УДК 621.39

В. І. ЗАБОЛОТНИЙ, канд. техн. наук

КЛАСИФІКАЦІЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

Організація системи захисту об'єкта від витоку інформації, як передбачено державними стандартами України у галузі технічного захисту інформації (ТЗІ) [1 – 3], потребує складати окрему модель загроз. Формалізований опис технічних каналів витоку інформації (ТКВІ) є суттєвою складовою окремої моделі загроз і основою для розробки необхідних заходів захисту. Класифікація ТКВІ являє собою якісну модель сукупності матеріального об'єкту, що містить інформацію з обмеженим доступом (ІзОД), середовища її розповсюдження та засобів технічних розвідок [3]. Декомпозиція ТКВІ дає змогу зробити адекватний кількісний опис кожної з окремих складових каналу, провести їх дослідження як без заходів ТЗІ, так і з певним набором останніх. Наведене далі відкриває шлях до оцінки ефективності захисту від витоку інформації технічними каналами.

1 Форми існування даних, що підлягають захисту

Аналіз змісту [1], а також першої редакції Положення про ТЗІ в Україні [4], дозволяє зробити висновки щодо існування двох взаємопов'язаних форм проявлення даних, що підлягають захисту від технічних розвідок: знакову та предметну. Знакова форма являє сукупність символів, літер, цифр, звуків, які відображають предмети та явища реального світу у віртуальному світі. Носіями ІзОД є документи на папері, магнітна, кіно-, відео-, фотоплівка, інші носії [5]. Також ІзОД може зберігатися, відображатися або передаватися у вигляді інформаційних сигналів [3] у формі фізичних полів (електромагнітних, оптичних, акустичних), електричних сигналів, вібраційних коливань у твердих предметах. Предметна форма існування даних проявляється самими матеріальними об'єктами реального світу у процесі виробництва й застосування продукції різного призначення [1]. Це електромагнітні, оптичні, гравітаційні, акустичні та інші поля й випромінювання, хімічні речовини.

Співвідношення між згаданими формами існування даних може бути проілюстровано (рис. 1) наступними міркуваннями.

Предмети та явища реального світу: продукція підприємств, вихідні комплектуючі та речовини, виробничі технології їх створення, способи застосування продукції у сучасному суспільстві, породжуються завдяки розробці й використанню комплектів документів, обговоренню цього безпосередньо вголос та у засобах зв'язку. При цьому віртуальний світ відображає реальний завдяки природним мовам (різних народів): вголос та письмово і штучним – кресленнями, кодами та символами, електричними сигналами та полями.

У визначенні первинності знакової і предметної форми перша частіше передує, бо у сучасному виробництві спочатку розробляють документацію, а вже потім створюють продукцію чи технологію. Фактичні співвідношення між об'єктами віртуального та реального світів наступні. Віртуальний світ (світ моделей) бідний за властивостями предметів, їх ознаками. Навпаки у реальному світі кількість властивостей предметів якщо не безмежна, то значно більша ніж у віртуальному світі. Ознаки, властивості предметів, явищ можуть проявлятися несподівано, і у небезпечному співвідношенні, не завжди можуть бути досліджені експериментально. У віртуальному світі з моделями можна проводити любі, досить ризиковані досліди.

Конкурентна боротьба вимагає добувати відомості як віртуального світу, так і реального: розвідувати ІзОД і дані предметної форми існування. Надалі не розглядаються такі шляхи здобуття даних конкурентами, як несанкціоноване придбання або викрадення документів, зразків продукції тощо. Навпаки, приділяється увага аналізу механізмів добування відомостей за рахунок використання різноманітних засобів технічних розвідок.

І останнє зауваження. Знакова форма існування ІзОД являє собою достатньо однорідні масиви даних про реальні предмети та явища світу. Структура знаків, з яких складається інформація, практично не залежить від їх змістовного навантаження. Алфавіт окремих знаків, що несуть інформацію, як правило, обмежений. Технічна апаратура розвідки може бути лише одного принципу дії. Добування інформації можливо з однієї точки. Дані щодо об'єкту розвідки можуть бути одержані задовго до виготовлення першого зразка продукції.

