1977, – № 1410 – 638 с. ***15.*** *Буланкин В. И. Исторические аспекты правовой природы общесоюзных перечней сведений, составляющих государственную тайну// Труды НИИ "Прогноз" КГБ СССР – М., 1982 – вып.2 - № 1096 – с.46 – 63.* ***16.*** *Положение о Центральном Управлении по делам печати при Главполитпросвете Наркомпроса УССР // Центральний архів вищих органів влади та управління України (ЦДАВОВ), Ф. 2, Оп. 2, Спр. 378 - с. 57 – 58.* ***17.*** *Постановление СНК УССР от 16 января 1924 г. „Об организации при Государственном Политическом Управлении УССР „Специального отдела" // ЦДАВОВ, Ф. 1, Оп. 2, Спр. 2238 - с. 18.* ***18.*** *"Инструкция по секретному делопроизводству" від 1928 р.// Державний Архів СБ України, Ф. 9, Спр. 610 – с. 222 – 254.* ***19.*** *История служб и органов противодействия техническим разведкам (История Гостехкомисии) //http: //www. vif2.ru/ users/ offtopic/ vio/ VIO/ IST31. HTM.* ***20.*** *Розанов И. С, Попов Ф. Д. Административно-правовой режим охраны государственных секретов в СРСР- М., 1976 - № 442 – 159 с.* ***21.*** *Рубанов В. "От культа секретности" – к информационной культуре"// "Коммунист" – М., 1988 – № 13 – с. 24 – 36.* ***22.*** *Рубанов В. А. Основные направления перестройки режимно-секретной деятельности //Труды НИИ «Прогноз» КГБ СССР – М., 1988 – вып. 8 - № 1101 – с. 6 – 20.*

УДК 681.3.06

ОБ'ЄКТИ ЗАХИСТУ ІНФОРМАЦІЇ. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Володимир Василюк
Інститут захисту інформації з обмеженим доступом Національної академії Служби безпеки України

Анотація: **Наведено узагальнюючу схему можливих каналів витоку і несанкціонованого доступу до інформації, оброблюваної в типовому одноповерховому офісі.**
Summary: **In the article the author represented generalized scheme of possible ways of leak and unauthorized access to the information processed at standard one-storeyed office.**
Ключові слова: **Інформація з обмеженим доступом, технічній захист інформації, технічні канали витоку інформації.**

І Вступ

Однією з відмінних, визначних ознак сучасного світового соціального прогресу є зростання значимості інформації в суспільних відносинах.

Суспільні інформаційні відносини постійно розвиваються, особливо з удосконаленням техніки та технологій збирання, обробки, зберігання та передавання інформації. Зазначені процеси визначають сутність інформаційного суспільства. Поряд із позитивними здобутками в інформаційному суспільстві виникли соціальні проблеми криміногенного характеру, які потребують вирішення.

Завдання забезпечення інформаційної безпеки старі як цей світ. На сучасному етапі можна виділити три підходи до її рішення:

- перший (приватний) підхід ґрунтується на рішенні приватних завдань забезпечення інформаційної безпеки; цей підхід є малоефективним, але досить часто використовується, тому що не вимагає значних фінансових і інтелектуальних витрат;
- другий (комплексний) підхід ґрунтується на рішенні комплексу приватних завдань єдиної програми; цей підхід наразі є основним;
- третій (інтегральний) підхід заснований на інтеграції різних підсистем зв'язку, підсистем забезпечення безпеки в єдину систему із загальними технічними засобами, каналами зв'язку, програмним забезпеченням і базами даних.

Третій підхід спрямований на досягнення інтегральної інформаційної безпеки. Поняття інтегральної безпеки припускає обов'язкову безперервність процесу забезпечення безпеки як у часі, так і в просторі (за всім технологічним циклом діяльності) з обов'язковим обліком всіх можливих видів загроз (несанкціонований доступ, знімання інформації, тероризм, пожежа, стихійні лиха й т. п.).

