Київський національний торговельно-економічний університет

Кафедра загальноправових дисциплін

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ПРОТИДІЯ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ НА ПІДПРИЄМСТВІ»

студента 2 курсу, 7 м групи
спеціальності 081, «Право»
спеціалізації «Правове забезпечення
безпеки підприємницької діяльності» Магаляс Ганни
_____ Андріївні

Науковий керівник
кандидат юридичних наук, Давиденко Валерій
доцент _____ Степанович

Гарант освітньої програми
кандидат юридичних наук, Крегул Юрій
професор _____ Іванович

Київ 2018

ЗМІСТ

ВСТУП

В сучасних умовах розвитку ринкових відносин забезпечити існування суб'єкта господарювання на основі високотехнологічного виробництва, ефективних методів організації праці можливо тільки шляхом одержання і використання необхідного обсягу і якості інформації, яка виступає особливим товаром.

Цінність інформації як товару (ресурсу) визначається її достовірністю, цілісністю, доступністю. Конфіденційність робить інформацію тільки привабливою, що визначається, по-перше, колом осіб, які мають право володіти нею, а , по-друге, встановленням особливого режиму доступу.

Інформаційний простір стає ареною зіткнень різних інтересів держав за умов міжнародної конкуренції та глобальної інтеграції. Дієва система захисту держави та господарюючих суб'єктів дає можливість ефективно використовувати інформацію, що впливатиме на зростання значення управлінських методів з використанням інформаційних технологій.

Науковим підґрунтям дослідження питання інформаційної безпеки підприємств стали праці Андрєєва В.І., Ахрамовича В.М., Бандурки О.М., Баранова О.А., Гуцалюка М.О., Живко З.Б., Калюжного Р.А., Климника І.І., Кормича Б.А., Крегула Ю.І., Кулініча О.О., Ліпкана В.А., Максименко Ю.С., Нашинець-Наумової А.Ю., Петрика В.М., Северина Л.І., Степко О.М., Ткачука Т.Ю., Цимбалюк В.С., Чередниченка В.С., Шелеста М.Є.

Констатуючи значний науковий внесок учених у розроблення зазначеної проблематики, зауважимо, що їх дослідження стосувалися лише в певних аспектів інформаційної безпеки підприємства.

Додатковому вивченню і висвітленню підлягає, зокрема, проблема протидії загрозам інформаційній безпеці на підприємстві, яка ще не виступала як окреме наукове дослідження. Це обумовлює **актуальність обраної тематики.**

Мета і зміст поставлених задач. Метою роботи є комплексний науково-теоретичний аналіз юридичної природи протидії загрозам інформаційної

безпеки на підприємстві та отримання об'єктивних даних, необхідних для формулювання наукових висновків та обґрунтування пропозицій щодо вдосконалення українського законодавства в сфері протидії загрозам інформаційній безпеці на підприємстві.

Для досягнення зазначеної мети необхідно було вирішити такі задачі:

- схарактеризувати суть і поняття інформації, системи захисту інформації, інформаційної безпеки;
- виокремити різні види інформації;
- визначити роль та значення правового регулювання інформаційної безпеки;
- розкрити організаційні засади захисту інформації на підприємстві;
- дослідити функції підрозділу захисту інформації;
- виокремити специфіку технічного захисту інформації;
- розкрити механізми стратегічного інформаційного протиборства;
- дослідити міжнародні аспекти інформаційної безпеки в умовах глобалізації;
- охарактеризувати захист інформації підприємства від промислового шпигунства.

Об'єкт дослідження становлять суспільні відносини, врегульовані правовими нормами, в яких закріплені основи інформаційної безпеки на підприємстві та зазначені організаційні і функціональні засади протидії її загрозам.

Предметом дослідження є протидія загрозам інформаційній безпеці на підприємстві.

Методи дослідження. Методологічну основу дослідження склали загальнонаукові методи пізнання правових явищ, як то: діалектичний, історичний, порівняльно-історичний, структурно-функціональний, формально-логічний, метод системного аналізу і синтезу, а також властиві теорії права соціально-наукові методи, а саме: порівняльно-правовий та метод тлумачення правових норм. Комплексне застосування різних методів наукового пізнання

спрямоване на забезпечення обґрунтованості висновків та аргументованості пропозицій, зроблених в результаті виконання роботи.

