РАДІОТЕХНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

УДК 004.056.5
DOI https://doi.org/10.32838/TNU-2663-5941/2020.6-1/02

Клименко К.О.
Науково-дослідний інститут інформатики і права Національної академії правових наук України

Костенко О.В.
Науково-дослідний інститут інформатики і права Національної академії правових наук України

Ільченко О.М.
незалежний дослідник

ЗАГАЛЬНА КЛАСИФІКАЦІЯ ЗАСОБІВ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ ТА МЕТОДИК ЇХ ВИЯВЛЕННЯ

У статті розглядається одне з головних завдань у сучасному інформаційному суспільстві – забезпечення безпеки інформації від потай встановлених на об'єкті інформаційної діяльності технічних засобів негласного отримання інформації, які створюють загрозу її витоку. Розглянуто їх класифікацію та демаскуючі ознаки. Розроблено підхід до вибору рекомендацій та обґрунтування показників ефективності заходів із захисту інформації можливо впроваджених засобів негласного отримання інформації.

Зазначається вплив новітніх інформаційно-комунікаційних технологій практично на всі сфери життєдіяльності людини та державних інституцій, а також на інноваційний розвиток сучасного інформаційного суспільства. Зауважується на масштабне застосування різноманітних інформаційних технологій як у діяльності спеціальних державних служб, так і окремими приватними суб'єктами спрямоване на отримання доступу до всіх видів даних та інформації із застосуванням засобів негласного отримання інформації.

Запропоновано класифікувати засоби негласного отримання інформації за конструктивними особливостями та принципом дії, за різновидом інформації, яка перехоплюється, за типами датчиків перехоплення інформації, за видами сигналів і діапазону частот передавання перехопленої інформації, за періодом роботи пристроїв, видами камуфляжу, способом живлення тощо. Також класифікації піддано різновиди демаскуючих ознак, притаманних різним видам засобів негласного отримання інформації, а також засоби та методи пошуку потай встановлених на об'єкті інформаційної діяльності технічних засобів негласного отримання інформації, які створюють загрозу її витоку.

Розглянуто і сукупність варіацій заподіяння шкоди внаслідок застосування на об'єкті інформаційної діяльності засобів отримання інформації. Запропоновано застосувати інтегральні показники оцінки заподіяної шкоди, які характеризують вартість втрат для суб'єктів під час втручання у їхні інформаційні ресурси сторонніх осіб з метою доступу до інформації, що оброблюється, втручання в інформаційні системи, кібератаки на інформаційні ресурси, реєстри, бази даних, електронні системи управління тощо.

Ключові слова: *інформація, безпека інформації, перехоплення інформації, технічні засоби негласного отримання інформації, закладний пристрій, канал витоку інформації, власники інформації, заходи із захисту інформації, показники ефективності, інформаційні відносини.*

Постановка проблеми. Підвищення рівня захищеності об'єктів інформаційної діяльності в Україні шляхом запобігання впровадженню потай встановлених технічних засобів негласного отримання інформації, які створюють загрозу її витоку (далі – ЗП) [1], захист об'єктів інформаційної діяльності від впровадження ЗП є сьогодні актуальним завданням як підприємств різних форм власності, так і суспільства загалом. Визначальним у цьому аспекті є розроблення рекомендацій щодо вибору й обґрунтування показників ефективності заходів із захисту інформації від її витоку за рахунок можливо впроваджених на об'єкті інформаційної діяльності засобів негласного отримання інформації, які створюють загрозу її витоку.

Таким чином, поєднання невисокої ціни та виключно високої ефективності, а також відсутність можливості на рівні держави викрити

механізми придбання і встановлення на об'єктах інформаційної діяльності технічних засобів негласного отримання інформації, що створюють загрозу її витоку, роблять цей канал витоку інформації одним із найнебезпечніших.

Аналіз основних досліджень і публікацій. У наукових працях вітчизняних спеціалістів у сфері захисту інформації проблеми комплексного технічного захисту об'єктів і методик виявлення закладних пристроїв висвітлено достатньо широко (А.А. Хорев, В.І. Ярочкин, В.В. Баканов, В.Б. Шумбар, І.М. Машковский, Г.О. Максименко, С.В. Биков, К.І. Яковлев, В.О. Хорошко, Д.В. Чирков, В.В. Єрмошин).

Однак недостатньо дослідженими лишаються питання, пов'язані із класифікацією засобів негласного отримання інформації з урахуванням впливу на сферу захисту інформації розвитку сучасних інформаційно-комунікаційних технологій.

Постановка завдання. Дослідити потенційні напрями застосування сучасних засобів негласного отримання інформації, запропонувати їх сучасну класифікацію, впорядкувати методики їх виявлення та надати рекомендації щодо удосконалення сфери захисту інформації, в т. ч. і для захисту інформаційних ресурсів України.

Виклад основного матеріалу дослідження. Розвиток інформаційно-комунікаційних технологій безпосередньо впливає на сфери діяльності всіх країн світу і є пріоритетним напрямом інноваційного розвитку та сучасного інформаційного суспільства. Водночас інформаційні технології широко використовуються як спеціальними державними службами, так і окремими юридичними та фізичними особами з метою отримання доступу до інформації та втручання в інформаційні системи, кібератак на інформаційні ресурси, реєстри, бази даних, електронні системи управління державними органами та підприємствами критичної інфраструктури. Одним із ефективних напрямів такої діяльності стало застосування засобів негласного отримання інформації.

