такого дозволу є висновок експертизи автоматизованої системи, тобто перевірки відповідності реалізованої комплексної системи захисту інформації встановленим нормам

Якщо порядок обробки і захисту інформації не регламентується законодавством, експертиза може виконуватись в необов'язковому порядку за поданням замовника (власника автоматизованої системи або інформації).

В процесі експертизи оцінюється комплексна система захисту інформації автоматизованої системи в цілому. В тому числі виконується оцінка реалізованих в обчислювальній системі засобів захисту, які слід розглядати як підсистему захисту від несанкціонованого доступу в складі комплексної системи захисту інформації.

Отже, залежно від особливостей функціонування автоматизованої системи необхідно визначити відповідний профіль її захищеності та розробити комплексну систему захисту інформації. При цьому слід врахувати основні принципи забезпечення безпеки інформації та керування доступом. Оцінюючи повноту реалізації послуг безпеки необхідно використати критерії оцінки захищеності інформації.

З точки зору методології в проблемі захисту інформації від несанкціонованого доступу слід виділити два напрями:

- забезпечення і оцінка захищеності інформації в автоматизованій системі, що функціонує;
- реалізація та оцінка засобів захисту, що входять до складу компонентів, з яких будується обчислювальна система.

Кінцевою метою всіх заходів щодо захисту інформації, які реалізуються, має бути забезпечення безпеки інформації під час її обробки в автоматизованій системі на всіх стадіях її життєвого циклу, на всіх технологічних етапах обробки інформації та в усіх режимах функціонування.

*Література:* ***1.*** *НД ТЗІ 1. 1-003-99. «Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».* ***2.*** *Закон України «Про захист інформації в автоматизованих системах».* ***3.*** *НД ТЗІ 2. 5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».* ***4.*** *НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».****5.*** *НД ТЗІ 2. 5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».*

**УДК 316.776:351.741:34:650.0128**

# ЗАГАЛЬНА ПАРАДИГМА ЗАХИСТУ ІНФОРМАЦІЇ: ВИЗНАЧЕННЯ ТЕРМІНІВ

***Ігор Громико***

*Харківський національний університет внутрішніх справ*

*Анотація:* **Визначено новий підхід до розв'язання проблем, що існують в теорії та практиці захисту інформації.**

*Summary:* **Certain a new approach to decision of problems which exist in a theory and practice of protection of the information in Ukraine.**

*Ключові слова:* **Парадигма, захист інформації, інформаційна безпека, канали витоку інформації.**

## Вступ

В рамках державної політики забезпечення безпеки інформаційних ресурсів вкрай потрібна сучасна методологія ефективного забезпечення безпеки інформації [1]. На сьогоднішній день найбільш структурованою є теорія захисту інформації в інформаційних (автоматизованих) системах (ІС). У цій теорії сформульовано низку аксіом і тверджень (теорем), що розкривають методологію створення й функціонування захищених ІС. Узагальнення цієї теорії, що увібрала світовий досвід боротьби з правопорушеннями в інформаційній сфері, і поширення її на загальну інформаційну сферу дозволило автору сформулювати загальну парадигму захисту інформації [2 – 4]:

Дослідження, проведені автором, показали, що зокрема в теорії захисту інформації слід скоректувати ряд положень та визначень термінів.

Невизначеність, неточність 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 комерційного продажу документації на секретну зброю; в Англії – це витік секретної інформації щодо плану евакуації жителів Лондона, продаж комп'ютерів з військового підводного човна, які містили секретну інформацію; в Україні – це виявлений і перекритий канал несанкціонованого доступу до бази даних Державтоінспекції; в Росії – це масове безперешкодне просочування закритої інформації в космічні дослідницькі центри Китаю і багато що інше. Порушення інформаційної безпеки найімовірніше там, де панує корупція, постійні зловживання чиновників, нехтування світовим досвідом та відсутність фундаментальних досліджень [5].

Далі матеріал подається 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].

## І Інформація

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

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];
- відомості про суб'єкти, об'єкти, явища та процеси [6];
- 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, в [1] інформацію поділено на такі види: 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.

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 обмеження доступу до даної інформації [8].

## ІІ Носії інформації

Дослідження властивостей інформації показують, що інформація завжди існує тільки на носіях інформації [4], які є матеріальними об’єктами, в тому числі фізичними полями [8]. З технічної точки зору до носіїв інформації відносяться матеріальні об'єкти, що забезпечують запис, зберігання і передавання інформації у просторі і часі [7].

Зі строгої позиції діалектичного матеріалізму при тлумаченні про зміст терміну „носій інформації” необхідно підкреслювати, що "носій інформації" може не містити інформації, але зворотній варіант неможливий, бо маючи наувазі інформацію, не можна застосовувати словосполучення "інформація без носія" або "інформація не на носії" й т. ін.

