УДК 658.15

О. І. Відоменко,
к.е.н., доцент, доцент кафедри економіки і права,
Національний університет харчових технологій, м. Київ

ВИКОРИСТАННЯ ТЕХНІЧНИХ ЗАСОБІВ ЯК СКЛАДОВА СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

O. I. Vidomenko,
PhD in Economics, Associate Professor of Economics and Law,
National University of Food Technology, Kyiv

THE USE OF TECHNICAL MEANS AS A COMPONENT OF THE SYSTEM OF ECONOMIC SECURITY OF ENTERPRISES

Анотація.
Стаття присвячена дослідженню особливостей використання технічних засобів у системі економічної безпеки підприємства. У результаті проведених досліджень розкрито такі поняття як «складові системи економічної безпеки», «канали витоку інформації», «види розвідки», «технічні засоби в системі економічної безпеки».
У процесі дослідження розглянуто джерела та причини витоку інформації і комерційних таємниць. Акцентовано увагу на сучасних (відносно нових) джерелах витоку - інформації в мережі Інтернет. Класифіковано канали витоку інформації за фізичними властивостями. Виявлено особливості використання технічних засобів з метою збору інформації та захисту проти таких дій. Описано призначення технічних систем розвідки. Вказано на переваги використання технічних засобів захисту інформації перед людським ресурсом. Визначено основні види інформації на підприємстві, яка може становити комерційну таємницю. Сформовано цілі інформаційного захисту технічними засобами. Виділено етапи та засоби пошуку пристроїв зняття інформації. Класифіковано засоби захисту бізнесу та виділено цілі використання технічних засобів захисту інформації.

Summary.
The article is devoted to the exploration of the usage of technical means in the system of economic security of the enterprise. As a result of the carried out research reveals such concepts as "the components of the system of economic security", "channels of information leakage", "types of intelligence", "technical means in the system of economic security.
In the course of the study examined the sources and causes of the leakage of information and commercial secrets. Attention on modern (relatively new) sources of leaks of information in the Internet. Classified channels of information leakage by physical properties. Revealed features of the use of technical means in order to

gather information and protect against such action. Describes the purpose of technical systems. On the advantages of using technical means of protection of information before human resource. Identified the main types of information in the enterprise, which may be a commercial secret. Formed the goals of information protection technical means. Selected stages and search tools.

Ключові слова: *економічна безпека, технічні засоби захисту економічної безпеки, захист інформації, технічні засоби економічної розвідки, технічні засоби захисту бізнесу, канали витоку інформації, конкурентна розвідка.*

Keywords: *economic security, technical means of protection of economic safety, information security, technical means of economic intelligence, technical protection means business, channels of information leakage, competitive intelligence.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. У сучасному інформаційному суспільстві загрози економічній безпеці підприємства настільки великі, що їх мінімізація чи нейтралізація переходять з розряду актуальних питань об’єкту господарювання на мезо- і, навіть, макрорівень. Все частіше зловмисники для ведення економічної розвідки застосовують різноманітні технічні засоби і технології. Для протидії яким, необхідно бути обізнаним в їх типах і особливостях, та використовувати для охорони відповідні технічні засоби захисту, що підвищать ефективність економічної безпеки підприємства.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми. Вивченню проблем захисту інформації присвячені праці Аверченко В.І., Додонова А.Г., Ландє Д.В., Прищепи В.В., Путятина В.Г., Торокіна О.О. Останніми десятиліттями все більше робіт спрямовано на аналіз захисту саме економічної інформації підприємства в системі забезпечення його безпеки, серед них можна виділити праці Іванюти Т.М., Богуш В.М., Бондарчука Ю.В., Марущак А.І., Юдіна О.К. Заслуговує на увагу і те, що ряд робіт вітчизняних вчених присвячений захисту інформації в комп’ютерних мережах. Однак вивчення наукових публікацій виявило відсутність системності в дослідженні даних питань.

Формулювання цілей статті (постановка завдання). Метою даного

дослідження є вивчення особливостей та систематизація використання технічних засобів у системі економічної безпеки підприємства.