Засоби негласного отримання інформації за конструктивними особливостями та принципом дії [7–9] можна поділити на такі типи (рис. 1):

1. За видом інформації, яка перехоплюється ЗП: акустична, видова, перехоплення інформації з основних технічних засобів (далі – ОТЗ) та допоміжних технічних засобів (далі – ДТЗС).

2. За видом датчика перехоплення інформації: мікрофон, вібродатчик, гальванічне підключення до лінії, індуктивний / ємнісний датчик, оптичні перетворювачі, приймальні антени.

3. За видом сигналу передавання перехопленої інформації: радіоканал, електричний сигнал, що розповсюджується комунікаціями, сигнали оптичного діапазону, вібраційні хвилі, акустичні хвилі, ультразвукові хвилі.

4. За діапазоном частот передавання перехопленої інформації: звукові частоти, ультразвукові частоти, радіодіапазон, оптичний діапазон.

5. За способом формування сигналу передавання інформації: без перетворення, з перетворенням (складні види модуляції, шифрування тощо).

6. За періодом роботи: постійно діючі, таймерні, активація зовнішнім датчиком (керування голосом, датчиком руху, тощо), дистанційне керування накопиченням і передачею за короткий проміжок часу.

7. Наявність камуфляжу: без камуфляжу, камуфльовані під предмети інтер'єру або речі.

8. За способом передавання інформації: пряме передавання, передавання через ретранслятор.

9. За способом живлення: автономні джерела живлення (елементи живлення, акумулятори, сонячні батареї, радіоізотопні джерела тощо), живлення від стаціонарних мереж у місці встановлення (силова або слабкострумова мережа), живлення зовнішнім опроміненням.

10. За способом встановлення: без порушення цілісності будівельних конструкцій та інтер'єру, з порушенням цілісності.

11. За видом комунікацій, які використовують ЗП: легально прокладені на об'єкті встановлення ЗП, потай прокладені комунікації ЗП.

Виявлення можливо впроваджених на об'єкті інформаційної діяльності ЗП здійснюється відповідно до наведеної вище класифікації та за їх демаскуючими ознаками.

Основними демаскуючими ознаками ЗП [3; 4], що дозволяють проводити їх виявлення та ідентифікацію, є:

– випромінювання в радіодіапазоні (до десятків ГГц) з ознаками модуляції інформацією, яка циркулює на об'єкті інформаційної діяльності [4];

– випромінювання в радіодіапазоні від передавача ЗП, що в безпосередній близькості значно перевищує рівень сигналу від інших джерел випромінювань у радіодіапазоні, у т. ч. і загальнодержавних мовних станцій [4];

– наявність побічних випромінювань у радіодіапазоні, зокрема випромінювань на другий і третій гармоніках, субгармоніках тощо [4];

– опромінення об'єкта інформаційної діяльності спрямованим (зондуючим) потужним випромінюванням (зазвичай гармонійним) [3; 4];

– наявність у приміщеннях об'єкта інформаційної діяльності перевипроміненого зондуючого випромінювання з амплітудною або частотною модуляцією інформацією, що циркулює на об'єкті інформаційної діяльності;

– тонкий дріт невідомого призначення, зазвичай екранований, приховано прокладений на об'єкті інформаційної діяльності, що виходить в інше приміщення (суміжне приміщення, підвал, горище тощо) або сусідню будівлю;

– наявність у лінії (дроті) невідомого призначення, прокладеній на об'єкті інформаційної діяльності, постійної (кілька вольт) напруги та низькочастотного інформативного сигналу;

– наявність у металевих конструкціях (елементах приточно-витяжної вентиляції, армування огороджувальних конструкцій об'єкта, трубної розводки або системи опалення та водопостачання тощо) постійної напруги (декілька вольт);

– наявність струму витоку (від одиниць до декількох десятків мА) в лінії електроживлення об'єкта інформаційної діяльності за всіх без винятку відключених споживачів;

– відмінність ємності лінії електроживлення об'єкта інформаційної діяльності від типових значень (значення лінії суміжного об'єкта інформаційної діяльності) за відключення лінії від джерела живлення (на розподільчому щитку елек-