***Примітка 1***. Важливо пам’ятати, що залежно від тезауруса користувача один і той же носій інформації для одного користувача не містить інформації, а для іншого (наприклад, працівника системи ТЗІ) містить корисну інформацію [9].

Для припинення помилкових варіантів тлумачення терміну "носій інформації" та важливості підкреслення самої **матеріальності** носія **на державному рівні** в документах застосовується термін "матеріальний носій інформації" [8].

***Примітка 2.*** У деяких документах і навіть законах зустрічається об'єднання в єдиний ряд інформації і їх носіїв. 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 теорії захисту інформації. Так, у статті 6 [8] 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)". 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 помилки 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 в 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, які є переносниками інформації, підтримується й в інших роботах сучасних вчених [7].

Як проміжний носій інформації може бути тільки матерія:

– речовина (повітря, вода, каміння, метал, перетворювачі й інші об'єкти живої та неживої природи);
– поле (електричне, магнітне, електромагнітне, гравітаційне).

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.

## III Зміна 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) через взаємну зміну розмірів і, відповідно, координат магнітних доменів; під дією ЕРС носії зарядів впорядковують рух, породжуючи магнітне поле або сукупність (що породжує одне одного) магнітного і електричного полів, які поширюються від джерела зі швидкістю, близькою до швидкості світла і т. д.

**Кількісні зміни параметрів носіїв інформації** 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 швидкості хаотичного руху молекул, атомів і вільних носіїв зарядів при підвищенні або зниженні температури провідника;
- виникнення або припинення впорядкованого руху носіїв електричних зарядів, збільшення або зменшення електричного струму, що тече в електричному колі під дією різниці потенціалів;
- випромінювання або припинення випромінювання електромагнітного поля, збільшення або зменшення потужності радіопередавача;
- сканування за азимутом і кутом місця променя фотонів або радіоактивних частинок;
- зміна кількості мод і їх розташування в перетині променя лазера або НВЧ хвилеводу і ін.

**Якісні зміни параметрів носіїв інформації** також достатньо широко вивчені, проте ці дані слабо систематизовані і зберігаються у бібліотеках науково-дослідницьких інститутів, 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 властивостей речовини – носія інформації, достатньо поширено. Особливо, якщо йдеться про фазу, в термодинамічному її розумінні. Прикладом може слугувати:

- вода**,** яка здатна знаходитися в трьох агрегатних станах [11];
- вуглець**,** що має декілька основних кристалічних модифікацій, 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 поширення 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 це розглядається вченими, як окреме фізичне явище. ланцюг причинно-наслідкових зв'язків розглядається

вченими, як окреме фізичне явище. Наприклад, радіохвилі і звукові хвилі піддаються сильній рефракції через Зміна одного параметра носія інформації здатна настільки (якісно) змінити інший параметр, що це розглядається вченими, як окреме фізичне явище. відмінність 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 атмосферними і підводними хвилеводами створює додаткові труднощі для фахівців ТЗІ, що вирішують задачі приховування випробувань нових зразків спецтехніки. В діапазоні частот 500 – 2000 Гц дальність поширення звуку середньої інтенсивності досягає 15 – 20 кілометрів, але гучні звуки можуть бути зареєстровані на відстанях в сотні і тисячі кілометрів через наявність підводних звукових каналів (хвилеводів) [12].

Далі під "якісною зміною параметрів носіїв інформації" ми розумітимемо таку кількісну зміну просторово-часових і енергетичних параметрів носія інформації, при якій вони істотно відрізняються від середнього значення без участі в процесі роботи яких-небудь перетворювачів

## IV Перетворювачі

На процес перетворення може витрачатися енергія як зовнішньої сили, так і додаткового джерела енергії.

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

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

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

Таблиця – Деякі приклади фізичних ефектів

| Ефект | Суть ефекту | Примітка |
|---|---|---|
| Прямий п'єзоефект | 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 | Поява механічної деформації кристалічних речовин (п'єзоелектрики) під дією електричного поля. | |
| ефект Керра | Квадратичний електрооптичний ефект, виникнення подвійного променезаломлення в оптично ізотропних речовинах (рідинах, склах, кристалах з центром симетрії) під впливом однорідного електричного поля. | Застосовується при створенні мало-інерційних ($10^{-13}$с) модуляторів світлового потоку від випромінювачів. |
| ефект Холла | Виникнення у твердому провіднику зі струмом, розміщеному в магнітному полі**,** 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 ВЧ і НВЧ генераторів мініатюрних закладних пристроїв. |
| ефект Ганна | Генерація ВЧ коливань електричного струму в напівпровіднику з N-подібного вольт-амперною характеристикою. | |
| ефект Шотткі | Зменшення роботи виходу електронів з твердих тіл під дією електричного поля, що прискорює електрони. | Діоди Шотткі застосовуються для створення НВЧ детекторів і змішувачів, фотодіодів і транзисторів. |

Перетворювачі, слід виділити як окремий підклас 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 проводовими системами зв’язку,

та а 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 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.