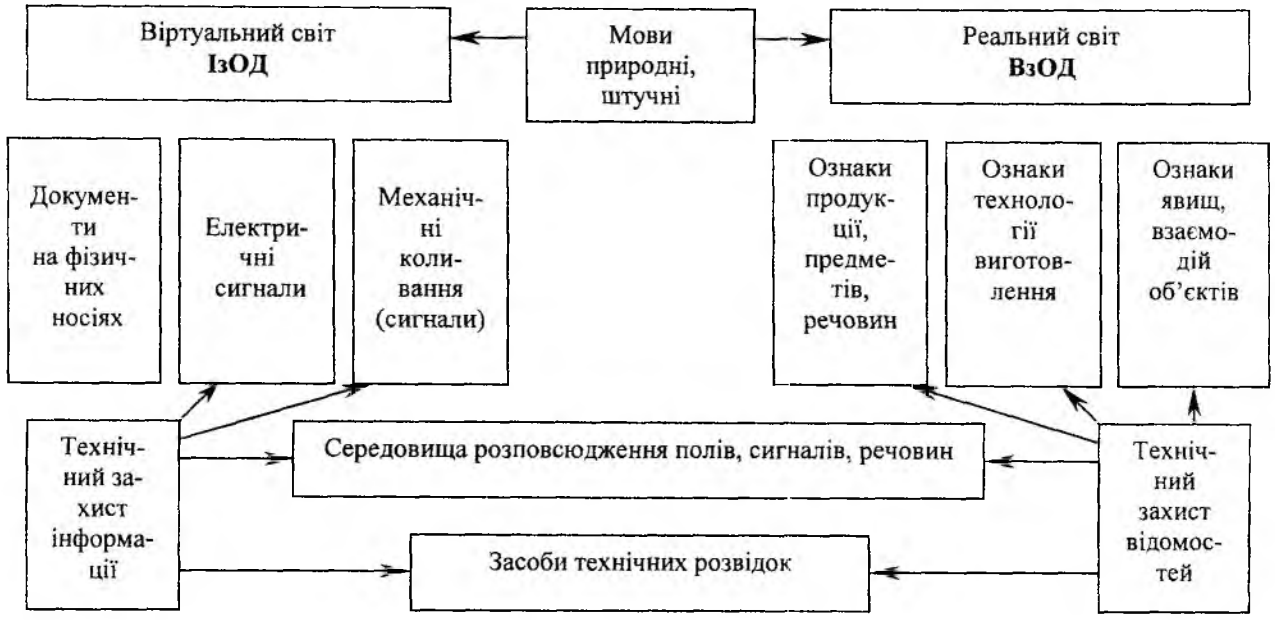

Рис. 1

Предметна форма проявлення та існування даних у наборі їх ознак потребує, як правило, різноманітної за фізикою дії апаратури розвідки, розташування такої апаратури може вимагати декількох пунктів навколо об'єктів. Дані про об'єкт можуть бути одержані лише після виготовлення або застосування першого зразка продукції речовини, нової технології.

Є потреба (хоча б у рамках даної роботи) ввести термін, що дозволить відрізняти предметну форму виразу даних від знакової. Це може бути слово «відомості». Відповідно будуть мати місце терміни «відомості з обмеженим доступом», «технічний захист відомостей» та словоскорочення: ВзОД, ТЗВ.

2 Класифікація ТКВІ знакової форми проявлення

Класифікація ТКВІ дозволяє аналізувати та детально вивчати можливі канали витоку інформації для розробки заходів захисту інформації. На сьогодні дослідження щодо створення повної класифікації ТКВІ ще не завершені. Тому у якості подальшої розробки класифікації можна запропонувати систематизувати ТКВІ за наступними критеріями (рис.2).

За *структурою* сигнали ІзОД, що циркулюють у технічних засобах передачі, обробки, зберігання, відображення інформації (ТЗПІ), поділяються на аналогові та дискретні (цифрові). Аналогові сигнали характерні аудіо- та відео- апаратурі, іншим системам і засобам, які встановлені у приміщеннях, де обговорюються питання обмеженого доступу. Дискретні сигнали характерні засобам обчислювальної техніки, цифровим факсимільним апаратам.

Наявність повторення сигналів, що циркулюють у ТЗПІ, грає суттєву роль у можливості їх розвідки. До сигналів одноразового існування можна віднести розмову, а до тих, що багато разів повторюються – електромагнітні випромінювання моніторів ПЕОМ.