Застосування діалектичного методу пізнання ґрунтується на взаємозалежності та взаємообумовленості систем правового регулювання у сфері інформаційної безпеки підприємства та відповідних суспільних відносин, що пов'язані із забезпеченням протидії її загрозам.

Історичний та порівняльно-правовий методи покладені в основу висвітлення історії виникнення такого явища як інформація. Структурно-функціональний метод застосовувався при визначенні методів здійснення механізмів захисту інформаційної безпеки на підприємстві. За допомогою формально-логічного методу в роботі сформульовані визначення інформації, інформаційної безпеки, захисту інформації; визначені види інформації, а також виконувалось з'ясування змісту правових норм, що регулюють суспільні відносини, які складаються з приводу захисту інформації підприємства від промислового шпигунства. Методи системного аналізу та синтезу були використані при розкритті класифікації видів інформації, характеристиці організації захисту інформації на підприємстві та розкритті функцій підрозділу захисту інформації. За допомогою порівняльно-правового методу були співставленні та проаналізовані теоретичні положення юридичної науки України щодо суспільних відносин, які складаються з приводу протидії загрозам інформаційній безпеці на підприємстві.

Наукова новизна. Виконувана кваліфікаційна робота є першим в Україні комплексним дослідженням протидії загрозам інформаційній безпеці на підприємстві. У результаті проведеної роботи сформульовано та обґрунтовано низку положень і висновків концептуального характеру.

Практичне значення полягає в тому, що сформульовані та аргументовані в роботі теоретичні положення, висновки та пропозиції можуть бути впроваджені як в практичній діяльності суб'єктів господарювання з метою протидіяти загрозі їх інформаційній безпеці, а також у навчальному процесі та вдосконаленні національного законодавства.

Структура та обсяг роботи. Робота складається із трьох розділів, кожен з яких має три підрозділи, що викладені на_____ сторінках. Автор використала _____ джерело.

РОЗДІЛ 1. ЗАГАЛЬНОТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ПРАВОВОГО РОЗУМІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Суть і поняття інформації, системи захисту інформації, інформаційної безпеки

Термін «інформація» походить з латинського «informatio», цей термін має декілька значень:

- виклад, роз'яснення, витлумачення;
- представлення, поняття;
- просвіта, ознайомлення.

Слово «information» вперше з'явилося на світ в англійській мові в 1387 р. У східнослов'янські мови дане слово поширилось через Польщу у XVII ст.

Інформація стала загальнонауковим поняттям із середини XX ст. Загальноприйнятого визначення інформації не існує, і воно використовується переважно на інтуїтивному рівні [18, с.28]

На нашу думку, *інформація з погляду безпеки* – це відомості, дані про суб'єкти, об'єкти, явища та процеси. Також це документи, які захищені через їх важливість для суб'єкта діяльності від незаконного розголошування, розкриття чи втручання.

Термін «інформація» залежно від галузі використання має доволі багато визначень. Наприклад:

- будь-який вид інформації у матеріальній або нематеріальній формі [67, с.32];
- роз'яснення, виклад [55, с.63];
- передача різноманітності [4, с.38];
- відомості у будь-яких формах і вигляді, збережені на різних носіях [51, с.47];
- позначення змісту, отриманого з зовнішнього світу в процесі нашого пристосування до нього [49, с.44];

- відомості про явища, предмети й процеси навколишнього світу [20, с.58].

У нормативно-правових актах можна знайти більш повний опис поняття «інформація». Дане поняття «інформація» зустрічається в законодавчих та підзаконних нормативно-правових актах. Це обумовлено:

- розвитком національного законодавства, яке сформувалося, на основі термінового врегулювання багатьох сфер суспільного життя;

- інформаційні відносини та інформація як їх предмет є складовою різних видів суспільних відносин;

- інформація може бути товаром, а саме об'єктом цивільно-правових відносин, а предметом регулювання адміністративного права є обіг управлінської інформації [19; с.21].

Правовий статус інформації визначає Закон України «Про інформацію». У Законі зазначено, що *інформація* – це документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі [85].