Застосування інтегрального підходу пов'язане з рішенням ряду складних різнопланових окремих завдань у їхньому тісному взаємозв'язку. Найбільш очевидними з них є завдання обмеження доступу до інформації, технічного й криптографічного закриття інформації, обмеження рівнів паразитних випромінювань технічних засобів, технічної захищеності об'єктів, охорони й оснащення їх тривожною сигналізацією. Однак необхідні рішення й інших, не менш важливих завдань. Так, наприклад, виведення з ладу керівників підприємства, членів їхніх родин або ключових працівників може поставити під сумнів

саме існування даного підприємства. Цьому ж можуть сприяти стихійні лиха, аварії, тероризм і т. п.

Необхідною умовою реалізації інтегрального підходу є блокування всіх технічних каналів витоку й несанкціонованого доступу до інформації, тому для створення ефективних систем безпеки в першу чергу необхідно досліджувати можливі канали витоку [аналіз загроз (ризиків), як реальних (діючих у цей момент), так і потенційних (здатних у майбутньому)] і їхні характеристики.

II Об'єкти захисту інформації та особливості технічних каналів витоку і несанкціонованого доступу

Захист інформації – це сукупність організаційних, технічних та правових заходів, спрямованих на запобігання нанесенню збитків інтересам власника інформації.

Основними об'єктами захисту інформації є [1 – 3]:

3. інформація з обмеженим доступом (ІзОД), тобто інформаційні ресурси, зокрема, ті, що містять відомості, які належать або до таємної, або до конфіденційної інформації;
4. технічні засоби приймання, обробки, зберігання та передання інформації (ТЗПІ), а саме: системи та засоби інформатизації (обчислювальна техніка, інформаційно-обчислювальні комплекси, мережі та системи); програмні засоби (операційні системи, системи керування базами даних та інше загально системне і прикладне програмне забезпечення); автоматизовані системи керування; системи зв'язку; технічні засоби отримання, передання та обробки ІзОД (звукозапис, звукопідсилення, звукосупроводження, переговорні та телевізійні пристрої; засоби тиражування і виготовлення документів та інші технічні засоби обробки графічної, алфавітно-цифрової та текстової інформації), їх інформативні фізичні поля;
5. допоміжні технічні засоби і системи (ДТЗС), тобто технічні засоби і системи, які не належать до ТЗПІ, але розташовані в приміщеннях, де оброблюється ІзОД; до них відносять технічні засоби відкритого телефонного або гучномовного зв'язку, системи пожежної та охоронної сигналізації, система енергопостачання, радіотрансляційна мережа, система часофікації, енергопобутові прилади тощо, а також самі приміщення, де циркулює ІзОД.

За результатами аналізу матеріалів вітчизняної й закордонної преси [1 – 9] на рис. наведено узагальнюючу схему можливих каналів витоку і несанкціонованого доступу до інформації, оброблюваної в типовому одноповерховому офісі.

