куту місця променя (пучка) фотонів або радіоактивних частинок;

– зміна кількості мод і їх розташування в перетині променя лазера або СВЧ хвилеводу і ін.

Якісні зміни параметрів носіїв інформації також достатньо широко вивчені, проте дані по ним слабо систематизовані і зберігаються у бібліотеках науково-дослідницьких інститутів СНД, літературних джерелах і численних спеціалізованих звітах НДР відкритого і обмеженого доступу.

При розгляді процесу якісної зміни параметрів носіїв інформації, можна побачити, що ми маємо справу з істотною (у разах) кількісною зміною параметрів носіїв інформації, викликаною зміною самої структури або агрегатного стану носія.

Таке явище, як якісна зміна речовини – носія інформації, з фізичної точки зору, цілком припустимо і достатньо поширено. Особливо, якщо йдеться про фазу, в термодинамічному її розумінні. Прикладом може служити:

– вода**,** яка здатна знаходитися в трьох агрегатних станах (в трьох фазах – [11]);

– вуглець**,** що має дві основні кристалічні модифікації, й інші речовини.

Важливо відзначити, що якісна зміна настільки істотно змінює параметри носія інформації, що він розглядається фахівцями ТЗІ як декілька носіїв. Візьмемо, наприклад, швидкість розповсюдження звуку ($V_{зв}$) у воді (H_2O) [11]:

– водяна пара – $V_{зв}$ = 401 м/с;

– дистильована (або морська) вода – $V_{зв}$ = 1484 (1490) м/с;

– лід – $V_{зв}$ = 3280 м/с.

Зміна одного параметра носія інформації здатна настільки (якісно) змінити інший параметр, що цей ланцюг причинно-наслідкових зв'язків розглядається вченими, як окреме фізичне явище. Наприклад, радіохвилі і звукові хвилі піддаються сильній рефракції із-за відмінності швидкостей поширення в шарах повітря (води). У свою чергу, рефракція може привести і до зменшення дальності поширення звукових і радіохвиль, і до її істотного збільшення. Так, поширення хвиль по атмосферних і підводних хвилеводах створює додаткові труднощі для фахівців ТЗІ, що вирішують задачі утаєння випробувань нових зразків спецтехніки. Не дивлячись на те, що в діапазоні частот 500 - 2000 Гц дальність поширення звуку середньої інтенсивності досягає 15 – 20 кілометрів, гучні звуки можуть бути зареєстровані на відстанях в сотні і тисячі кілометрів із-за наявності підводних звукових каналів (хвилеводів) [12].

Далі під "якісною зміною параметрів носіїв інформації" ми розумітимемо таку *кількісну зміну* просторово-часових і енергетичних параметрів носія інформації, *що істотно відрізняється від середнього значення*, без участі в процесі яких-небудь перетворювачів.

4. Перетворювачі

Перетворювачі – прилади, пристрої або яка-небудь речовина, що сприймають від одного носія інформації зовнішню дію і перетворюють її в дію, що змінює параметри іншого носія інформації. На процес перетворення може витрачатися енергія як від зовнішньої дії, так і від додаткового джерела енергії.

Параметр – величина, що характеризує ті або інші властивості процесу, явища або системи. Наприклад, ємність, індуктивність і активний опір є параметрами коливального контуру, які можуть бути зосередженими або розподіленими у просторі [13].

У основі дії перетворювачів, як правило, лежать які-небудь фізичні явища, часто об'єднані під терміном "фізичний ефект".

У таблиці приведені деякі фізичні ефекти, що лежать в основі роботи різних конструкцій, тим чи іншим чином пов’язані з технічним захистом інформації.

Перетворювачі, можна виділити окремим підкласом носіїв інформації. Вони можуть бути і проміжними носіями інформації, і одержувачами. Наприклад, прилади із зарядовим зв'язком, з одного боку, перетворюють зображення в електричні сигнали, що поширюються далі по проводовим системам зв’язку, та з другого боку, достатньо довго зберігають зображення у вигляді дискретного потенційного рельєфу [14].