Трактування «інформації» у Цивільному кодексі України відрізняється від Закону України «Про інформацію». В кодексі зазначено, що інформація – це документовані або публічно оголошені відомості про явища та події, що мали або мають місце в суспільстві, державі та навколишньому середовищі [103].

Захист інформації – це сукупність засобів, методів, організаційних заходів щодо запобігання можливим випадковим або навмисним впливам природного чи штучного характеру, наслідком яких може бути збитки чи шкода, завдані власникам інформації або її користувачам, інформаційному простору. Захист інформації полягає в забезпеченні її доступності при збереженні цілісності та гарантованої конфіденційності.

Система захисту державної таємниці – сукупність органів захисту державної таємниці, що діють у взаємодії та координації відповідно до наданої законодавством компетенції, використовуваних ними форм, методів і засобів

захисту відомостей, що становлять державну таємницю, їх носіїв та заходів, що впровадяться в їх інтересах [18, с.108].

Існують різні уявлення про системи захисту інформації (СЗІ) з точки зору їх призначення, складу і виконуваних функцій. Для формування повного уявлення про СЗІ нижче наведено їх основні складові, а саме:

- законодавча, нормативно-методична і наукова база;
- структура і задачі органів комплексного ЗІ;
- організаційно-технічні та режимні заходи;
- програмно-технічні методи і засоби ЗІ.

Основною складовою СЗІ є нормативно-методологічна база, яка містить у змісті документа такі групи питань:

1. Основи:
- структура і задачі органів, що забезпечують захист інформації;
- організаційно-технічні та режимні заходи і методи;
- програмно-технічні способи і засоби.

2. Напрями:
- захист об'єктів корпоративних систем;
- захист процесів, процедур і програм оброблення інформації;
- захист каналів зв'язку;
- управління системою захисту.

3. Етапи:
- визначення інформаційних і технічних ресурсів, що підлягають захисту;
- виявлення потенційно можливих загроз і каналів витоку інформації;
- проведення оцінювання уразливості та ризиків інформації при наявних загрозах і каналах витоку;
- визначення вимог до системи захисту;
- здійснення вибору засобів захисту інформації та їх характеристики;
- впровадження і організація використання обраних заходів, способів і засобів захисту [92, с.9].

Визначення «*інформаційної безпеки»,* за словами Северина Л. І., – це вид інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов їх життєдіяльності; стан правовідносин, пов'язаних з безпечним створенням, обробкою, використанням та розповсюдженням у певному просторі, часу та колі осіб; це суспільні процеси, пов'язані зі створенням нормальних умов поширення, зберігання та використання інформації [92, с.8].

Науковці В.С. Чередниченко, М.Є. Шелест, В.І. Андрєєв, В.О. Хорошко трактують інформаційну безпеку як захищеність інформації та інфраструктури, яка її підтримує від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних і відносин, у тому числі власникам і користувачам інформації [1, с.55].

Баранов О. А. дає визначення інформаційної безпеки як стану захищеності життєво важливих інтересів особистості суспільства й держави, за якого зводиться до мінімуму заподіяння збитків через неповноту, несвоєчасність і недостовірність інформації, через негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [5, с.134].

Степко О.М. розкриває інформаційну безпеку як стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [94].

Петрик В. М. тлумачить інформаційну безпеку як стан захищеності об'єктів (особистого, суспільства, держави, інформаційно-технічної інфраструктури), за якого досягається його нормальне функціонування незалежно від наявності внутрішніх і зовнішніх інформаційних впливів [68, с.160-161].

Калюжний Р.А. вважає, що інформаційна безпека - це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності; суспільних правовідносин пов'язаних із створенням, розповсюдженням, зберіганням та використанням інформації [70,с. 20].

Цимбалюк В.С. зазначає, що інформаційна безпека - це стан захищеності передбачених законодавством норм і параметрів інформаційної процесії та відносин, що забезпечує необхідні умови існування держави, людини та суспільства як суб'єктних процесів і відносин [66, с.78-79].

Аналіз багатьох джерел показує, що структурні складові забезпечення інформаційної безпеки недостатньо систематизовані.

Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. в системі забезпечення інформаційної безпеки розуміють сукупність адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення [47, с.158].

Отже, Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. пропонують розуміти в понятті «адміністративно-правове забезпечення інформаційної безпеки» комплекс превентивних дій економічного, політичного, юридичного, технологічного та організаційного характеру, спрямованих на попередження, виявлення і ліквідацію загроз інтересам особи, держави та суспільства в інформаційній сфері.

У сучасному інформаційному суспільстві система забезпечення інформаційної безпеки України створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері. Основу даної системи складають органи, сили та засоби забезпечення інформаційної безпеки, які застосовують комплекс адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських, та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління.

Правову основу у сфері національної безпеки України становлять Конституція, закони України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання законів інші нормативно-правові акти, а саме: Закони України: «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про інформацію», «Про доступ до публічної інформації».

1.2. Класифікація і характеристика видів інформації

Цивільний кодекс України наголошує, що інформація – це об'єкт прав, що належить до категорії нематеріальних благ. Інформація може вільно відчужуватися або переходити за правонаступництвом чи успадковуватися іншим способом, якщо вона не вилучена із цивільного обороту чи не обмежена в ньому або є невід'ємною частиною фізичної чи юридичної особи [103].

На сьогодні виділяють декілька категорій інформації, а саме:

1. Відкрита інформація – доступ до такої інформації може отримати будь-яка особа.

2. Корисна інформація – потрібна для діяльності, при знищені може бути легко відновлена.

3. Важлива інформація – ця інформація незамінна та необхідна для діяльності, відновлення такої інформації практично неможливе.

4. Конфіденційна інформація – сторонні особи чи персонал не допускаються до такої інформації, оскільки є ймовірність спричинити моральні чи матеріальні витрати.

Сукупність різної інформації, яка призначена для ухвалення рішень у сфері підприємництва, можна вважати інформаційним забезпеченням підприємства. Є вхідна та вихідна інформація. З боку захисту інформації найбільш важлива вихідна інформація. Вихідна інформація поділена на:

1. Інформацію про стан зовнішнього середовища.

2. Інформація про стан підприємства або наявні передумови її створення.

Для діяльності підприємства важливою інформацією є:

- фінансовий стан;

- конкурентоспроможність продукції;

- кількість і якість персоналу.

До інформації, що характеризує стан підприємства, можна віднести:

- *організаційно-правові характеристики:* правовий статус, форма власності, організаційна структура, наявність філій, торгова марка;

- *виробничі потужності:* розмір, структура, відповідність характеристиці нового товару;

- *матеріальні ресурси:* специфіка матеріальних ресурсів, розмір запасів, наявність і характеристика інформації, умови зберігання;

- *трудові ресурси:* кількість персоналу, його, склад і характеристики, джерела поповнення;

- *організаційно-технологічні можливості:* відповідність техніки, технології, організації виробництва вимогам до конкурентоспроможної продукції, наявність ліцензій і патентів;

- *економічні характеристики:* рентабельність, продуктивність праці, фінансовий стан;

- *екологічні характеристики:* рівень екологічної безпеки виробництва, можливості його сертифікації, атестації продукції;

- *інші види інформації:* кліматичні умови, наближеність до джерел ресурсів [18; с.109].

Згідно ст. 10 Закону України «Про інформацію» основними видами інформації є:

- інформація про фізичну особу;

- інформація довідково-енциклопедичного характеру;

- інформація про стан довкілля (екологічна інформація);

- інформація про товар (роботу, послугу);

- науково-технічна інформація;

- податкова інформація;
- правова інформація;
- статистична інформація;
- соціологічна інформація;
- інші види інформації.

Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Основними даними про особу є: національність, дата і місце народження, адреса, сімейний стан, освіта, стан здоров'я.

Інформація довідково-енциклопедичного характеру - систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище.

Основні джерела даної інформації: енциклопедії, словники, довідники, рекламні повідомлення та оголошення, путівники, картографічні матеріали, електронні бази та банки даних, архіви різноманітних довідкових інформаційних служб, мереж та систем, а також довідки, що видаються уповноваженими на те органами державної влади та органами місцевого самоврядування, об'єднаннями громадян, організаціями, їх працівниками та автоматизованими інформаційно-телекомунікаційними системами.