Виклад основного матеріалу дослідження. Будь-яка бізнес-діяльність нерозривно пов'язана з обміном і опрацюванням різнобічної інформації. На сучасному етапі розвитку суспільства, інформація розглядається як особливий вид товару, і стає навіть ціннішою за будь-які матеріальні товари. Від неї безпосередньо залежить досягнення підприємницьких цілей організації. Її розголошення може не лише поставити під удар роботу підприємства і його безпеку, але й навіть привести до повного банкрутства. Тому, особливо важлива й цінна інформація підприємства, повинна бути надійно захищена. І це незалежно від того, буде проводитися по відношенню до такого підприємства конкурентна розвідка[1] чи промисловий шпіонаж.

Поняття «безпека підприємства» характеризує умови, що забезпечують стійку й прибуткову діяльність, з реалізацією всіх запланованих організацією комерційних програм і гарантують захист від внутрішніх та зовнішніх деструктивних факторів. Незаперечним є факт, що система економічної безпеки підприємства включає наступні складові: 1) інтелектуальну і кадрову; 2) інформаційну; 3) техніко-технологічну; 4) фінансову; 5) політико-правову та екологічну; 6) силову [1]. «Витік інформації» може підірвати стійкість однієї з цих складових, а відповідно, принципу «доміно», призвести до втрати фінансово-економічної стійкості бізнесу.

Весь інформаційний простір можна підрозділити на такі типи інформації, як «відкриту» (для вільного й офіційного доступу), «закриту» (тобто складає комерційну чи державну таємницю) та «слухову» (що передається неофіційно в усній формі). Тому, з метою розвідування, існують різні схеми доступу до інформації: «агентурна розвідка» (конфіденційна), «технічна розвідка» (таємнича), «аналітична розвідка» (цілком легальна) (рис. 1).

[1] Конкурентна (ділова) розвідка на відміну від промислового шпіонажу, розглядається як добросовісна конкуренція та вважається легальною діяльністю

Рис. 1. Схема доступу до розвідувальної інформації при здійсненні конкурентної розвідки (подано за А.А. Торокіним [2])

Перебіг одержання розвідувальної інформації може істотно відрізнятися від моделі, що початково запланована. Це залежить від якості проведення трьох етапів, таких як: 1) прогнозування та підготовча робота; 2) моделювання; 3) впровадження вибраної моделі. Саме на виконавцях лежить відповідальність за якісну підготовку та успіх розвідки. У разі помилки, вони будуть змушені виправляти недоліки попередніх етапів.

Доволі часто причинами, за якими конфіденційною інформацією можуть оволодіти треті особи, є елементарне недотримання керівниками та персоналом певних правил безпеки.

Можна виділити такі причини витоку комерційних таємниць:

- незнання та недотримання персоналом організації необхідних норм захисту конфіденційної інформації, або нерозуміння їх важливості;
- недостатній контроль у дотриманні норм захисту інформації інженерно-технічними, організаційними та правовими методами;
- застосування для обробки конфіденційної інформації технічних приладів, що не пройшли атестацію;

- організаційні помилки, завдяки яким виток інформації відбувається через працівників ІТ та ІС відділів;
- плинність кадрів, особливо тих, що мали доступ до комерційних секретів.

Основна частина перелічених вище технічних проблем несанкціонованого доступу, підлягає блокуванню у разі вірної розробки та реалізації системи забезпечення безпеки. Однак, виникають великі труднощі у боротьбі з різноманітними інформаційними вірусами. Справа у великій кількості таких шкідливих програм. Їх постійно вдосконалюють, розробляють нові версії, що не дозволяє винайти надійні та сталі засоби протидії їм. Основним завданням таких програм є шпигунство за інформацією, розміщеною на комп'ютерах, а також псування програмного забезпечення та баз даних, що являє собою пряму диверсію проти фірми.