Примітка 3. Сучасні дослідження вимагають систематизації параметрів і характеристик носіїв інформації, що впливають на час її знаходження на тому або іншому носії. Це дозволить по відношенню до інформації зменшити кількість таких вживаних термінів, як "достатньо довго", "невеликий проміжок часу", "істотний період часу" і ін.

Зміна параметрів носіїв інформації і, навіть їх перетворення можуть бути матеріальним втіленням "повідомлення" про яку-небудь подію, явище, стан об'єкту або команду управління, сповіщення т.д.

Таблиця

Деякі приклади фізичних ефектів

Ефект	Суть ефекту	Примітка
Прямий п'єзоефект (1880 рік)	Виникнення електричної поляризації кристалічних речовин (п'єзоелектрики) при їх стисненні або розтягуванні	П'єзоелектричні властивості виявлені у більш ніж 1500 речовин. Застосовується як перетворювач для закладних пристроїв.
Зворотний п'єзоефект (1880 рік)	Поява механічної деформації кристалічних речовин (п'єзоелектрики) під дією електричного поля.	
Керр ефект (1875 рік)	Квадратичний електрооптичний ефект, виникнення подвійного променезаломлення в оптично ізотропних речовинах (рідинах, стеклах, кристалах з центром симетрії) під впливом однорідного електричного поля.	Застосовується при створенні мало-інерційних (10^{-13}с) модуляторів світлового потоку від випромінювачів.
Холу ефект (1879 рік)	Виникнення у твердому провіднику із струмом, поміщеному в магнітне поле**,** електричного поля, перпендикулярного векторам струму і магнітного поля.	Використовується для вимірювання напруженості магнітного поля і рішення ін. завдань.
Тунельний ефект	Подолання мікрочасткою потенційного бар'єру у разі, коли її повна енергія менше висоти бар'єру.	Тунельні діоди і діоди Ганна застосовують для створення простих схем ВЧ і НВЧ генераторів мініатюрних закладених пристроїв.
Ганна ефект (1963 рік)	Генерація ВЧ коливань електричного струму в напівпровіднику з N-образною вольт-амперною характеристикою.	
Шоткі ефект (1939 рік)	Зменшення роботи виходу електронів з твердих тіл під дією електричного поля, що прискорює електрони.	Діоди з Шоткі бар'єром застосовуються для створення СВЧ детекторів і змішувачів, фотодіодів і транзисторів.

Застосування терміну "повідомлення" визначає, обов'язкову участь в інформаційному процесі двох (джерело та одержувач) і більш носіїв інформації.

Примітка 4. Слід зазначити, що в загальній парадигмі захисту інформації виділений окремий клас носіїв інформації, що мають таку властивість як комунікабельність. Комунікабельність (від лат. communicabilis - сполучний, сполучуваний). Комунікабельність це сумісність (здатність до спільної роботи) різнотипних систем передачі інформації (наприклад, в електрозв'язку - аналогових і дискретних систем, у телебаченні – систем з різним числом рядків розкладання телевізійного кадру); здатність до спілкування, товариськість [13]. Новий науковий напрям у цьому ракурсі, буде розглянуто в наступній статті.

Іноді, разом з терміном "носій інформації" застосовується термін "сигналоносій", як "носій запису", – тверда речовина, призначена для фіксації і тривалого зберігання в ньому інформації [15].

5. Сигнал

Коректне визначення „сигналу” є дуже складним моментом, бо зачіпає основи термодинаміки, види та властивості інформації як предмету захисту, якості джерел і одержувачів та їхні стани (психологічний, тезаурус й т.ін.) . Тому автор дає скорочене визначення цього терміну, виходячи з матеріалів базової статті [2]. Але, визначенню терміну “сигнал” буде присвячено окрему статтю с розгляданням особливостей [7], що визначені вище.

Сигнал – це зафіксована одержувачем зміна параметрів носіїв інформації, яка корельована зі станом чи змінами стану об’єктів (предметів, подій, явищ й т.ін.), або очікувана відсутність змін в процесі інформаційних відносин [1], що має значення [28] для одержувача.