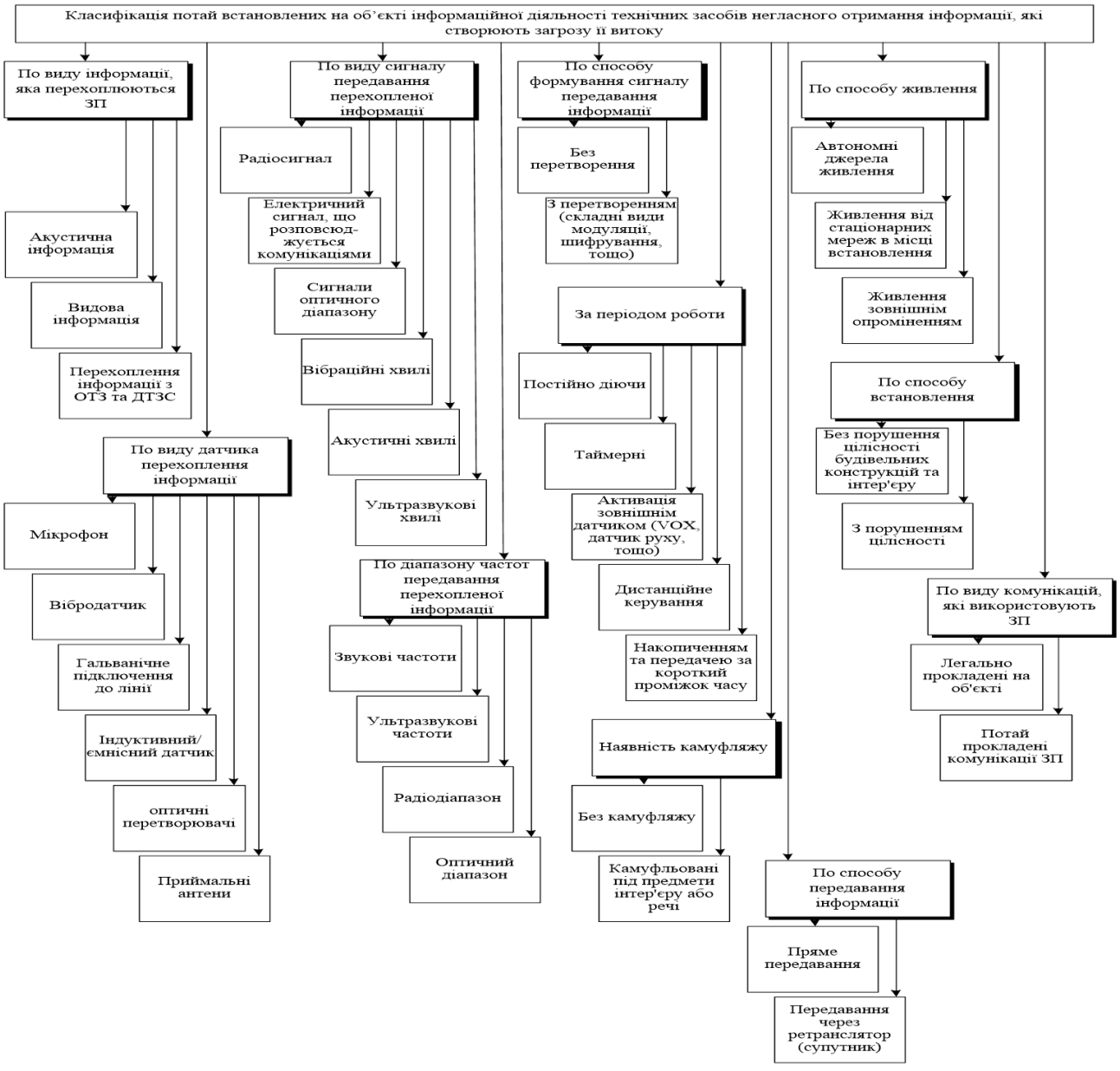

Рис. 1. Класифікація технічних засобів негласного отримання інформації

троживлення) та відключення всіх без винятку споживачів;

– наявність у лінії електроживлення об'єкта інформаційної діяльності високочастотного сигналу (зазвичай несуча частота від 40 до 600 кГц, але можлива наявність сигналу на частотах до 15 МГц), модульованого інформативним низькочастотним сигналом;

– наявність струму витоку (від одиниць до декількох десятків мА) в телефонній лінії об'єкта інформаційної діяльності за відключеного телефонного апарата;

– падіння напруги (від декількох десятих до 1,5–2 В) в телефонній лінії (щодо інших телефонних ліній, підключених до відповідної розподільчої коробки) при покладеній і піднятій телефонній трубці телефонного апарата, встановленого на об'єкта інформаційної діяльності;

– відмінність опору телефонної лінії об'єкта інформаційної діяльності від типового значення (для цієї лінії) при відключенні телефонного апарата і відключення лінії (від'єднання телефонних дротів) на розподільчий коробці (щитку) або кросовій об'єкта;

– придушення (не проходження) одного-двох викликів при наборі номера телефонного апарата.

Додатковими демаскуючими ознаками ЗП [3; 4], що дозволяють проводити їх виявлення та ідентифікацію, є:

– малогабаритний предмет невідомого походження та призначення, що знаходиться на об'єкті інформаційної діяльності та має одне або кілька отворів малого діаметра в корпусі;

– наявність невеликого відрізка дроту або кількох дротів, що виходить із корпусу малогабаритного предмета невідомого походження;

– наявність малогабаритного предмета на об'єкті інформаційної діяльності, походження якого невідоме і до якого підключений малогабаритний мікрофон, що знаходиться в термоусадці або пластиковій трубці;

– наявність збірок автономних елементів живлення (акумуляторних батарей) або блоків живлення невідомого призначення, які не належать до систем та / або обладнання об'єкта інформаційної діяльності;

– наявність у малогабаритних предметах невідомого походження та призначення напівпровідникових елементів, що виявляються при обстеженні їх локатором нелінійностей;

– наявність у малогабаритних предметах невідомого походження та призначення провідників або інших деталей, які виявляються при просвічуванні рентгенівськими променями.

Крім того, на об'єкті інформаційної діяльності можуть бути впроваджені камуфльовані ЗП, що за зовнішнім виглядом не відрізняються від об'єкта імітації, особливо якщо ЗП встановлюється в корпус побутового предмета без зміни його зовнішнього вигляду. Камуфльовані ЗП, які встановлюються в малогабаритні предмети, обмежують можливості останніх. Ці обмеження можуть служити непрямими ознаками закладних пристроїв.

У ряді випадків камуфльовані ЗП виявляються за наявністю в обстежуваному предметі не властивих йому напівпровідникових елементів, що виявляється при обстеженні предмета локатором нелінійностей. Деякі камуфльовані ЗУ не відрізняються від оригіналів навіть за ретельного зовнішнього огляду. Їх можна виявити тільки при просвічуванні предметів рентгенівськими променями.