Тож захисту комп'ютерної інформації потрібно приділяти особливу увагу. За винятком загальних організаційно-режимних заходів, необхідно періодично проводити інструментальні перевірки об'єктів та приміщень кваліфікованими фахівцями. Це допомагає своєчасно виявляти встановлену шпигунську апаратуру. Крім того, проводячи переговори, доцільно використовувати додаткові засоби технічного захисту від ймовірного шпигунства конкурентів

Особливої уваги заслуговує і такий потужний пласт для конкурентної розвідки, шпигунства і, навіть, підриву безпеки країни, як управління інформацією в мережі Інтернет [3]. Саме за-для припинення таких дій, враховуючи зовнішню агресію по відношенню до України, Указом Президента України від 15 травня 2017 року [4], було введено у дію рішення РНБО щодо блокування (терміном на три роки) активів російських сайтів "ВКонтакте", "Одноклассники", "Мейл.ру" та "Яндекс" та заборони інтернет-провайдерам надавати доступ до вказаних ресурсів.

Як наголошують фахівці, Інтернет – це не лише ресурс для збору інформації, але й з його допомогою нині можна «формувати» суспільну думку, смаки, переконання, ідеологію і т.д. [3, с.108-116].

Не говорячи вже про програмні засоби, які «працюють» на комп'ютерах підприємства (зі згоди керівників цього підприємства), а паралельно можуть збирати інформацію про дане підприємство. Це, наприклад, можуть бути антивірусні програми чи, скажімо, бухгалтерські програми. Тож зрозумілим стає крок щодо вимоги вищезгаданого Указу [4] з блокування сайтів російських антивірусних компаній "Лабораторія Касперського" і DrWeb та бухгалтерської програми «1С».

Значно старший спосіб ведення розвідки: за допомогою технічних засобів.

У середині минулого століття А. Даллес відмітив наступні види використання технічних засобів щодо розвідки [5]: 1) прослуховування переговорів; 2) радіолокація; 3) фотографування; 4) хімічний аналіз середовища біля об'єкта спостереження (ґрунту, води повітря).

Нині до переліку вищеназваних засобів додалися: біологічний аналіз, комп'ютерна розвідка, телевізійні спостереження. Тепер ця інформація одержується і обробляється набагато простіше прямо з об'єкта стеження, завдяки технічним засобам. Єдиною складністю тепер може бути лише процес розшифрування зібраної інформації за рахунок технічних засобів.

Для ведення розвідки широко застосовуються різноманітні технічні системи, машини, апарати, інструменти та обладнання. Призначення їх використання доволі широке:

- одержання розвідувальної інформації з інформаційних систем, каналів електрозв'язку, засобів обробки інформації;
- приховане спостереження за джерелами інформації розвідувальними органами;
- злом криптографічного та технічного захисту інформації;
- організація постачання розвідувальної інформації;
- передавання розвідувальної інформації;

- отримання розвідувальної інформації за рахунок сканування космічного та повітряного простору, випромінювань різноманітного характеру, поверхні Землі та окремих її об’єктів.

Під час функціонування, технічні засоби генерують у навколишній світ сторонні випромінювання різноманітної природи (механічні, теплові, електричні, електромагнітні тощо) [2]. Так чи інакше, це пов’язано з обробкою інформації.

Так звані «канали витоку інформації» виникають, при ведені зловмисником розвідки із застосуванням відповідних технічних засобів для одержання конфіденційної інформації, за умови невступання ним у прямий контакт із її джерелом інформації. При формуванні системи безпеки необхідно враховувати особливості тих чи інших каналів витоку інформації. Дотримання цього необхідне для правильної побудови ефективної системи захисту. Не кожне випромінювання приладу говорить про витік інформації, для прикладу – робоче світіння монітору. Тут треба враховувати технічні можливості супротивника, напруженість певного енергетичного поля за межами охоронної зони. Для правильного визначення потрібен висококваліфікований фахівець оснащений відповідними технічними засобами.

Крім цього, противник може ефективно використовувати якості дійсних каналів витоку інформації і отримувати її шпигунськими методами. Це обов’язково треба брати до уваги. Як зазначає О. Крижанівський, знімання інформації з акустичних каналів може бути здійснено через скло 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 сигналізації чи сигналу тривоги, 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 неефективною [6].