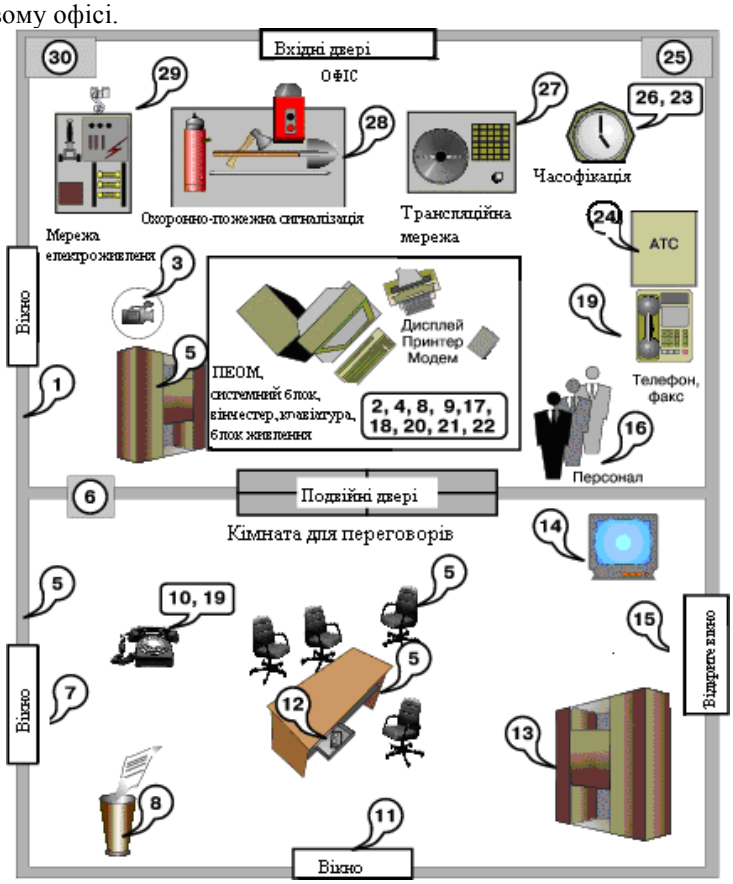

Рисунок – Схема каналу витоку і несанкціонованого доступу до інформації в типовому одноповерховому офісі:

1. витік за рахунок структурного звуку в стінах і перекриттях;
2. знімання інформації зі стрічки принтера, погано стертих дискет і т. п.;
3. знімання інформації з використанням відеозакладок;
4. програмно-апаратні закладки в ПЕОМ;
5. радіо-закладки в стінах і меблях;
6. знімання інформації з системи вентиляції;
7. лазерне знімання акустичної інформації з вікон;
8. виробничі й технологічні відходи;
9. комп'ютерні віруси, логічні бомби й т. п.;
10. знімання інформації за рахунок наведень і "нав'язування";
11. дистанційне знімання відео інформації (оптика);
12. знімання акустичної інформації з використанням диктофонів;
13. розкрадання носіїв інформації;
14. високочастотний канал витоку в побутовій техніці;
15. знімання інформації спрямованим мікрофоном;
16. внутрішні канали витоку інформації (через обслуговуючий персонал);
17. несанкціоноване копіювання;
18. витік за рахунок побічного випромінювання термінала;
19. знімання інформації за рахунок використання "телефонного вуха";
20. знімання з клавіатури й принтера акустичним каналом;
21. знімання з дисплея по електромагнітному каналу;
22. візуальне знімання з дисплея й принтера;
23. наведення на лінії комунікацій і сторонні провідники;
24. витік через лінії зв'язку;
25. витік мережею заземлення;
26. витік мережею часофікації;
27. витік трансляційною мережею й гучномовним зв'язком;
28. витік охоронно-пожежною сигналізацією;
29. витік мережею електроживлення;
30. витік мережею опалення, газо- і водопостачання.

Розглянемо більш докладно особливості каналів витоку і несанкціонованого доступу до інформації. Далі в тексті цифри в круглих дужках відповідають позначенням на рисунку.

Як елементи каналів витоку інформації найбільший інтерес становлять ТЗПІ та ДТЗС із виходом за межі контрольованої зони (КЗ), тобто зони, де виключена можливість появи осіб чи транспортних засобів без постійних чи тимчасових перепусток [3].

Окрім з'єднувальних ліній ТЗПІ та ДТЗС за межі КЗ можуть виходити дроти та кабелі, які їх не стосуються, але проходять через приміщення, де встановлено такі технічні засоби, а також металеві труби опалення, водопостачання та інші струмопровідні металоконструкції. Такі дроти, кабелі та струмопровідні елементи називають сторонніми провідниками.

Перехоплення інформації, оброблюваної на об'єктах ТЗПІ, здійснюється технічними каналами. Під технічним каналом витоку інформації (ТКВІ) розуміють сукупність об'єкта розвідки, технічного засобу розвідки (ТЗР), за допомогою якого отримують інформацію про цей об'єкт, та фізичного середовища, в якому поширюється інформаційний сигнал. По суті, ТКВІ – це спосіб отримання за допомогою ТЗР інформації про об'єкт розвідки. При цьому форма подання інформації може бути довільною.

Сигнали є матеріальними носіями інформації. За своєю фізичною природою вони можуть бути електричними, електромагнітними, акустичними, оптичними тощо. Залежно від природи сигнали поширюються у визначених фізичних середовищах – газових, рідинних, твердих (наприклад, у повітрі, конструкціях будівель, струмопровідних кабелях та дротах, заземленому ґрунті тощо).