Крім того, щоб виключити можливість виявлення ЗП шляхом розбирання, місця з'єднань частин склеюють кустарним способом.

Вивчення й узагальнення матеріалів вітчизняної та зарубіжної преси за останні роки, а також матеріали, розміщені в мережі Internet, свідчать про те, що суб'єкти оперативно-розшукової діяльності та фірми-виробники при розробці та виробництві ЗП приділяють особливу увагу скритності їх роботи.

Крім того, провідні країни віддають перевагу науковим дослідженням і розробкам у сфері мікромеханіки. Західні експерти вважають, що унікальні технології в поєднанні з новітніми засобами мікроелектроніки вже в недалекій перспективі дозволять створити і налагодити промисловий випуск надмалих інтегральних пристроїв, які мають функції роботів. Розміри подібних конструкцій обмежуватимуться міліметрами. Вони застосовуватимуться в різних сферах життя, включаючи інформаційно-технічну боротьбу. Таким чином, подальший розвиток ЗП [7–9], швидше за все, буде здійснюватися за такими основними напрямами, як:

– мініатюризація закладних пристроїв на основі сучасних досягнень у галузі мікроелектроніки;

– зниження їх електроспоживання та / або перехід на живлення від стаціонарних мереж у місці їх встановлення;

– розробка технічних і схемних рішень у напрямі підвищення просторової, частотної, енергетичної, тимчасової, структурної та інформаційної скритності роботи ЗП. Зокрема, як рішення для ЗП можуть використовуватися:

а) цифрові та імпульсні види модуляції;

б) накопичення перехопленої інформації та її передача за короткий проміжок часу;

в) застосування для передачі перехопленої інформації шумоподібних сигналів;

г) застосування для передачі нових, більш високих діапазонів частот від десятків до сотень ГГц;

д) використання для передачі перехопленої інформації спеціальних вузькоспрямованих антенних систем;

е) максимальне зниження потужності передавача;

ж) застосування для передачі перехопленої інформації наявних у країні мереж стільникового зв'язку тощо;

– розробка і створення мініатюрних керованих засобів доставки ЗП на об'єкт інформаційної діяльності;

– розробка і впровадження засобів ретрансляції перехопленої інформації, що використовують для передачі на пункти контролю мережі загального користування, та відповідні протоколи обміну даними;

– розвиток і вдосконалення систем дистанційного керування ЗП;

– розробка джерел автономного електроживлення на нових принципах побудови;

– розробка та вдосконалення вже наявних пасивних і напівактивних ЗП – ендовібраторів. Використання для їхньої роботи наявних мереж загального користування.

Позитивні результати, отримані при проведені інформаційно-технічних заходів із використанням потай встановлених на об'єкті інформаційної діяльності технічних засобів негласного отримання інформації, які створюють загрозу її витоку, дозволяють прогнозувати можливість їх широкого використання в Україні найближчим часом.

Пошук і виявлення закладних пристроїв здійснюється з використанням пошукової апаратури: детекторів відеокамер, індикаторів поля зі функцією частотоміра, радіоприймачів і аналізаторів спектра, програмно-апаратних комплексів, апаратури для перевірки провідних ліній, локаторів нелінійностей, рентгенівських комплексів, металошукачів, тепловізорів, ультразвукових та інших приладів і допоміжного обладнання.

Послідовність етапів виявлення ЗП [2–4]:

1. Підготовчий етап:

– обстеження та вивчення об'єкта інформаційної діяльності (вивчення та попередній огляд);

– визначення заходів і способів активації ЗП і вимог до тестових сигналів, вибір (розробка) тестових сигналів;

– вибір технічних засобів, приладів та обладнання, необхідних для проведення робіт;

– розробка плану проведення пошукових робіт;

– попередній аналіз радіочастотної обстановки (в т. ч. випромінювань в оптичному діапазоні частот) за межами (в оточенні) ОІД;

– розподіл сил пошукової групи, технічних засобів, приладів та обладнання за місцем і часом проведення робіт.

2. Основний етап:

– заходи з активації ЗП, що, можливо, встановлені на ОІД;

– заходи з виявлення прихованих систем відеоспостереження;

– аналіз радіочастотної обстановки в межах ОІД (у т. ч. випромінювань в оптичному діапазоні частот) та ідентифікація виявлених сигналів;

– заходи з локалізації виявлених на ОІД джерел радіовипромінювання;

– пошук ЗП, встановлених (підключених) на проводових комунікаціях, що розташовані на ОІД (проходять через ОІД);

– пошук ЗП методами неруйнівного контролю (за допомогою нелінійних локаторів, металошукачів, рентгенівських комплексів, тепловізорів, ультразвукових та інших приладів неруйнівного контролю);

– пошук ЗП, встановлених на / у будівельних, огороджувальних та оздоблювальних конструкціях (матеріалах), меблях, предметах інтер'єру, сувенірах, технічних засобах тощо, які розміщені на ОІД.

Найпростішими і найбільш дешевими пошуковими пристроями для виявлення ЗП є індикатори електромагнітного поля із функцією індикації частоти, які світловим або звуковим сигналом сигналізують про наявність у точці розташування антени електромагнітного поля з напруженістю, вищою за порогову (встановлену).