Для виникнення технічних каналів витоку інформації, необхідна наявність певних можливостей та знарядь технічного характеру. Не завжди вдається виявити та знешкодити такі небезпечні засоби. Це пов’язано з тим, що розвідувальним засобом може слугувати звичайний прилад повсякденного користування, як наприклад, робочий комп’ютер, мобільний телефон чи навіть електромережа в офісі. Аналіз різноманітних випромінювачів чи перетворювачів свідчить, що:

- генерувати небезпечний сигнал здатна будь-яка електронна та радіоапаратура, а також окремі елементи чи вузли техніки;
- з кожного генерованого небезпечного сигналу, можна за певних обставин, сформувати канал витоку інформації;
- будь-яка електронна система, що складається з комплексу вузлів та елементів, налічує сукупність джерел небезпечного сигналу, які за певних умов можуть перетворитися на канали для витоку інформації.

Бурхливий розвиток сучасних технологій і техніки сприяє постійному розширенню спектру ймовірних каналів витоку інформації, через це дослідження каналів витоку стає все більше актуальним, і складним завданням.

Канали витоку інформації поділяють на: матеріально-речові, акустичні, акустико-перетворювальні, електричні, електромагнітні, візуальні [7]. Наведемо приклади їх утворення, застосування:

1. Матеріально-речові - паперові документи, магнітні носії, фотоматеріали, різноманітні відходи тощо.
2. Акустичні - виникають внаслідок утворення звукових хвиль в будь-якому звукопровідному середовищі – акустичному полі. Такі канали зароджуються в приміщеннях організації, вентиляційних шахтах, дверях, стінних перегородках, будівельних конструкціях, через вібрацію скла у вікнах тощо.
3. Акустико-перетворювальні - формуються внаслідок мікрофонного ефекту – механічному впливу звукових хвиль на радіоелектронну апаратуру.

Вони з’являються в динаміках радіотрансляцій та електродинаміках, деталях телефонних мереж тощо.

4. Електричні – формуються за рахунок змін величини та характеру струму і напруги в електро-комунікаціях та інших електропровідних елементах.
5. Електромагнітні (радіоканальні, як їх різновид) - утворюються внаслідок впливу електромагнітних хвиль, через які стає можливим витік інформації. Такі канали виникають при роботі мобільних та радіотелефонів, ліній радіозв’язку, відео та аудіо апаратури, різноманітної обчислювальної техніки тощо.
6. Візуальні (візуально-оптичні) - з’являються завдяки спостереженню за об’єктом (можливо, з використанням фото і відеотехніки). Виникають внаслідок випромінювання електромагнітних хвиль у видимому, інфрачервоному, рентгенівському та ультрафіолетовому діапазоні спектру.

Використання для забезпечення як охорони, так і розвідки, технічних засобів значно здешевлює ці послуги, внаслідок падіння цін на електронні пристрої. Тоді як послуги фахівців та розвідників у цій сфері продовжують рости в ціні. Одним з чинників цього, є правова відповідальність за здійснення економічного шпигунства [8]. Крім цього, варто зазначити, що:

- коефіцієнт керованості технічних засобів наближається до одиниці, на відміну від керованості фахівцем-людиною, яка може мати свої мотиви до певної дії;
- технічним засобам не потрібно виплачувати соціальне страхування і зарплату, на противагу фахівцям;
- завдяки технічним засобам стає можливим отримання потокової інформації і зберігання її надалі, що є цінним для розвідки та охорони;

До того ж виявлений "жучок" чи "електронне вухо", на відміну від людини, не викриє таємницю щодо свого власника.

Будь-який економічний об’єкт являє собою цілу систему. В своїй діяльності вона використовує ресурси, які переробляє або використовує для

виробництва продукції чи надання послуг. Також вона має виробничі відходи, викиди чи відпрацьовані матеріали. До того ж, вона має комунікативні зв'язки із зовнішнім середовищем. І все це може бути піддано економічному аналізу зловмисником в своїх цілях.

Використання технічних засобів є важливим елементом для розробки ефективної системи захисту підприємства. За призначенням їх поділяють на засоби: 1) для отримання інформації; 2) для захисту інформації чи обмеження до неї доступу.