Якщо процес інформаційних відносин між джерелом і одержувачем був заздалегідь синхронізований, відсутність очікуваного сигналу (синхронна відсутність) "в потрібному місці і в потрібний час" також фіксується одержувачем як сигнал.

Примітка 5. Треба зазначити, що у державному стандарті України є некоректним постановка "сигналів" в одну групу з носіями інформації (див. "фізичні поля" і "хімічні речовини" у п.3.3. [16]), бо це руйнує стрункy систему термінів та визначень іншого державного стандарту (п.6.2 у [6]). Але і цей стандарт породжує багато питань (наприклад, до смислового значення терміну „інформативний сигнал”), що повинні бути розглянуті з матеріалістичної точки зору [6, 28].

6. Від середовища поширення до середовища впливу

Прийнято вважати, що середовищем поширення носіїв інформації можуть бути лінії зв'язку, сигналізації, управління, енергетичні мережі, устатку-

вання, інженерні комунікації і споруди, що захищають будівельні конструкції, а також світлопроникні елементи будівель і споруди (отвори), повітря, водне середовище, ґрунт, рослинність і т.п. [16, 17].

Загальна парадигма захисту інформації конкретизує абстрактне уявлення про середовище. А саме:

"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 переходу кількості в якість).

Під чинником розуміється причина, рушійна сила якого-небудь процесу, явища, що визначає його характер або окремі його риси [13]. Навколишнє середовище включає природне середовище і штучне (техногенне) середовище [17]. З врахуванням того, що людина офіційно розглядається як носій інформації [18, 19], найбільш коректним варіантом визначення терміну „середовище" є варіант приведений українськими вченими [18]:

"**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".

Вищевикладений матеріал дозволяє сформулювати визначення каналу витоку інформації і охарактеризувати процес утворення каналу витоку інформації.

7. Канал витоку інформації, технічний канал витоку інформації

У багатьох ведучих авторських працях під "каналом витоку інформації", а також "технічним каналом витоку інформації" розуміється наступне [20 – 26]:

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 [20].

2. Канал витоку інформації (технічний) – сукупність джерела небезпечного сигналу, **середовища поширення носія небезпечного сигналу** і засобу розвідки [21].

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** [22, 23].

4. Канал витоку інформації [Covert channel] – канал комунікації, що дозволяє процесу передавати інформацію шляхом, що порушує безпеку системи [24]. 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) [25].

6. Під каналом витоку інформації розумітимемо фізичний шлях від джерела конфіденційної інформації до зловмисника [26]. Відносно сигналу цей шлях містить послідовний ланцюг з елементів: "джерело – джерело сигналу – **середовище** – приймач – зловмисник"[26].

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.

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 наступною (рис. 3). 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.

Примітка 6. Слід врахувати, що на рис. 3 приведений спрощений варіант технічного каналу витоку інформації, в якому не показані зворотні зв'язки, наявність яких строго обґрунтована в наукових працях [27].

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.

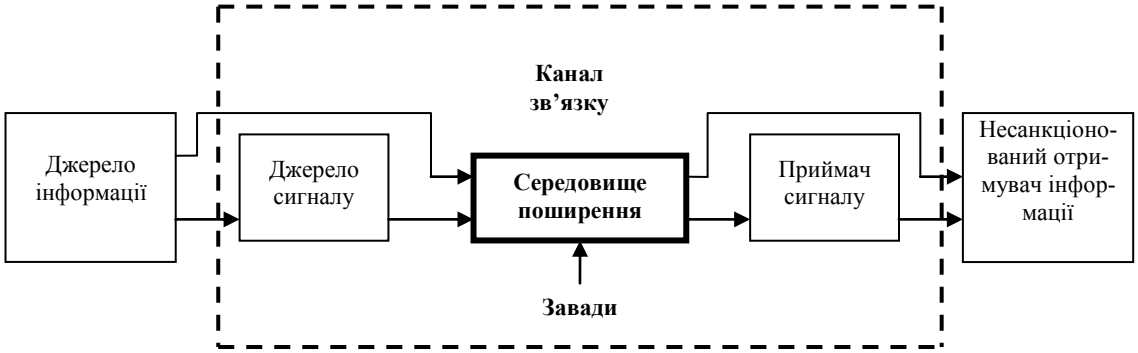

Рис. 1. Структура технічного каналу витоку інформації [25]