Чутливість індикаторів електромагнітного поля мала, тому вони дозволяють виявляти радіовипромінювання ЗП в безпосередній близькості від них. Істотно кращу чутливість мають спеціальні радіоприймачі з можливістю автоматизованого скануванням радіодіапазону. Вони забезпечують пошук у діапазоні частот від десятків кГц до десятків ГГц.

Найкращі можливості для пошуку ЗП з передачею перехопленої інформації в радіодіапазоні мають аналізатори спектра. Крім перехоплення радіовипромінювань закладних пристроїв, вони дозволяють аналізувати їхні характеристики, що важливо при виявленні ЗП, які використовують для передачі інформації складні види модуляції.

Можливість сполучення сучасних спеціальних радіоприймачів із переносними комп'ютерами

послужило основою для створення автоматизованих комплексів для пошуку ЗП (програмно-апаратних комплексів контролю).

Крім програмно-апаратних комплексів, побудованих на базі приймачів із функцією сканування радіодіапазону і переносних комп'ютерів, для пошуку закладних пристроїв використовуються спеціально розроблені багатофункціональні комплекси типу «OSCOR» або його аналоги.

Спеціальні комплекси та / або апаратура для контролю проводових ліній дозволяють проводити вимірювання параметрів (напруги, струмів, опорів тощо) телефонних, слабкострумових ліній і ліній електроживлення, а також виявляти в них сигнали закладних пристроїв.

Велику групу утворюють пошукові пристрої, призначені для виявлення та / або локалізації закладних пристроїв за фізичними властивостями елементів електричних схем, що входять до їх складу, або елементів їх конструкцій. Нині найбільш достовірні результати забезпечують засоби для виявлення напівпровідникових елементів по їх нелінійним властивостями – локатори нелінійностей.

Принцип роботи локаторів нелінійностей близький до принципів роботи радіолокаційних станцій, широко застосовуваних для радіолокаційної розвідки об'єктів. Істотна відмінність полягає в тому, що, якщо приймач радіолокаційної станції приймає перевипромінений об'єктом зондуючий радіосигнал на частоті випромінюваного радіосигналу, то приймач локатора нелінійностей приймає 2-ю і 3-ю гармоніки перевипроміненого радіосигналу. Поява у перевипроміненому сигналі цих гармонійних складових частин зумовлена нелінійністю характеристик напівпровідникових елементів.

Металошукачі дозволяють виявляти ЗП за наявності в них металевих елементів конструкцій, насамперед металевих корпусів ЗП або інших металевих елементів конструкцій.

Переносні рентгенівські комплекси застосовуються для виявлення камуфльованих ЗП або ЗП, призначення яких не вдається виявити без їх розбирання, насамперед тоді, коли розбирання неможливе без руйнування знайденого об'єкта.

Рекомендації з вибору й обґрунтування показників ефективності заходів із захисту інформації від її витоку за рахунок можливо впроваджених засобів негласного отримання інформації, які створюють загрозу її витоку.

Вибір показників ефективності заходів із захисту інформації (далі – заходів ЗІ) від її витоку за рахунок можливо впроваджених засобів негласного отримання інформації, які створюють загрозу її витоку, визначаються такими факторами, як призначення методик; технологія оцінки ефективності та вибір заходів ЗІ; цільове призначення заходів із ЗІ, яке полягає в запобіганні шкоди суб'єктам інформаційних відносин (далі – ІВ) від загроз безпеці інформації [5; 6].

Виходячи з призначення методик, загальної технології оцінки ефективності та вибору заходів захисту інформації, можна сформулювати деякі вимоги до показників ефективності заходів із ЗІ:

– показники ефективності повинні вибиратися з урахуванням системного підходу до дослідження питань оцінки ефективності та вибору заходів ЗІ, тобто з урахуванням завдань, що вирішуються у процесі аналізу та синтезу;

– на етапі аналізу для оцінки ступеня небезпеки загроз витоку інформації за рахунок ЗП бажано, щоб показники ефективності могли набувати абсолютні значення;

– на етапі синтезу показники ефективності повинні забезпечувати можливість проведення порівняльної оцінки різних за характером і способом реалізації заходів ЗІ, тому бажано, щоб зазначені показники могли вимірюватися у відносних одиницях.

З огляду на те, що цільовим призначенням заходів ЗІ є запобігання загрозам інформації, як показники ефективності заходів ЗІ повинні бути обрані показники запобігання шкоди з використанням цих заходів суб'єктами інформаційних відносин від загроз витоку інформації.

Як суб'єкти інформаційних відносин розглядаються: користувачі інформації, особи, про яких інформація гласно або негласно накопичується й обробляється, власники інформації або уповноважені ними органи та / або організації з правом володіння і розпорядження, власники та користувачі інформації, органи управління інформацією.

Для вибору показників, що характеризують збиток від загроз витоку інформації через впровадження ЗП, необхідно проаналізувати механізм виникнення збитків від цих загроз безпеці інформації (далі – БІ).

На нашу думку, шкода від порушення безпеки інформації за рахунок можливо впроваджених ЗП на типовому об'єкті інформаційної діяльності є наслідком таких подій (рис. 2):

– загрози БІ за рахунок перехоплення інформації, що обробляється технічними засобами обробки інформації, встановленими на об'єкті інформаційної діяльності;

– загрози БІ за рахунок перехоплення фізичних полів, які створюються основними та

допоміжними технічними засобами, встановленими на об'єкті інформаційної діяльності;

– загрози БІ за рахунок людей – носіїв інформації та / або маючих доступ до інформації у процесі її обробки.