Принцип утворення небезпечних сигналів у технічних засобах полягає в тому, що кожний технічний засіб містить ті чи інші фізичні перетворювачі, функції яких засновані на різних фізичних принципах дії. Лише маючи уявлення про принцип дії кожного з таких перетворювачів, можна виявити неконтрольовані прояви фізичних полів, що утворюють канали витоку [4].

Розглянемо спочатку електромагнітні, електричні й параметричні технічні канали витоку інформації.

Через електромагнітні ТКВІ перехоплюють:

- побічні електромагнітні випромінювання (ПЕМВ) елементів ТЗПІ (18), (21);
- ПЕМВ на частотах роботи високочастотних генераторів ТЗПІ й ДТЗС (14);

- ПЕМВ на частотах самозбудження низької частоти підсилювачів (ТЗПІ) (27).

Побічні електромагнітні випромінювання ТЗПІ перехоплюють засобами радіотехнічної розвідки, розміщеними за межами КЗ.

Електричні ТКВІ слугують для знімання:

- наведених сигналів ПЕМВ ТЗПІ зі з'єднувальних ліній ДТЗС і сторонніх провідників (23);
- інформаційних сигналів з ліній електроживлення ТЗПІ (29);
- інформаційних сигналів з мереж заземлення ТЗПІ і ДТЗС (25);
- інформації шляхом розміщення в ТЗПІ електронних пристроїв перехоплення інформації (5).

Останні іноді називають закладними пристроями або апаратними закладками. Вони являють собою мініпередавачі, сигнали від яких модулюються інформаційними сигналами.

Параметричні ТКВІ створюють ВЧ опроміненням ТЗПІ (10). Для перехоплення інформації цими каналами потрібні ВЧ генератори з антенами, що мають вузьку діаграму спрямованості, а також спеціальні радіоприймальні пристрої.

У повітряних (прямих акустичних) ТКВІ середовищем поширення є повітря. Для перехоплення акустичних сигналів використовують мікрофони (15). Сигнали з мікрофонів або записуються на пристрої звукозапису, або транслюються передавачами на пункти приймання.

Для перехоплення акустичної (мовної) інформації використовують:

- портативні диктофони (12) та дротові мікрофони для прихованого звукозапису;
- спрямовані мікрофони;
- акустичні радіозакладки для передавання інформації по радіоканалу;
- акустичні мережні закладки для передавання сигналів по лініях силових мереж електроживлення;
- акустичні ІЧ закладки для передавання інформації по оптичному каналу в ІЧ діапазоні;
- акустичні телефонні закладки для передавання інформації по телефонних лініях зв'язку на підвищених частотах;
- акустичні телефонні закладки типу «електронне вухо» (19) для передавання інформації по телефонній лінії «телефону-спостерігачу» на низькій частоті.

У вібраційних (віброакустичних) ТКВІ середовищем поширення акустичних сигналів є конструкційні елементи споруд і будівель (стіни, перекриття, підлога), труби водопостачання, каналізації та інші тверді тіла (1), (30).

Для перехоплення акустичних коливань через вібраційні ТКВІ використовують ТЗР із контактними мікрофонами:

- електронні стетоскопи;
- радіостетоскопи (для передавання інформації радіоканалом).

Акустичні ТКВІ виникають за рахунок перетворення акустичних сигналів у електричні (акустоелектричні перетворення) і дозволяють перехоплювати акустичні коливання через ДТЗС із мікрофонним ефектом, а також ВЧ нав'язуванням.

Наприклад, приєднуючи такі ДТЗС до ліній зв'язку телефонних апаратів з електромеханічним дзвінком виклику, можна підслуховувати розмови у приміщеннях, де розміщені такі апарати.

Створити ТКВІ методом ВЧ нав'язування можна шляхом несанкціонованого контактного введення ВЧ струму від генератора, підключеного до лінії (кола), яка має функціональний зв'язок з нелінійним чи параметричним елементом ДТЗС, на яких здійснюється модуляція ВЧ сигналу інформаційним (10). Останній в елементах ДТЗС з'являється внаслідок акустоелектричного перетворення акустичних сигналів у електричні (21), (27). У зв'язку з тим, що нелінійні або параметричні елементи ДТЗС для ВЧ сигналу, як правило, являють собою неузгоджені навантаження, промодульований ВЧ сигнал буде випромінюватися або відбиватися від нього і поширюватись у зворотному напрямку по лінії. Для приймання випроменених або відбитих ВЧ сигналів використовують спеціальні високочутливі приймачі.