Так, технічні засоби, що використовуються в економічній розвідці, призначені для отримання інформації щодо:

– обсягу та складу ресурсів підприємства (потрібно для оцінки його потенційної здатності). Так, наприклад, знаючи особливості технологічного процесу та обсяги споживання електроенергії (води) в енергомісткому (водомісткому) виробництві, можна достеменно визначити обсяги виробництва і т.п.;

– випуску продукції та відходів, які виникають у процесі перероблення ресурсів;

– ефективності процесу виробництва, технологічного та виробничого стану економічної системи;

– наявних зв'язків підприємства з об'єктами зовнішнього середовища.

Необхідність розвитку технічного захисту інформації спричинене зростанням рівня загроз щодо інформації. Це визвано рядом факторів, серед яких:

- кризовий стан економіки;
- лібералізація відносин (суспільних і міждержавних);
- застосування іноземних засобів оброблення інформації та зв'язку;
- популяризація приладів несанкціонованого доступу до інформації та її обробки тощо.

Взагалі, технічний захист інформації розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу (НСД) і захисту інформації від витоку технічними каналами [9].

Виділяють наступні технічні засоби інформаційного захисту:

- від небезпеки витоку інформації, блокування та порушення її цілісності;
- для пошуку прихованих пристроїв, що становлять загрозу;
- для контролю дієвості технічного захисту;
- спеціального призначення;
- додаткового призначення (прилади, які крім своїх основних функцій, виконують ще й захисні).

Засоби, що використовуються для захисту інформації повинні бути надійними. В Україні передбачено спеціальну процедуру сертифікації засобів технічного захисту інформації, її виконання доручено Інституту проблем математичних машин і систем НАН України УКРСЕРТКОМП'ЮТЕР [10].

Іванютою Т.М. виділено сім етапів процесу пошуку пристроїв зняття інформації [11, с.162]: (1) вивчення оперативної ситуації поблизу об'єкту; (2),(3) перевірка радіоефіру за межами приміщення та в межах нього; (4) візуальне обстеження всіх меблів й інших предметів; (5) перевірка стану приміщення радіолокатором; (6) контроль електротехніки; (7) перевірка (телефонної, електричної) ліній (рис. 2).

Для захисту інформації застосовується спеціальне устаткування. Далі розглянемо деякі з видів систем захисту [11, с.162-163]:

1. Телефонні лінії можна захистити використанням:
   - скремблерів;
   - аналізаторів телефонних ліній;
   - випалювачів засобів зйому;
   - приладів активного слухання;
   - фільтрів;
   - універсальних приладів.