Як приклад, для встановлення причинно-наслідкових зав'язків, що описують процес виникнення збитків суб'єктам інформаційних відносин внаслідок порушення безпеки інформації через застосування ЗП, розглянемо наслідки впливу загроз витоку інформації з об'єкта інформаційної діяльності: перехоплення інформації, яка обробляється технічними засобами обробки інформації, встановленими на об'єкті інформаційної діяльності, втрата відомостей як про окремі елементи, так і про об'єкт інформаційної діяльності загалом, перехоплення елементів доступу як до технічних засобів (залежно від типу засобу), так і на ОІД загалом, репутаційні (судові позиви, пов'язані з розголошенням інформації) та фінансова шкода, погіршення якості функціонування технічних засобів, яке може проявлятися як погіршення їх тактико-технічних характеристик (часових, енергетичних, частотних тощо).

З огляду на те, що технічні засоби обробки інформації, встановлені на об'єкті інформаційної діяльності, є матеріальною основою процесу обробки інформації на ОІД, перехоплення елементів доступу та / або погіршення їх тактико-технічних характеристик (далі – ТТХ) автоматично веде до зниження ефективності процесу обробки інформації і далі, через зниження ефективності завдань, що вирішуються, до зниження ефективності функціонування ОІД загалом.

У свою чергу, це призводить до втрат та / або витрат, які несуть ОІД, вид і масштаб яких визначаються такими факторами:

– змістом інформації, що обробляється на ОІД;

– сферою застосування (використання) результатів обробки інформації (вихідної інформації);

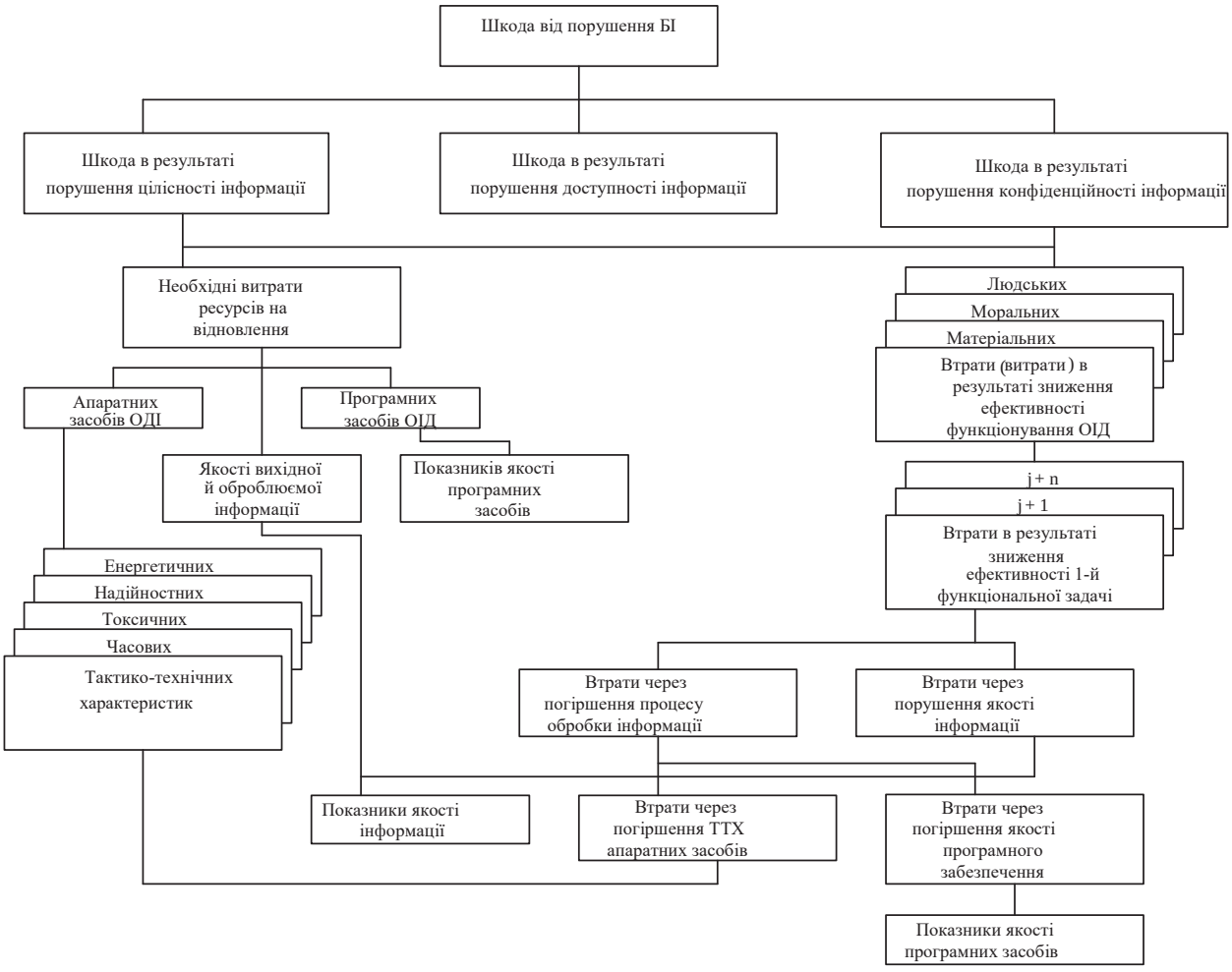

Рис. 2. Шкода від загроз безпеці інформації

– ступенем та обсягом інформації;

– видом джерела загроз інформації та метою його діяльності.