За співвідношенням спектрів вихідного сигналу джерела ІзОД і того, що присутній у ТКВІ, їх можна поділити на співпадаючі, позасмугові, на гармоніках, паразитні та задані штучно. У ТКВІ зі співпадаючим спектром спектр частот, в основному, співпадає зі спектром сигналів, які циркулюють в ТЗПІ. У ТКВІ з позасмуговим спектром спектр частот такого ка-

налу наближений до спектру частот сигналу ІзОД і створюється за рахунок розширених понад заданих значень смуг частот підсилювачів, високої крутизни фронтів імпульсів.

Як правило, частоти позасмугових спектрів лежать вище частот основних спектрів сигналів. Природа ТКВІ на гармоніках обумовлена нелінійностями амплітудних характеристик

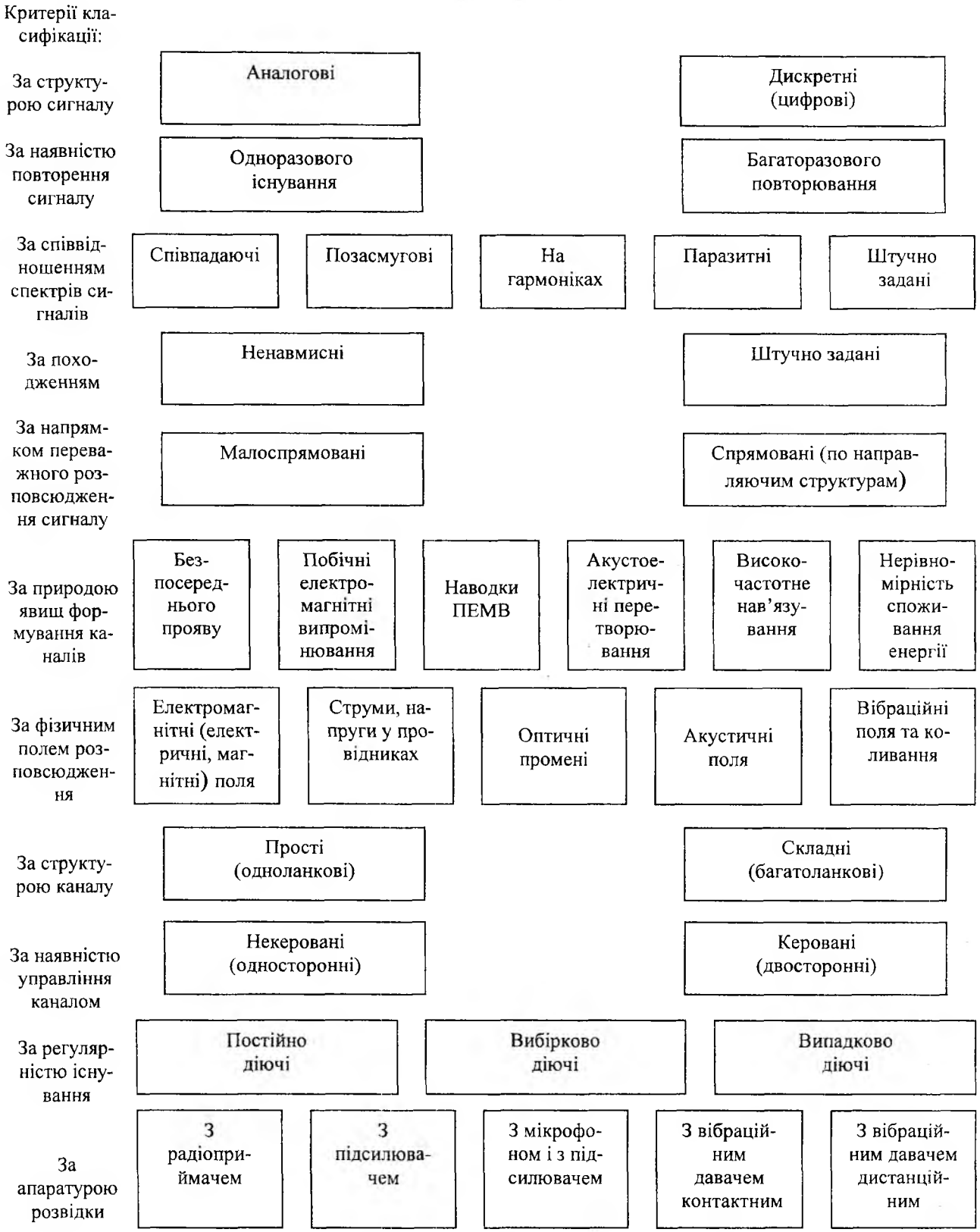

Рис. 2

підсилювачів. ТКВІ на паразитних частотах породжуються за рахунок самозбудження підсилювачів із-за паразитних зворотних зв'язків між каскадами підсилювачів. Значення їх частот обумовлені випадковими причинами виконання умов балансу фаз і амплітуд. Реактивні елементи схем, ємність p-n переходів, розподілені значення індуктивностей, ємностей монтажних проводів, тощо приводять до паразитних збуджень. Задані штучно спектри сигналів ТКВІ відносяться у цій класифікації до підкладних пристроїв і випадків зовнішнього впливу високочастотним сигналом на ТЗПІ. Наведені категорії за змістом подібні до однойменних назв введених в галузі електромагнітної сумісності [6].

За походженням ТКВІ можуть поділятися на ненавмисні та штучні. Ненавмисні ТКВІ породжуються конструктивними особливостями або недоліками апаратури. А навмисні – спеціально створюються зацікавленими в ІзОД особами.

За напрямком переважного розповсюдження ТКВІ підрозділяються на малоспрямовані та ті, що мають певну спрямованість. У малоспрямованих ТКВІ енергія електромагнітних та акустичних полів розповсюджується переважно вільно у всі сторони без особливих переваг. Направляючі структури і проводи, хвильоводи, лазерні випромінювання концентрують суттєву частину енергії ТКВІ у відповідному напрямку.