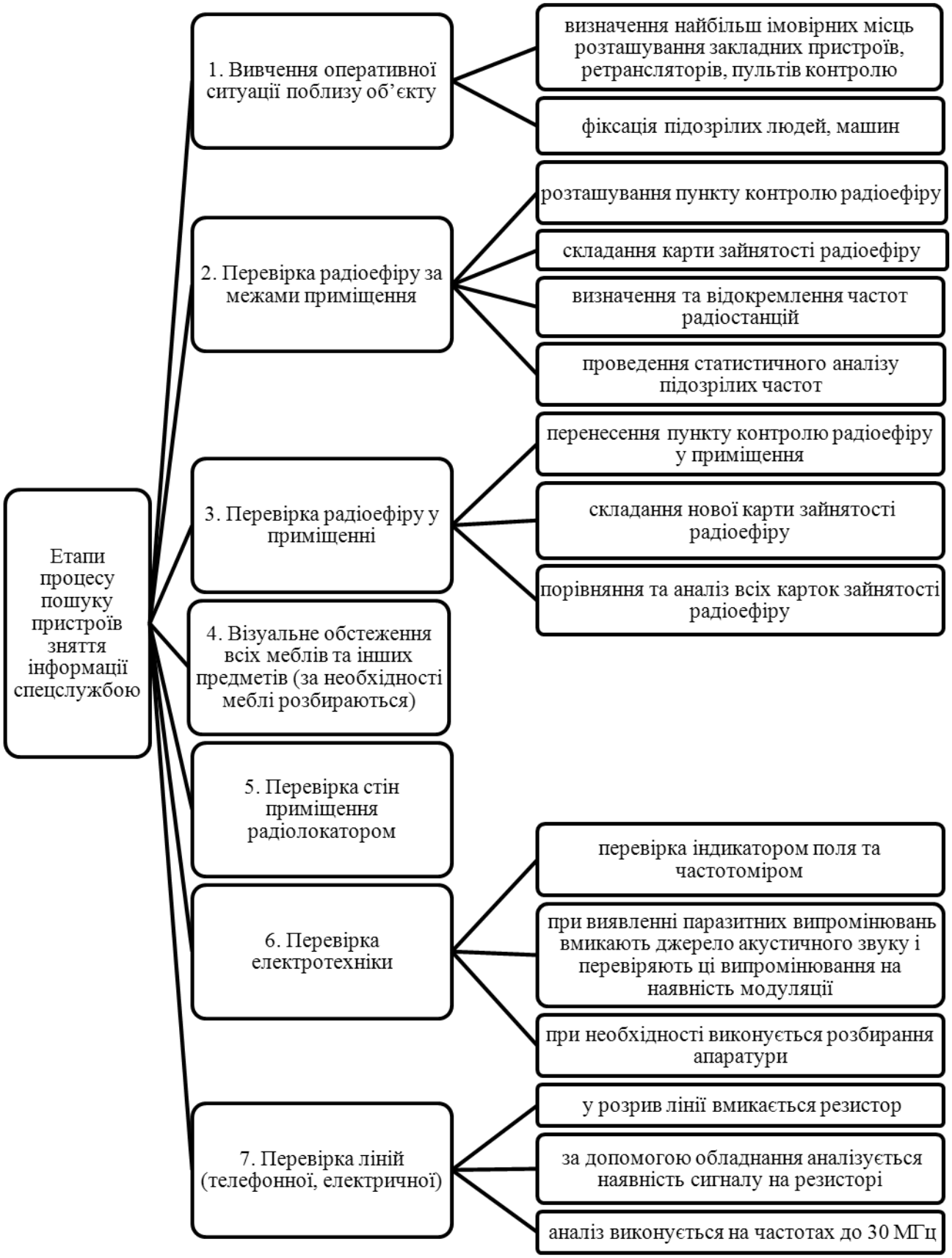

Рис. 2. Етапи процесу пошуку пристроїв зняття інформації

2. Захиститися від радіозакладок можна застосуванням джерел радіошумів.

3. Від диктофонного шпіонажу захищаються застосуванням:

- диктофонних детекторів;
- обладнання дистанційного стирання запису (для касетних).

4. Від перехвату сигналів інформації лазерними пристроями з віконного скла, застосовують вібратори.

5. Захист ліній електромереж від шпигунства відбувається за рахунок:

- джерел шуму певного діапазону частот;
- діелектричних муфт, що встановлюються в мережі тепло- та водопостачання;
- спеціальних фільтрів;
- контролю оперативної ситуації на прилеглої до підприємства території (охорона, розміщення камер);
- демонтажу всіх електричних кабелів, які свідомо не використовуються.

Технічні засоби охорони призначені для:

- ідентифікації персоналу та інших осіб, що відвідують організацію чи її певні об’єкти;
- встановлення пропускного режиму чи лімітування доступу до окремих об’єктів організації та на її територію;
- визначення та протоколювання правопорушень спрямованих проти організації;
- викриття технічних засобів конкурентів, які ведуть розвідку;
- подачі сигналу тривоги (у разі небезпеки).

Інформаційні загрози безпеці підприємства стимулюють до пошуку схем його захисту, що в результаті збільшує попит на нові технології та технічні засоби. Звичайно, на противагу засобам ведення розвідки, розробляються і засоби, які б перешкоджали їй, та могли боронити підприємницьку діяльність. Засоби які використовують для захисту бізнесу заведено поділяти на: фізичні, апаратні, програмні, криптографічні [12] (рис. 3).

Фізичні засоби

- різноманітні пристрої, конструкції, апарати, вироби, призначенні для створення перепон на шляху руху зловмисників;
- охоронні та охоронно-пожежні системи;
- охоронне телебачення;
- охоронне освітлення;
- засоби фізичного захисту.