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

***Примітка 4.*** Слід зазначити, що в загальній парадигмі захисту інформації виділено окремий клас носіїв інформації, що мають таку властивість, як комунікабельність. Комунікабельність (від лат. communicabilis – сполучний, сполучуваний) – 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].

## V Сигнал

Дати коректне визначення „сигналу” важко, 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 [2].

Сигнал – це зафіксована зміна параметрів носіїв інформації корельовано 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, то 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]).

## VI Від середовища поширення до середовища впливу

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 споруд (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 ланцюжком (послідовним, послідовно-паралельним 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, наведений в [18]:

“**середовище** це:

1. речовина і/чи поле, що оточують розглянутий об'єкт (у нашому випадку – носій інформації);
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.

## VII Канал витоку інформації

Міркуючи про канал витоку інформації, багато авторів говорять про шляхи та напрями

несанкціонованого доступу до інформації [20 – 26]. Але при визначенні технічного каналу витоку інформації автори вводять поняття „**середовище поширення”** або не конкретизуючи „поширення чого?” [26], або розкриваючи зміст цього поширення: носіїв сигналів [21] чи сигналів [22, 23].

Автор згоден з наступним визначенням технічного каналу: „Якщо поширення інформації відбувається за допомогою технічних засобів, то відповідний канал називається технічним каналом [25]”. Як правило, більшість схем технічних каналів витоку інформації автори зводять до структури, наведеній на рис. 1.

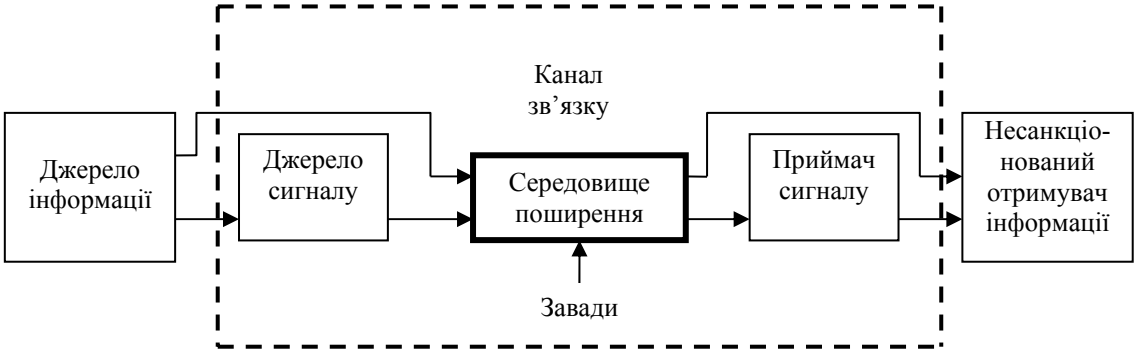


**Рисунок 1 – Структура технічного каналу витоку інформації [25]**

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", узагальнену структурну схему каналу витоку інформації можна подати таким чином (рис. 2):

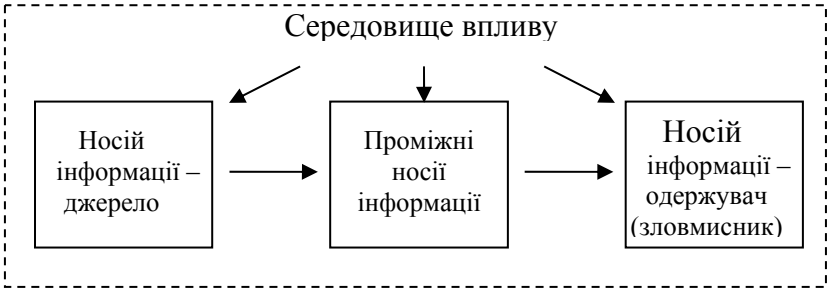


**Рисунок 2 – Узагальнена структурна схема каналу витоку інформації**

Тоді структурна схема технічного каналу витоку інформації буде такою, як показано на (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 наведено спрощений варіант технічного каналу витіку інформації, в якому не показані зворотні зв'язки, наявність яких суворо обгрунтована в наукових працях [27].

Під утворенням каналу витоку інформації ми будемо розуміти виникнення під дією різних чинників небажаної (паразитної) 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.