За природою явищ формування каналів ТКВІ підрозділяються на такі класи. ТКВІ безпосереднього прояву формуються, наприклад, акустичним полем розмови, яка проходить через звукоізолюючі перепони і потрапляє на спрямований мікрофон. Побічні електромагнітні випромінювання (ПЕМВ) формуються змінним електричним струмом сигналів ІзОД. Навід на провідники, що проходять навколо ТЗПІ, дають ПЕМВ. Ефектом акустоелектричних перетворювань володіють ряд приладів та апаратура: дзвоники, гучномовці тощо. Останнім часом все більше застосовується зовнішній вплив на ТЗПІ високочастотними випромінюваннями або напругами, які породжують коливання, модульовані сигналами ІзОД. Рівень споживання підсилювачем енергії залежить від сигналу, що підсилюється, а це може бути шляхом витоку ІзОД.

За фізичним полем ТКВІ поділяються на електромагнітні (електричні, магнітні), акустичні поля, вібрації, оптичні випромінювання, струми та напруги.

За структурою ТКВІ підрозділяються на прості (одноланкові) та складні (багатоланкові). Простий канал являє собою «джерело – середовище – приймач сигналу», а у складному каналі сигнал, перш ніж попаде у приймач, два чи більше разів перетворюється у фізичних носіях. Наприклад, ПЕМВ-джерела перетворюються у провідниках, розташованих поблизу ТЗПІ, у електричний струм, який цими провідниками поширюється за межі контрольованої території, де потрапляє до апаратури розвідки.

За наявністю управління ТКВІ можуть бути некерованими (односторонніми) або керованими (двосторонніми). До останніх належать керовані підкладні пристрої, лазерна апаратура зйому мовної інформації з шибок вікна, що коливаються під змінним звуковим полем.

За регулярністю існування ТКВІ підрозділяються на постійні, вибірково діючі та випадкові. Перші діють досить тривалий час, практично не змінюючи свої характеристики. Вибірково діючі ТКВІ функціонують на «замовлення» оператора. Випадкові ТКВІ суттєво змінюють свої характеристики передачі інформації у залежності від випадкових факторів, які можуть впливати на джерело або середовище розповсюдження сигналу. До випадкових ТКВІ можна віднести підсилювач звукової частоти, який самозбуджується та у якому сила самозбудження залежить від рівня сигналу на вході, напруги джерела живлення, переміщення проводів у просторі тощо.

За апаратурою розвідки ТКВІ підрозділяються на ті, що використовують апаратуру радіоприйому, підсилювачі, мікрофони, вібродавачи контактної та неконтактної дії.

Наведена класифікація ТКВІ може і надалі розширюватися в залежності від потрібного ступеню деталізації для розробки заходів ТЗІ.