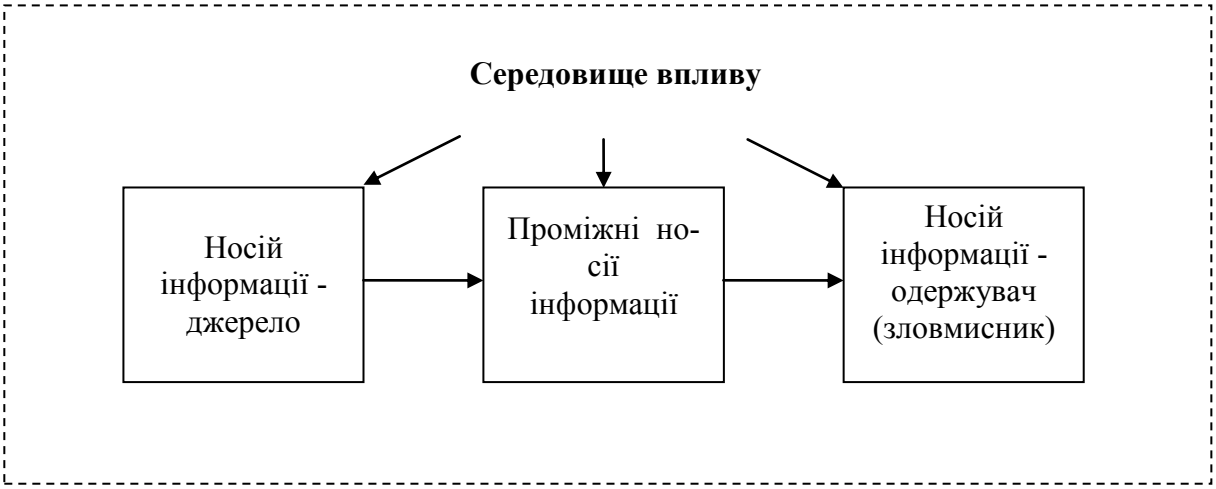

Рис. 2. Узагальнена структурна схема каналу витоку інформації

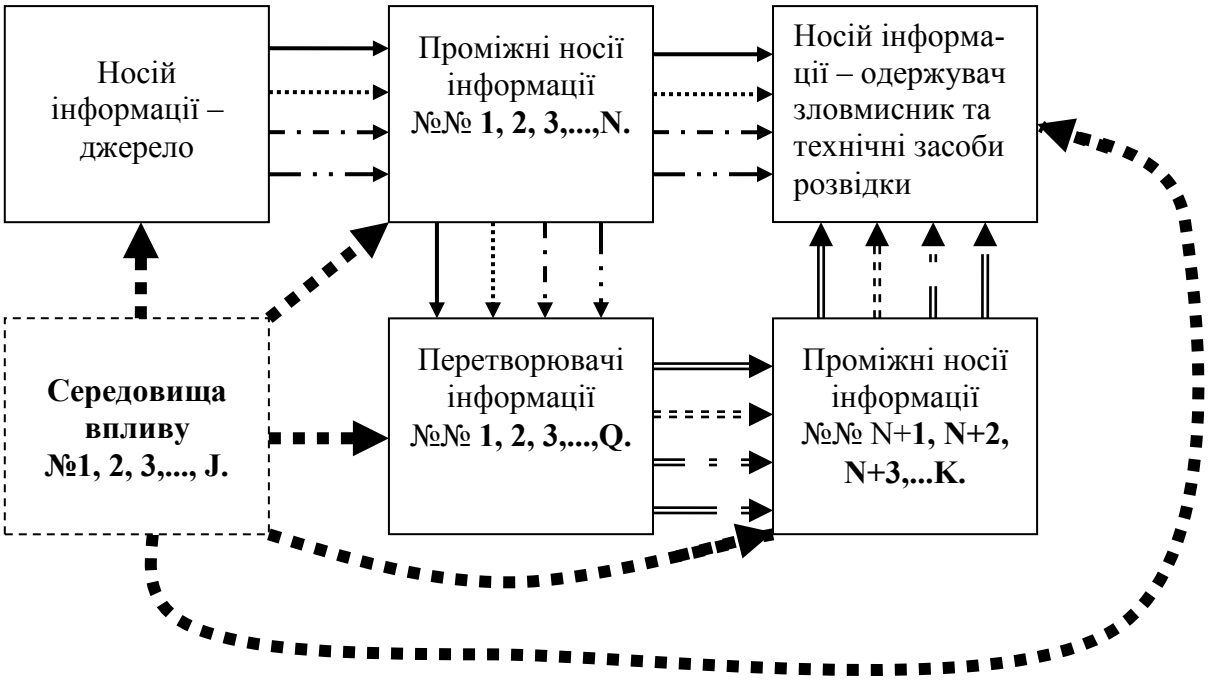

Рис. 3. Структурна схема технічного каналу витоку інформації

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

Висновки

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

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. Теорія перетворювачів, як носіїв інформації, вимагає додаткових досліджень, систематизації і виділення в окрему дисципліну при підготовці фахівців в області ТЗІ.

4. 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.

Список літератури

1. Закон України №2657-XII від 2 жовтня 1992 року "Про інформацію".

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

3. 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.

4. Загальна парадигма захисту інформації / П.І. Орлов та ін. // Науково-практичний посібник «Інформація та інформатизація». 2-е видання, доп. й перероб. – Х.: НУВС, 2003. – 320 с.

5. Громико І.О., Оспіщев Є.Я. Проблемні аспекти захисту інформації в Україні // Право і безпека. Розділ "Технічне забезпечення діяльності правоохоронних органів". – 2005. – № 4'4. – С. 176-179.

6. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

7. Богуш В.М., Юдін О.К. Інформаційна безпека держави. – К.: МК-Прес, 2005. – 432 с.

8. Закон України № 3855-XII від 21 січня 1994 року "Про державну таємницю".

9. Информационная безопасность офиса. Научно-практический сборник. – К.: ООО "ТИД "ДС", 2003. – 216 с.

10. Темников Ф.Е., Афонин В.А., Дмитриев В.И. Теоретические основы информационной техники. – М.: Энергия, 1971. – 424 с.

11. Кузмичев В.Е. Законы и формулы физики / Под ред. В.К. Тартаковского. – К.: Наукова думка, 1989. – 864 с.