Апаратні засоби

- різноманітні технічні конструкції, які забезпечують припинення розголошення, захист від витоку та протидію несанкціонованому доступу до джерел конфіденційної інформації;
- апаратура для проведення спеціальних досліджень технічних засобів забезпечення виробничої діяльності на наявність можливого витоку інформації;
- засоби виявлення каналів витоку інформації на об'єктах та у приміщеннях;
- засоби локалізації каналів витоку;
- апаратура для пошуку та виявлення засобів промислового шпіонажу;
- засоби протидії несанкціонованого доступу до джерел конфіденційної інформації.

Програмні засоби

- система спеціальних програм, які входять до складу програмного забезпечення;
- програми для захисту інформації від несанкціонованого доступу;
- програми для захисту інформації від копіювання;
- програмні засоби для захисту програм від вірусів;
- програмні засоби для захисту інформації від вірусів;
- засоби програмного захисту каналів зв'язку.

Криптографічні засоби

- апаратні, програмні та програмно-апаратні засоби, що реалізують захист інформації за допомогою криптографічних перетворень.

Рис. 3. Технічні засоби захисту бізнесу

(подано за Юдін О.К., Богуш В.М. [12, с.276])

Крім засобів вузькопрофільного (спеціального) застосування для захисту бізнесу, існують відповідні із комплексною дією. Вони можуть виконувати декілька захисних функцій перелічених на рисунку вище. Такі засоби можна

характеризувати, як універсальні або багатопрофільні.

В еру науково-технічного прогресу використання технічних засобів стало невід'ємною складовою системи економічної безпеки. Без їх застосовування, просто неможливо створити надійну систему охорони підприємницької діяльності.

Висновок з даного дослідження і перспективи подальших розвідок у даному напрямі. Технічні засоби використовуються для того, щоб попередити проникнення чужинця на територію, в інформаційну мережу, а також не дозволити доступ до документації об'єкта. Дія технічних засобів повинна спрямовуватись на працівників інших підприємств, злочинців та окремих осіб. Комп'ютерні мережі підприємств є вразливим елементом, тому потребують особливого захисту технічними засобами. Іншими сферами, які повинні бути під технічним наглядом, є внутрішні приміщення об'єкта, лабораторії та цехи, а також приміщення для експериментів та інноваційної діяльності, кімнати переговорів тощо.

Список літератури.

1. Бондарчук, Ю. В. Безпека бізнесу: організаційно-правові основи / Ю. В. Бондарчук, А. І. Марущак. - К.: Видавничий дім «Скіф», КНТ, 2008. - 372с.
2. Торокин, А. А. Основы инженерно-технической защиты информации. - М.: «Ось-89», 1998. - 336 с.;
3. Додонов, А. Г. Конкурентная разведка в компьютерных сетях / [Додонов А. Г., Ландэ Д. В., Прищепа В. В., Путятин В. Г.] - К.: ИПРИ НАН Украины , 2013. – 250 с.
4. Указ Президента України №133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)"» // Офіційний сайт Президента України [Електронний ресурс] - Режим доступу : http://www.president.gov.ua/documents/all?s-num=133%2F2017&contain-rule=contains&s-text=&date-from=25-06-2016&date-to=25-06-2017&order=desc& (дата звернення 15.06.2017 р.). – Назва з екрану.
5. Даллес, А. Искусство разведки : пер. с англ. с сокращен. / А. Даллес. – М.: Международные отношения, 1992. – 288с.
6. Крижанівський, О. Положення про конфіденційну інформацію (комерційну таємницю) – базовий документ економічної безпеки фірми // О. Крижанівський // Інтелектуальна власність. – 2006. – № 3. – С. 33-35.

7. Технічний захист інформації // Телекомунікаційні системи та мережі. Структура й основні функції. - Том 1 : [Електронний ресурс]. / [В. В. Поповський, О. В. Лемешко, В. К. Ковальчук та ін.] - Режим доступу : http://www.znanius.com/3853.html?&L= (дата звернення 20.06.2017 р.). – Назва з екрану.