3 Класифікація даних предметної форми виразу та їх ознак

На відміну від прояви знакової форми даних ВзОД та ознаки відомостей (ОВ) мають більш широкий спектр фізичного прояву, що потребує відповідної аналітичної роботи щодо їх вивчення з метою проведення подальшої класифікації. Дану роботу доцільно виконувати експертною групою із залученням фахівців, які володіють усіма сторонами розробки та застосування об'єктів дослідження.

Отже, предметні дані *за визначеністю шкал виміру* можуть бути кількісними та якісними, що ілюстровано на рис. 3. Кількісні відомості відображаються дійсними числами, які належать до відповідних шкал виміру. Це можуть бути шкали швидкості, далекості, кількості продукції, величини пропускної спроможності підприємства та ін. Для подальшого аналізу треба мати уяву про діапазон можливих значень показників і точності їх задання. Наприклад, діапазон робочих частот радіостанції – 20...60 МГц, точність настройки – 1 кГц. Якісні відомості виражають відношення об'єкту або явища до визначеного класу за сукупністю характеристик. Наприклад, тип легкового автомобіля, що розробляє фірма: масового застосування, представницький, спортивний. Формально розрізнити якісні відомості інколи буває досить важко. В такому випадку потрібно скласти таблицю за всіма можливими показниками:

потужність двигуна,
тип кузова,
типові палітри кольорів,
кількість посадочних місць,
максимальна швидкість,
час набору певної швидкості,
економічність,
обладнання салону,
розміри багажника,
габарити кузова тощо.

Далі за сукупністю співпадаючих параметрів віднести оцінюваний зразок до потрібної групи.

За проявою у повсякденній ситуації ВзОД підрозділяють на відомості безпосереднього проявлення і на відомості такі, що не проявляються. До першої групи відноситься більшість відомостей, а до другої – такі, наприклад, як стійкість автомобіля при лобовому зіткненні.

За співвідношенням часу існування і терміну часу захисту ВзОД можуть бути довготривалого або термінового часу захисту. ВзОД довготривалого часу захисту – це найчастіше за все нові технології, на розробку яких підприємство затратило великі кошти, і такі технології дають суттєву перевагу перед конкурентами. Довготривалі ВзОД потрібно захищати весь час їх існування. До термінових відомостей відносять такі, що треба захищати певний час, до якогось строку, наприклад, до початку широкого продажу продукції.

Перед проведенням аналізу ВзОД слід провести декомпозицію їх описів, привести до сукупності елементарних висловів, які б за змістом повністю перекривали зміст загального вислову. Простіше за все перевести вислів у групу висловів простих речень. Для кожного з елементарних ВзОД встановити шкали виміру, місце та час захисту.

Технічні розвідки можуть встановлювати значення ВзОД через ознаки, що супроводжують відомості. Поширений у військовій сфері термін «демаскуючі ознаки» не у повній мірі відповідає суті у напрямку захисту ВзОД, оскільки у виробничій сфері йде мова не про маскування матеріального об'єкта, а про захист його характеристик. Таким чином, надалі можна прийняти визначення, що ОВ – це фізичні поля, явища, характеристики різного роду, які піддаються виявленню та аналізу за допомогою розвідувальної апаратури і які можуть бути джерелом інформації про ВзОД. В основу цього визначення покладені підходи та визначення, прийняті у роботах, наприклад [7], А.Л. Горєліка, Г.І. Кутіна. Звідти також використані ідеї щодо критеріїв класифікації ОВ.

Ознаки, що характеризують відомості, можна класифікувати за такими критеріями.

За наближеністю до ВзОД ОВ бувають первинними та вторинними. Первинні ознаки – це фізичні характеристики об`єктів і хімічних речовин, які безпосередньо реєструються апаратурою розвідки та містять дані про ВзОД. До первинних ОВ можна віднести характеристики полів випромінювання, концентрацію хімічних середовищ, тощо. Вторинні ОВ є продуктом накопичення, обробки та аналізу первинних ОВ і дозволяють вирішувати завдання про

розпізнавання ВзОД складних об`єктів, технологій, взаємодій, явищ, хімічного складу речовин.