Оптико-електричний (лазерний) ТКВІ утворюється під час опромінення лазерним променем вібруючих в акустичному полі тонких відбиваючих поверхонь [скляних вікон, картин, дзеркал і т. п. (17)]. Для перехоплення мовної інформації таким каналом використовують складні лазерні акустичні локаційні системи (ЛАЛС). Іноді їх називають лазерними мікрофонами.

Параметричні ТКВІ утворюються під час ВЧ опромінення приміщення, де вмонтовані напівактивні закладні пристрої або технічні засоби з елементами, деякі параметри яких змінюються за законом зміни акустичного (мовного) сигналу (14). Для перехоплення інформації таким каналом потрібен спеціальний передавач із направленим променем і приймач.

Необхідно відзначити, що акустичний канал може бути джерелом витоку не тільки мовної інформації. В літературі описані випадки, коли за допомогою статистичної обробки акустичної інформації з принтера

або клавіатури вдавалося перехоплювати комп'ютерну текстову інформацію (20), у тому числі здійснювати знімання інформації з системи вентиляції (6).

Особливий інтерес представляє перехоплення інформації при її передачі каналами зв'язку (24). Як правило, в цьому випадку є вільний несанкціонований доступ до переданих сигналів. Залежно від виду каналів зв'язку, технічні канали перехоплення інформації можна розділити на електромагнітні, електричні і індукційні.

Електромагнітні випромінювання передавачів засобів зв'язку, які модульовані інформаційними сигналоми, можуть перехоплюватися з використанням стандартних технічних засобів. Цей електромагнітний канал перехоплення інформації широко використовується для прослуховування телефонних розмов, що ведуться за допомогою радіотелефонів, стільникових телефонів або радіорелейними і супутниковими лініями зв'язку (21).

Електричний канал перехоплення інформації, що передається кабельними лініями зв'язку, припускає контактне підключення до цих ліній. Цей канал найчастіше використовується для перехоплення телефонних розмов, при цьому перехоплюється інформація, що, може бути записана на диктофон або передана радіоканалом.

Безпосереднє електричне підключення апаратури перехоплення є компрометуючою ознакою, тому частіше використовується індукційний канал перехоплення, що не потребує контактного підключення до каналів зв'язку. Сучасні індукційні датчики, за повідомленнями відкритої преси, здатні знімати інформацію з кабелів, захищених не тільки ізоляцією, але й подвійною бронею зі сталевої стрічки й сталевого дроту, що щільно обвивають кабель.

Останнім часом значну увагу становлять канали витоку графічної інформації, що реалізуються технічними засобами у вигляді зображень об'єктів або копій документів, які одержуються шляхом спостереження за об'єктом, зйомкою об'єкту та зйомкою (копіюванням) документів. Залежно від умов спостереження використовуються відповідні технічні засоби, у тому числі: оптика [біноклі, підзорні труби, телескопи, монокуляри (11)], телекамери, прилади нічного бачення, тепловізори й т. п. Для документування результатів спостереження проводиться зйомка об'єктів, для чого використовуються фотографічні й телевізійні засоби, що відповідають умовам зйомки. Для зняття копій документів використовуються електронні й спеціальні (закамуфльовані) фотоапарати. Для дистанційного знімання видової інформації використовують відеозакладки (3).

Розглянуті вище методи одержання інформації засновані на використанні зовнішніх каналів витоку. Необхідно, однак, коротко зупинитися й на внутрішніх каналах витоку інформації, тим більше, що їм не приділяють належної уваги. Внутрішні канали витоку (16) зв'язані, як правило, з адміністрацією та обслуговуючим персоналом, з якістю організації режиму роботи. З них, у першу чергу, слід зазначити такі канали, як розкрадання носіїв інформації (13), знімання інформації зі стрічки принтера й погано стертих дискет (2), використання виробничих і технологічних відходів (8), візуальне знімання інформації з дисплея й принтера (22), несанкціоноване копіювання (17) і т. п.