Аналогічні наслідки виникають у разі впливу загроз БІ на програмні засоби, що використовуються у процесі обробки інформації на ОІД, а також впливу загроз БІ на фізичні поля – носії інформації і на людей – носіїв інформації та / або маючих доступ до інформації у процесі її обробки (персонал ОІД, користувачі ОІД, джерела інформації).

Як інтегральний показник для оцінки заподіяної шкоди обраний показник «вартість втрат внаслідок порушення БІ», який загалом є функцією від декількох показників нижнього рівня, що залежать від виду порушення БІ (порушення цілісності, доступності та / або конфіденційності інформації), а також від виду втрат, серед яких можна виділити:

– витрати на відновлення апаратних, програмних засобів і якості інформації;

– втрати внаслідок зниження ефективності функціонування ОІД.

Більш конкретний зміст показників заподіяної шкоди на цьому рівні залежить від конкретних умов, тобто від того, які показники обрані для оцінки ефективності функціонування ОІД (рис. 3). Наприклад, для автоматизованих систем управління залежно від їх призначення як показник ефективності може бути використаний один із таких

– середній час циклу управління;

– середній час обробки інформації;

– середній час виконання сукупності розрахунків;

– середній час доведення інформації до споживача тощо.

Отже, як показники заподіяної шкоди можуть бути використані:

– відносне або абсолютне збільшення середнього часу циклу управління або відповідна цій події вартість втрат для суб'єктів ІВ;

– відносне або абсолютне збільшення середнього часу обробки інформації або відповідна цій події вартість втрат для суб'єктів ІВ тощо.

Кожен із цих показників, у свою чергу, є функцією від показників більш низького ієрархічного рівня:

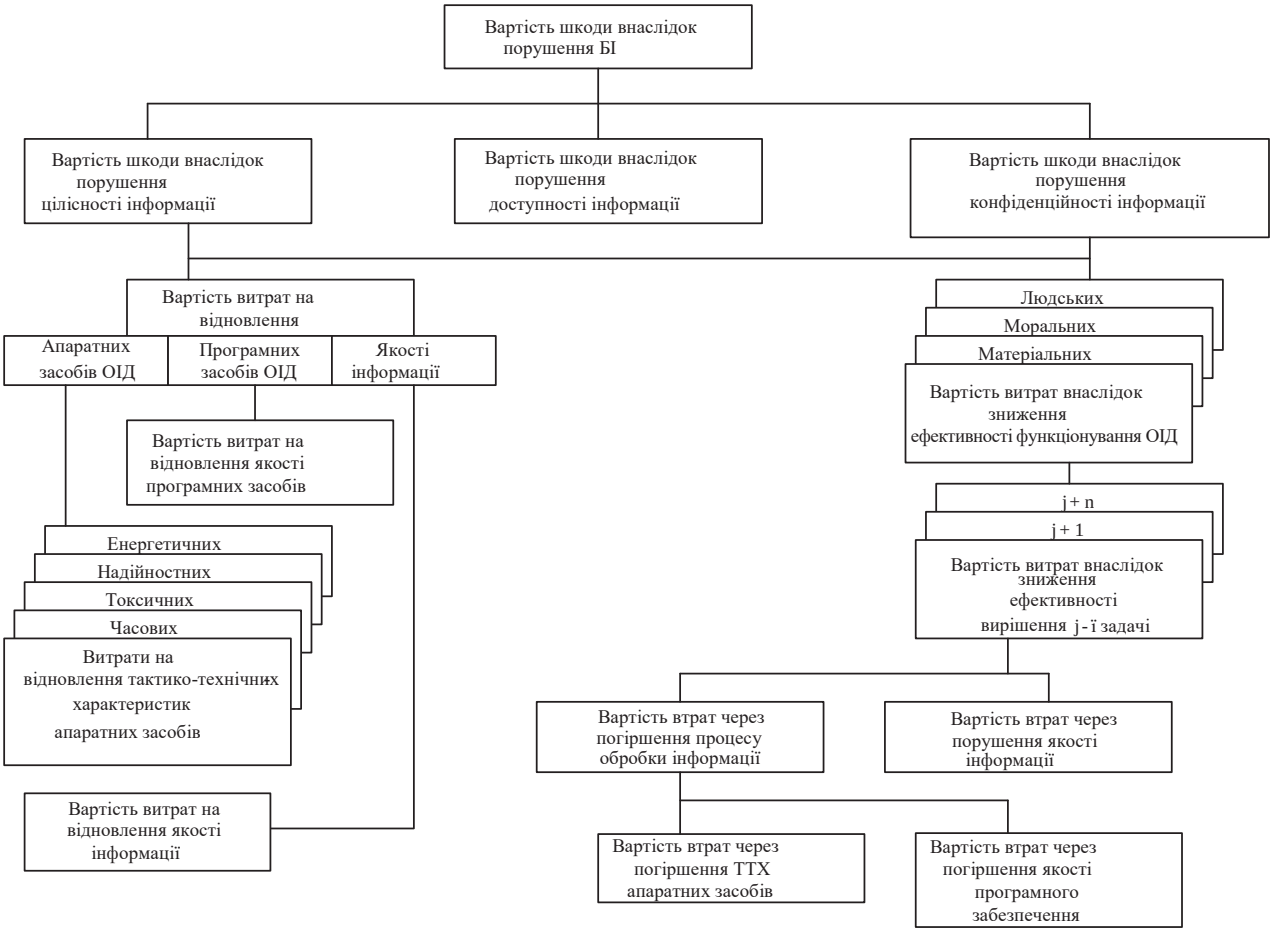

Рис. 3. Ієрархія видів шкоди від загроз безпеці інформації

– показників ефективності розв'язуваних об'єктом приватних функціональних завдань;

– показників ефективності процесу обробки інформації;

– показників якості вихідної та оброблюваної на об'єкті інформації;

– показників якості функціонування апаратних і програмних засобів.