Критерії класифікації:

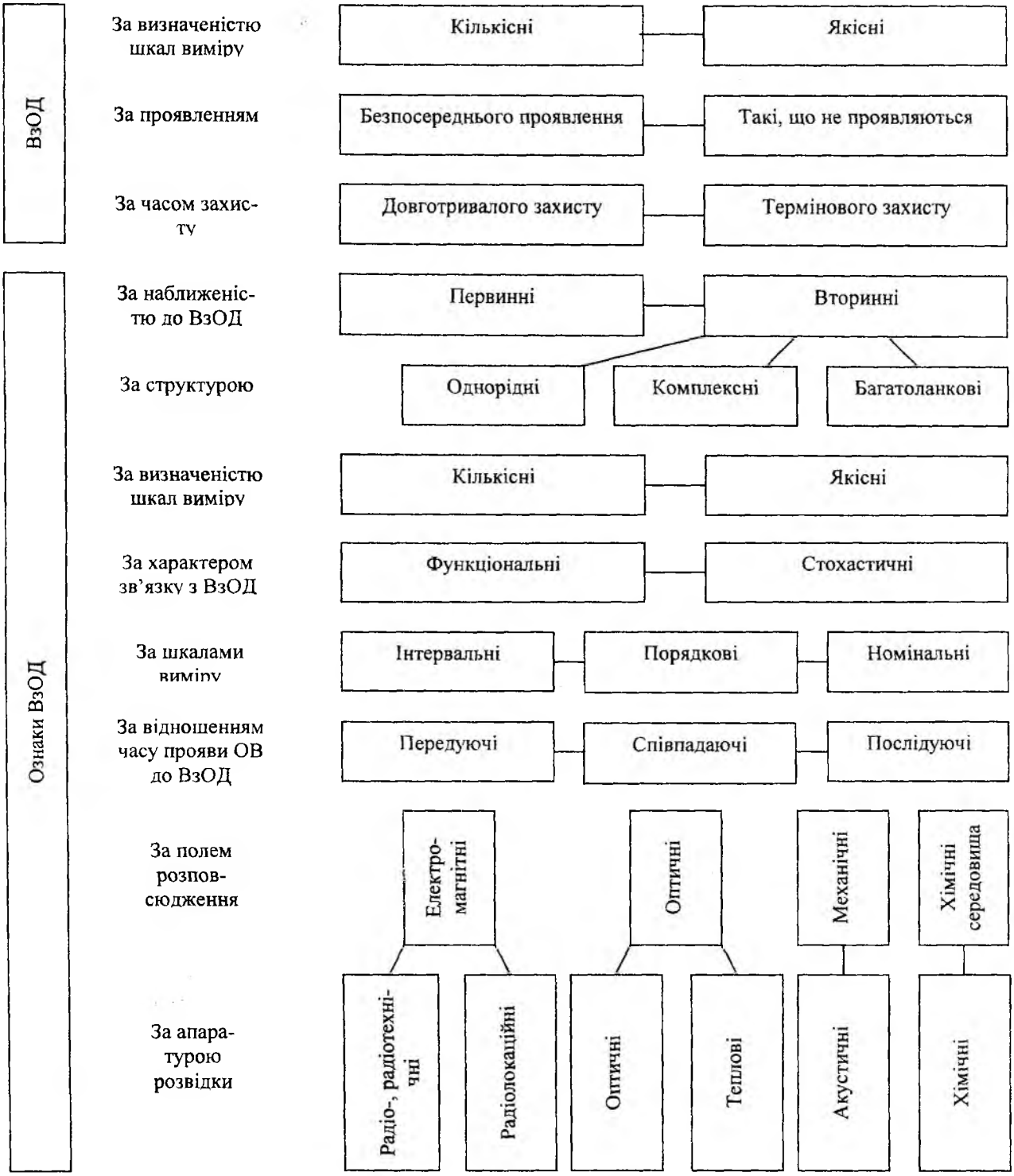

Рис. 3

За структурою вторинні ознаки можуть бути однорідні, одержані шляхом обробки однієї первинної ознаки характерної ВзОД (рівень радіосигналу, що приймає апаратура розвідки, може нести дані про діаграму спрямованості антени розвідуваного радіоелектронного засобу). Існують і комплексні ОВ, одержані на основі спостереження за комплексом різноманітних первинних або однорідних вторинних ознак, що характеризують відомості. Це, наприклад, за шумовими звуками та за хімічним складом вихлопних газів можна встановити тип двигуна, який випробовують на стенді у конструкторському бюро. Також можна відзначити і багатоланкові вторинні ОВ. Їх хронологічна або просторова прояви почергово породжує таку ознаку, що розкриває ВзОД. Прикладом цього може бути ВзОД «об'єм підземного сховища, що будується» і ланцюг ланок ОВ – кількість ходок автомашин, що вивезли ґрунт із котловану, кількість куп ґрунту на звалищі, розміри котловану, що утворився.