III Методи й засоби блокування каналів витоку інформації

Захист інформації від витоку технічними каналами забезпечують проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням портативних закладних пристроїв [5, 6].

Організаційні заходи – це спрямовані на захист інформації заходи, проведення яких не потребує спеціально розроблених технічних засобів.

До основних організаційних заходів відносять:

- залучення до робіт для захисту інформації організацій, що мають ліцензії відповідних органів на діяльність в області технічного захисту інформації (ТЗІ);
- категорування й атестацію об'єктів ТЗПІ та приміщень, виділених для проведення секретних заходів (виділених приміщень) щодо відповідності вимогам забезпечення захисту інформації під час проведення робіт з відомостями відповідного ступеня секретності;
- використання на об'єкті сертифікованих ТЗПІ та ДТЗС;
- встановлення КЗ навколо об'єкта;
- залучення до робіт із монтування апаратури, будування чи реконструкції об'єктів ТЗПІ організацій з відповідними ліцензіями;
- організацію контролю та обмеження доступу на об'єкти ТЗПІ та у виділені приміщення;
- введення територіальних, частотних, енергетичних, просторових і часових обмежень у режимах

використання технічних засобів, що підлягають захисту;

- відключення технічних засобів, що мають елементи властивостей електроакустичних перетворювачів, від ліній зв'язку на період проведення секретних заходів.

Технічні заходи - це спрямовані на захист інформації заходи, проведення яких передбачає використання спеціальних технічних засобів, а також реалізацію технічних рішень.

Технічні заходи слугують для закриття каналів витоку інформації за рахунок ослаблення рівня інформаційних сигналів або зменшення відношення сигнал /завада у місцях можливого розміщення ТЗР або їх датчиків до рівнів, що унеможливлюють виділення інформаційних сигналів засобами розвідки. Під час проведення таких заходів використовують активні та пасивні методи.

До технічних заходів із використанням пасивних методів відносять такі:

1. контроль і обмеження доступу на об'єкти ТЗПІ та у виділені приміщення (установлення на об'єктах ТЗПІ та у виділених приміщеннях технічних засобів та систем обмеження і контролю доступу);
2. локалізація випромінювання:
   - екранування ТЗПІ та з'єднувальних ліній;
   - заземлення ТЗПІ та екранів їх з'єднувальних ліній;
   - звукоізолювання виділених приміщень;
3. розв'язування інформаційних сигналів:
   - установлення спеціальних захисних засобів типу Граніт, Рікас у ДТЗС із мікрофонним ефектом і таких, що мають вихід за межі КЗ;
   - установлення спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалення, водозабезпечення і каналізації, що виходять за межі КЗ;
   - установлення автономних або стабілізованих пристроїв електроживлення ТЗПІ (наприклад, мотор-генераторів);
   - установлення в мережах електроживлення ТЗПІ, а в лініях освітлювальної та розеткової мережі виділених приміщень - завадоподавляючих фільтрів типу ФП, ФСП, ФС-2.

До технічних заходів із використанням активних методів належать такі:

1. просторове зашумлення:
   - просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад відповідними засобами (за умови виявлення та з'ясування частоти випромінювання закладного пристрою або ПЕМВ ТЗПІ);
   - створення акустичних і вібраційних завад із використанням генераторів акустичного шуму – шумотронів;
   - подавлення працюючих у режимі запису диктофонів за допомогою подавляючих пристроїв.
2. лінійне зашумлення:
   - мереж електроживлення та кіл заземлення;
   - сторонніх дротів та з'єднувальних ліній ДТЗС, що виходять за межі КЗ;
3. знешкодження підключених до лінії закладних пристроїв за допомогою спеціальних генераторів імпульсів (випалювачів «жучків»).

Виявити закладні пристрої можна завдяки спеціальним обстеженням (візуальний огляд без залучення технічних засобів) і спеціальним перевіркам (із використанням технічних засобів) об'єктів ТЗПІ та виділених приміщень.