Кожен із цих показників є функцією від показників більш низького ієрархічного рівня:

– показників ефективності розв'язуваних об'єктом окремих функціональних завдань;

– показників ефективності процесу обробки інформації;

– показників якості вихідної й оброблюваної на об'єкті інформації;

– показників якості функціонування апаратних і програмних засобів.

Кожен із перерахованих показників також може бути представлений системою показників ще більш низького рівня. Наприклад, для апаратних засобів такими показниками можуть служити тактико-технічні характеристики, вид і допустимі межі зміни котрих вказуються у формулярі на ці засоби.

Ця ж система показників може бути використана і для оцінки ефективності заходів ЗІ, якщо її розглядати як здатність запобігати заподіянню шкоди суб'єктам ІС від порушення БІ.

Для вибору проблемно-орієнтованої системи показників, тобто системи показників, які «покривають» конкретні умови ОІД, необхідно, виходячи з наведених вище рекомендацій, сформувати свою систему показників ефективності заходів ЗІ, прив'язавши її до конкретних умов експлуатації ОІД з урахуванням: призначення, сфери використання ОІД, завдань, що вирішуються на ОІД, найімовірніших видів і джерел загроз БІ, показників, які прийняті для оцінки ефективності ОІД та вирішуються на ОІД окремих функціональних завдань, структури та складу ОІД, моделі процесу обробки інформації на ОІД, змісту інформації, що обробляється на ОІД, тощо.

Висновки. Підсумовуючи вищевикладене, можна констатувати, що подальше широке застосування ЗП буде здійснюватися не лише суб'єктами оперативно-розшукової діяльності, а і політичними або бізнесовими угрупуваннями в Україні з метою як здійснення фінансового впливу на суб'єкта господарювання різних форм власності, так і зміни політичного курсу країни загалом.

Отже, за сучасних умов безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації. Комплексна система захисту інформації повинна бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки за повсякденних умов, але й у критичних ситуаціях.

Список літератури:

1. ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни і визначення. Київ : Держстандарт України, 1998. 19 с.

2. НД ТЗІ 2.7-011-2012. Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв. Київ: Адміністрація Державної служби спеціального зв'язку та захисту інформації України, 2012. 11 с.

3. Хорев А.А. Методы и средства поиска электронных устройств перехвата информации. Москва : МО РФ, 1998. 224 с.

4. Максименко Г.А. Принцип поиска радиозакладных устройств по максимальному уровню принимаемого сигнала. *Сборник научных трудов. КВИУС*. 1998. № 5. С. 224–230.

5. Хрошко В.А. Выбор критериев для оптимизации систем технической защиты информации. *Сборник научных трудов. КМУГА*. 1999. С. 7–9.

6. Ильченко А.Н., Хорошко В.О., Чирков Д.В., Браиловский М.М., Ермошин В.В. Алгоритм визначення доцільності застосування систем захисту інформації. *Збірник наукових праць. Європейський університет*. 2001.

7. Каталог фирмы COFREXPORT: Специальная техника: FRANCE, 1996. 48 с.

8. Каталог фирмы WESTIMGHOUSE Audio Intelligence Devices (WAID): Специальная техника: USA, 1996. 63 с.

9. Каталог фирмы Gesellschaft fur FunkkommuniKatation und Goniometrie GmbH (FUGON): Специальная техника: Germany

Klymenko K.O., Kostenko O.V., Ilchenko O.M. GENERAL CLASSIFICATION OF MEANS OF COVERT OBTAINING OF INFORMATION AND METHODS OF THEIR DETECTION

The article presents the task of ensuring the security of information, as one of the main in the modern information society, from the secretly installed on the object of information technical means of covert receipt of information, which pose a threat of its leakage. Their classification and unmasking features are considered. An approach to the selection of recommendations and substantiation of indicators of effectiveness of information protection measures of possibly implemented means of covert information retrieval has been developed.

The influence of the newest information and communication technologies on practically all spheres of human life and state institutions, as well as on innovative development and modern information society is noted. There is a large-scale application of various information technologies both in the activities of special public services and by individual private entities, aimed at gaining access to all types of data and information through the use of covert means of obtaining information.

It is proposed to classify the means of covert information retrieval according to design features and principle of operation, type of intercepted information, types of information interception sensors, types of signals and frequency range of intercepted information, device operation period, camouflage types, power mode, etc. Also classified are the types of unmasking features inherent in different types of means of covert information, as well as means and methods of searching for secretly installed on the object of information technical means of covert information, which pose a threat of its leakage.

The set of variations of causing damage as a result of application of means of obtaining information on the object of information activity is also considered. It is proposed to use integrated indicators of damage assessment, which characterize the cost of losses for entities during the intervention and their information resources of outsiders, in order to access the processed information, interference in information systems, cyber attacks on information resources, registers, databases, electronic control systems, etc.

Key words: *information, information security, information interception, technical means of secret information retrieval, embedded device, information leakage channel, information holders, information protection measures, efficiency indicators, information relations.*