Як і у класифікації ВзОД ОВ можуть бути *за визначеністю шкал виміру* кількісними та якісними.

За характером зв`язку ОВ з ВзОД можуть бути функціональними (ВзОД – дальність радіозв'язку, ОВ – потужність радіопередавача) або стохастичними (ВзОД – ресурс двигуна, ОВ – час роботи двигуна до виходу з ладу).

За шкалами виміру ОВ відносять до інтервальних, порядкових і номінальних. Інтервальні ОВ відображаються дійсними числовими величинами, що характеризують ступінь прояву визначеної властивості. До інтервальних ознак можна віднести «рівень шуму двигуна» по відношенню до ВзОД «потужність двигуна». Порядкові ОВ відображаються числами – номерами, які показують місце, що займає реалізація даної ознаки у впорядкованому ряді ступеня прояви властивості. Приклад порядкових ОВ відносно ВзОД як «призначення двигуна, що розробляється» за потужністю:

для авто масового користування – 70...120 кінських сил,
для представницького авто – 150...250 кінських сил,
для спортивного авто – 250...600 кінських сил.

Номінальні ознаки, що характеризують відомості, позначаються умовними символами та відображають факт наявності або відсутності визначеної властивості. Наприклад, для відомості «тип авто, що розробляється» однією з ознак буде «відкритий кузов», що характерно для спортивного авто.

Розгляд ОВ у статичному варіанті, без урахування співвідношення їх з часом прояву ВзОД не завжди дає повну картину. Тому доцільно проводити класифікацію *за відношенням часу прояви ОВ до ВзОД*. Таким чином, можна виділити такі класи. Передуючі – такі ОВ, які виникають в часі до реальної прояви ВзОД. До такого класу належить ознака «глибина котловану» відносно до ВзОД «об'єм сховища». Співпадаючі – такі ознаки, що виникають і діють під час прояви відомості. Це – «час роботи двигуна» при його випробуванні на ресурс. Послідуючі – такі ознаки, що характеризують відомості, які виникають після прояви ВзОД. До них належать «тривалості роботи контрольних двигунів», за якими оцінюють статистичні параметри ресурсу. Кількість подібних класів, при яких враховуються співвідношення часів початків і закінчень існування відомостей та ознак, може скласти до 15-ти.

За полем розповсюдження ОВ, можуть розрізнятися на поля:

електромагнітні,
оптичні,
механічні,
хімічні середовища.

За апаратурою розвідки, яка здатна фіксувати ОВ, класифікація ТКВІ слідуюча :

радіо-, радіотехнічні,
радіолокаційні,
оптичні,
теплові (інфрачервоні),
акустичні (звукові, гідроакустичні),
хімічні.

Наведений перелік критеріїв класифікації та прийнятих для цього класів не є остаточним. Він може доповнюватися та корегуватися в залежності від поставлених завдань класифікації та розвитку науки й техніки у відповідних галузях.

Висновки

Дані про результати виробничої, проектної та іншої діяльності установ, підприємств, юридичних та фізичних осіб, які потрібно захищати від витоку по технічних каналах доцільно поділяти на інформацію та відомості (ІзОД та ВзОД).

Запропоновані підходи до класифікації технічних каналів витоку інформації і відомостей дають змогу створювати окремі моделі загроз, для їх подальшого кількісного опису і розробки відповідних заходів захисту.

Список літератури: 1. *ДСТУ3396.0-96* Захист інформації. Технічний захист інформації. Основні положення. 2. *ДСТУ3396.1-96* Захист інформації. Технічний захист інформації. Порядок проведення робіт. 3. *ДСТУ3396.2-97* Захист інформації. Технічний захист інформації. Терміни та визначення. 4. *Положение* о технической защите информации в Украине // Безопасность информации. 1996. №2. С 56-67. 5. *Закон* Украины «Об информации» // Безопасность информации. 1995. №1. С 63-72. 6. *Родионов Ю.Н.* Обеспечение ЭМС РЭС. М.: Сов. радио, 1989. 256 с. 7. *Горелик А.Л. и др.* Методы распознавания. Учебник для вузов. М.: Высшая школа, 1984. 368 с.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 19.05.2003