Для виявлення закладних пристроїв використовують:

1) пасивні методи:
   - установлення засобів і систем виявлення лазерного випромінювання (підсвітлення скла на вікнах);
   - установлення стаціонарних детекторів диктофонів;
   - розшук закладних пристроїв за допомогою індикаторів поля, інтерсепторів, частотомірів, сканувальних приймачів та програмно-апаратних комплексів контролю;
   - організація радіоконтролю (постійно або на час проведення конфіденційних заходів) побічних електромагнітних випромінювань ТЗПІ;
2) активні методи:
   - спеціальна перевірка виділених приміщень із використанням нелінійних локаторів;
   - спеціальна перевірка виділених приміщень, ТЗПІ та ДТЗІ з використанням рентгенівських комплексів.

У табл. 1 зведено розглянуті вище канали витоку інформації й можливі методи їхнього блокування.

Таблиця 1 – Основні методи й засоби несанкціонованого одержання інформації й можливий захист від них

N п/п	Дії людини (типова ситуація)	Канали витоку інформації	Методи та засоби одержання інформації	Методи та засоби захисту інформації
1	Розмова в приміщенні або на вулиці	Акустика Віброакустика Гідроакустика Електроакустика	Підслуховування, диктофон, мікрофон, спрямований мікрофон, напівактивна система, стетоскоп, вібродатчик, гідроакустичний датчик, радіотехнічні спецприймачі	Шумові генератори, пошук закладок, захисні фільтри, обмеження доступу
2	Розмова по провідному телефону	Акустика Електросигнал у лінії наведення	Аналогічно п. 1 паралельний телефон, пряме підключення, електромагнітний датчик, диктофон, телефонна закладка	Аналогічно п. 1 Маскування, скремблювання, шифрування Спецтехніка
3	Розмова по радіотелефону	Акустика, електромагнітні хвилі	Аналогічно п. 1 радіоприймальні пристрої	Аналогічно п. 1 Аналогічно п.2
4	Документ на паперовому носії	Наявність	Крадіжка, візуально, копіювання, фотографування	Обмеження доступу, спецтехніка
5	Виготовлення документа на паперовому носії	Наявність Паразитні сигнали, наведення	Аналогічно п. 4 спеціальні радіотехнічні пристрої	Аналогічно п. 1 екранування
6	Поштове відправлення	Наявність	Крадіжка, прочитання	Спеціальні методи захисту
7	Документ на не паперовому носії	Носій	Розкрадання, копіювання, зчитування	Контроль доступу, фізичний захист, криптозащита
8	Виготовлення документа на не паперовому носії	Зображення на дисплеї Паразитні сигнали, наведення	Візуально, копіювання, фотографування Спеціальні радіотехнічні пристрої	Контроль доступу, криптозащита
9	Передача документа каналами зв'язку	Електричні і оптичні сигнали	Несанкціоноване підключення, імітація зареєстрованого користувача	Криптозащита
10	Виробничий процес	Відходи, випромінювання й т. п.	Спецапаратура різного призначення, оперативні заходи	Оргтехзаходи, фізичний захист

Таким чином, безпека досягається комплексним застосуванням апаратних, програмних і криптографічних методів, і засобів захисту, а також організаційних заходів.

IV Висновок

Бурхливий розвиток сучасних технологій і технічних засобів сприяє постійному розширенню спектра можливих каналів витоку інформації, тому дослідження каналів витоку стає все більше актуальним, і складним завданням.

На ефективність систем безпеки істотно впливають характеристики каналів витоку інформації, тому створення систем ефективного захисту має відбуватися з урахуванням особливостей реальних каналів. Цей висновок не є тривіальним, як може здатися на перший погляд. Наприклад, сам факт наявності випромінювання дисплея ще не говорить про витік інформації. Усе визначається конкретним рівнем напруженості поля за межами зони безпеки й технічних можливостей противника, тому остаточний висновок про витік інформації може зробити тільки кваліфікований фахівець, що використовує спеціальні технічні засоби. З іншого боку, особливості реальних каналів витоку інформації можуть бути успішно використані й противником для забезпечення несанкціонованого доступу до інформації, про що необхідно

постійно пам'ятати. Так, знімання інформації з акустичних каналів може бути здійснено через стекла вікон, будівельні, сантехнічні, вентиляційні, теплотехнічні й газорозподільні конструкції, з використанням для передачі сигналів радіо, радіотрансляційних, телефонних і комп'ютерних комунікацій, антенних, і телевізійних розподільних мереж, охоронно-пожежної й тривожної сигналізації, мереж електроживлення й часофікації, гучномовного й диспетчерського зв'язку, ланцюгів заземлення й т. п. Випадковий пропуск хоча б одного можливого каналу витоку може звести до нуля всі витрати й зробити систему захисту неефективної неефективною.