8. Аверченко, В. И. Разработка системы технической защиты информации / [Аверченко В. И., Рытов М. Ю., Кувыклин А. В., Гайнулин Т. Р.] - Брянск.: БГТУ, 2008. - 187 с.

9. Надання послуг в області технічного захисту інформації // Сайт компанії «УЛІС Сістемс» [Електронний ресурс] – Режим доступу : http://www.ulyssys.com/i/lng.ua/page.security (дата звернення 19.06.2017 р.). – Назва з екрану.

10. Сайт Державної служби спеціального зв’язку та захисту інформації України [Електронний ресурс]. – Режим доступу : http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=2B2C88197E5366F05CE8E2CD3C62ED3E.app2?art_id=252756&cat_id=39181 (дата звернення 26.06.2017 р.). – Назва з екрану.

11. Іванюта, Т. М. Економічна безпека підприємства / Т. М. Іванюта, А. О. Заїнчковський. – Київ : ЦУЛ, 2009. – 254с.

12. Юдін, О.К. Інформаційна безпека держави / О. К. Юдін, В. М. Богуш. — Харків: Консум, 2004. — 508 с.

References.

1. Bondarchuk, Yu. V., Maruschak, A. I. (2008), *Bezpeka biznesu: orhanizatsijno-pravovi osnovy* [Business security: organizational and legal basisъ] - Vydavnychyj dim «Skif», KNT, Kyiv, Ukraine.

2. Torokin, A.A. (1998), *Osnovy inzhenerno-tehnicheskoj zashhity informacii* [Fundamentals of engineering technical protection of information] – «Os'-89», Moscow, Russia.

3. Dodonov, A.G., Landje, D.V., Prishhepa, V.V., Putjatin, V.G. (2013), *Konkurentnaja razvedka v komp'juternyh setjah* [Competitive intelligence in computer networks] - IPRI NAN Ukraine, Kyiv, Ukraine.

4. Official website President of Ukraine (2017), “Decree of the President of Ukraine No 133 "On the decision of the National Security and Defense Council of Ukraine dated April 28, 2017" On the application of personal special economic and other restrictive measures (sanctions)"”, available at: http://www.president.gov.ua/documents/all?s-num=133%2F2017&contain-rule=contains&s-text=&date-from=25-06-2016&date-to=25-06-2017&order=desc& (Accessed 25 June 2017)

5. Dalles, A. (1992), *Iskusstvo razvedki* [Art of Intelligence] - Mezhdunarodnye otnoshenija, Moscow, Russia.

6. Kryzhanivs'kyj, O. (2006), “Provisions on the confidential information (trade secret) is the basic document of economic security firm”, *Intelektual'na vlasnist'*, vol. 3, pp. 33-35.

7. Electronic Learning Tools (2017), *Tekhnichnyj zakhyst informatsii* [Technical protection of information], *Telekomunikatsijni systemy ta merezhi. Struktura j osnovni funktsii* [Telecommunication systems and networks. Structure and basic functions], vol. 1, available at: http://www.znanius.com/3853.html?&L= (Accessed 20 June 2017).

8. Averchenko, V.I., Rytov, M.Ju., Kuvyklin, A.V., Gajnulin, T.V. (2008), *Razrabotka sistemy tehnicheskoj zashhity informacii* [Development of system of technical protection of the information] - BHTU, Briansk, Russia.

9. The official site of company "ULIS Systems" (2017), "Providing services in the field of technical protection of information", available at: http://www.ulyssys.com/i/lng.ua/page.security (Accessed 19 June 2017).

10. The State Service of Special Communications and Information Protection of Ukraine (2017), available at: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=2B2C88197E5366F05CE8E2CD3C62ED3E.app2?art_id=252756&cat_id=39181 (Accessed 26 June 2017).

11. Ivaniuta, T.M., Zainchkovs'kyj, A.O. (2009), *Ekonomichna bezpeka pidpryiemstva* [Economic security of the enterprise] – Tsentr uchbovoi literatury, Kyiv, Ukraine.

12. Yudin, O.K., Bohush, V.M. (2004), *Informatsijna bezpeka derzhavy* [Information security of the state] - Konsum, Kharkiv, Ukraine.