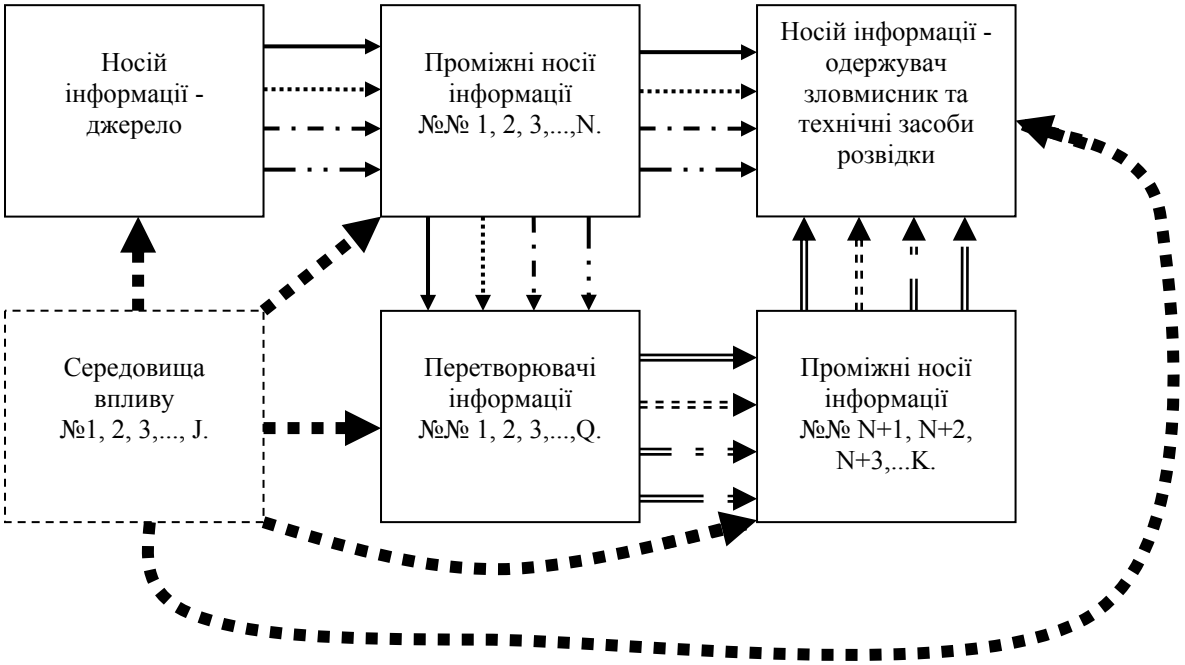


**Рисунок 3 – Структурна схема технічного каналу витоку інформації**

## Висновки

1. Запропоновані варіанти термінів і визначень дозволять провести корекцію і доповнення положень деяких Законів України з подальшим уточненням інших документів.
2. Запропоновано розглядати навколишнє середовище як таке, що бере участь в процесі поширення сигналів тільки шляхом дії його 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 урахуванням пункту 2 висновків, що наведені вище, у каналі витоку інформації сигнал поширюється по ланцюжку носіїв інформації „від носія-джерела – через проміжні (допоміжні) носії – до носія-одержувача, який не має санкції на доступ до інформації”. У такому визначенні термін "середовище поширення сигналу" не застосовується. Слід зазначити, що паразитний ланцюжок каналу витоку інформації може починатись як від джерела, так і від інших носіїв. Але закінчується цей ланцюжок у правопорушника або його спеціальною апаратурою.

*Література: **1.** Закон України №2657-XII від 2 жовтня 1992 року "Про інформацію". **2.** Общая парадигма защиты информации. Орлов П., Громико И., Носов В., Логвиненко Н., Громико Е. // Збірник "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. НТУУ "КПІ". - 2002. - №5. - С. 84 – 86. **3.** Орлов П. И., Громыко И. А., Носов В. В., Логвиненко Н. Ф., Громыко Е. И. Общая парадигма защиты информации // Конфидент. - 2003. - №1 (49). - с. 14 - 26. **4.** Загальна парадигма захисту інформації. Орлов П. І., та ін. в Науково-практичному посібнику «Інформація та інформатизація». 2-е видання, доп. й перероб. – Харків: Вид-во. НУВС, 2003 р. **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 /Отв. ред. В. К. Тартаковский. - 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 шк., 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.*** *Абрамов Ю. О., Грінченко Є. М., Кірочкін О. Ю., Коротинський П. А., Миронець С. М., Росоха В. О., Тютюник В. В., Чучковський В. М., Невченко Р. І. Моніторинг надзвичайних ситуацій. Підручник. Вид-во: АЦЗУ м. Харків, 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. - Київ, 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. СПб.: 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 / А. А.Торокин. - 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. Учеб. пособие для вузов. - М.: Горячая линия - Телеком, 2004. – 280 с. 28. Философский энциклопедический словарь. – М.: ИНФРА-М, 2000. – 576 с.*