Література: ***1.*** *Лаврентьев А. В. Организация в офисах защиты информации от утечки по техническим каналам. – Безопасность информации. – 1996. - № 3. – С. 62 – 66.* ***2.*** *Лаврентьев А. В. Анализ технических каналов утечки информации и классификация технических средств разведки.* - Безопасность информации. – *2000. - №4. – С. 32 – 38.* ***3.*** *Архипов О. Є, Луценко В. М., Худяков В. О. Захист інформації в телекомунікаційних мережах та системах зв'язку: Учеб. пособие. - К.: Політехніка, 2003 – 38 с.* ***4.*** *Петраков А. В., Лагутин В. С. Утечка и защита информации в телефонных каналах святи.* - М.: *Энергоатомиздат, 1997. – 304 с.* ***5.*** *Куренков Е. В., Лысов А. В., Остапенко А. Н. Рекомендации по оценке защищенности конфиденциальной информации от ее утечки за сет ПЭМИ. - Защита информации.—1998. – № 4. – С. 48 – 50.* ***6.*** *Хорев А. А. Способы и средства защиты информации: Учеб. пособие.* - М.: МО РФ, *1998. – 316 с.* ***7****. Калинцев Ю. Л. Конфиденциальность и защита информации: Учеб. пособие по курсу «Радиовещание и электроакустика». – М.:МТУСИ, 1997.- 60 с.* ***8.*** *Шаповалов П. П. Поиск и оперативное пересечение негласного съема информации. – М.: ЗАО «Щит», 2000. – 83 с.* ***9****. Ярочкин В. И. Информационная безопасность. – М.: Международные отношения, 2000. – 400 с.*

УДК 65.012.8

ДЕЯКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В ПРОВІДНИХ КРАЇНАХ СВІТУ

Сергій Князєв

Інститут захисту інформації з обмеженим доступом Національної академії СБ України

Анотація: **Розглядаються деякі особливості охорони інформації з обмеженим доступом в провідних країнах світу.**

Summary: **Under research are some features of classified data protection in leading countries of the world.**

Ключові слова: **Захист інформації, інформація з обмеженим доступом.**

І Вступ

Інформація є досить специфічним продуктом. Закон України "Про інформацію" під поняттям "інформація" розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі. Встановлення й реалізація загальних норм, які регулюють відносини щодо реалізації права на інформацію різних суб`єктів і держави, порядок захисту інформації як об`єкта відносин неможливо здійснювати без чітких меж, що визначають сферу інформації як об`єкта права та потребують врахування загроз її існуванню.

Вищезазначений Закон [1] за режимом доступу поділив інформацію на відкриту та інформацію з обмеженим доступом, уповноваживши відповідні державні органи здійснювати контроль за режимом доступу до інформації. На сьогоднішній день питання захисту вітчизняних інформаційних ресурсів набувають все більшого значення. Це пов`язано з тим, що зростаюча залежність промислово розвинутих країн від джерел інформації – технічної, економічної, політичної та військової, а також рівень розвитку та ефективності використання засобів передачі та обробки цієї інформації призвів до виникнення принципово нового поняття – національні інформаційні ресурси – та до оцінки стрімкого росту їх стратегічного значення.

На початку 80-х років XX століття професор Гарвардського університету А. Еттінгер зазначав: "наступає час, коли інформація стає таким же основним ресурсом, як матеріали та енергія, отже, відносно цього ресурсу повинні бути сформульовані ті ж критичні запитання: хто ними володіє, хто в цьому зацікавлений, наскільки він доступний, можливість його ефективного використання" [2]. В реальному часі інформація об`єднала світ в єдину інформаційну систему і зараз обумовлює технічні, суспільні, політичні, соціальні та економічні системи.

Зростання інформаційних потреб держав світу вимагає використання ними ефективних систем збору