12. Физика. Большой энциклопедический словарь / Гл. ред. А.М. Прохоров. – 4-е изд. – М.: Большая Российская энциклопедия, 1999. – 944 с.

13. Советский энциклопедический словарь / Научно-редакционный совет: А.М. Прохоров (пред.). – М.: Советская Энциклопедия, 1981. – 1600 с.

14. Радіотехніка: Енциклопедичний навчальний довідник: Навч. посібник / За ред. Ю.Л. Мазора, Є.А. Мачуського, В.І. Правди. – К.: Вища школа, 1999. – 838 с.

15. Политехнический словарь / Гл. ред. И.И. Артоболевский. – М.: Советская Энциклопедия, 1976. – 608 с.

16. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації Основні положення.

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

18. Моніторинг надзвичайних ситуацій: Підручник / Ю.О. Абрамов, Є.М. Грінченко та ін. – Х.: АЦЗУ, 2005. – 530 с.

19. 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.

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

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

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

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

24. Домарев В.В. Безпека інформаційних технологій. Системний підхід. – К.: ТОВ "ТВД" ДС", 2004. – 992 с.

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

26. Ярочкин В.И. Информационная безопасность: Учебное пособие для студентов непрофильных вузов. – М.: Междунар. отношения, 2000. – 4000 с.

27. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие. – М.: Горячая линия – Телеком, 2004. – 280 с.

28. Философский энциклопедический словарь. – М.: ИНФРА-М, 2000. – 576 с.

Надійшла до редколегії 15.09.2006

Рецензент: д-р техн. наук, проф. В.А. Краснобаєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.