Інформація про товар (роботу, послугу) - відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги).

Правова інформація - будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

Джерелами правової інформації є: Конституція України, інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

Науково-технічна інформація - будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Статистична інформація - документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

Соціологічна інформація - будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо[85].

Джерелами соціологічної інформації є передбачені або встановлені законом її носії: документи та інші носії інформації, які є матеріальними об'єктами, що зберігають інформацію, а також повідомлення засобів масової інформації, публічні виступи [18; с.73].

Також розрізняють інформацію *первину*, яка виникає в процесі спеціальних досліджень і *вторинну* – це данні досліджень, які проводилися в минулому, аналітичні узагальнення.

Первину інформацію отримують від:

- рекламного агентства;
- спеціалізованої консалтингової фірми;
- власного, створеного «під дослідження» підрозділу фірми [6].

Збір первинної інформації робиться вищезазначеними структурами. Вони створюють анкети з певними запитаннями, збирають дані за допомогою опитування, систематизують дані, підводять підсумки та передають дані замовнику. Така інформація потребую значних коштів та фірми, які займаються даною роботою нерідко викривляють справжні дані.

А ось вторинна інформація, має дещо свої привілеї. Вона значно дешевша, така інформація набагато швидше дістається. Вторинна інформація знаходиться у спеціалізованих публікаціях, такі як: «Все про бухгалтерський облік», «Вісник АПК», «Економіка України» та за допомогою Інтернету.

1.3. Роль та значення правового регулювання інформаційної безпеки

Сьогодні Україна не може претендувати на інформаційне домінування у світовому інформаційному просторі. Для України головне не відстати, зберігаючи національну, інтелектуальну, культурну та мовну самобутність. Усе це вимагає замислитися над перспективами використання новітніх інформаційних технологій та розвитку інформаційного суспільства в Україні. Концептуальні засади державної політики України в інформаційній сфері мають формуватися, зважаючи на національні інтереси країни, збалансовуючи інтереси особистості, суспільства і держави.

Тому існуюча політика держави в інформаційній сфері спрямована як на розвиток безпосередньо інформаційної сфери, так і на підвищення ефективності розвитку державності, безпеки, оборони пріоритетних галузей економіки, фінансової та грошової системи, соціальної сфери, галузей екології та використання природних ресурсів, науки, освіти і культури, міжнародного співробітництва за допомогою інформаційної сфери. Це підтверджується і Концепцією Національної програми інформатизації, в якій інформаційна сфера, інформатизація розглядається як важливий засіб для розвитку України [86].

Виробництво інформаційного продукту, а не продукту матеріального визначає інформаційне суспільство. Інформація та знання стають головними стратегічними ресурсами такого суспільства, в якому інформація проникає у всі сфери суспільства та держави.

Українська дослідниця Ірина Березовська слушно зауважує, що «в умовах становлення інформаційного суспільства в Україні і світі пріоритетне місце серед різних напрямів державного управління посідає управління інформаційною сферою. Фундаментальною основою його здійснення виступають норми права, які покликані врегулювати та впорядкувати відповідні управлінські процеси, забезпечили їх цілеспрямованість, системність, стабільність і збалансованість. Розглядаючи інформаційну безпеку як одну зі складових національної безпеки, вирішуючи завдання розвитку інформаційної сфери в Україні та проблеми створення умов для побудови

інформаційного суверенітету країни, неможливо обійтись без надійного правового підґрунтя» [9, с.32].

Сьогодні в національному законодавстві не легалізовано поняття «інформаційна сфера». В теперішній час як на побутовому, так і на науковому рівні інформаційна сфера розглядається як сфера, яка формується та розвивається під час інформаційної діяльності. У зв'язку з цим дослідження державного управління в інформаційній сфері виступає актуальним завданням сучасної адміністративно-правової науки.

З огляду державного управління в інформаційній сфері варто загалом, розуміти підзаконну виконавчо-розпорядчу діяльність уповноважених державних органів, їх посадових осіб з реалізації функцій і завдань держави у сфері суспільних інформаційних та інформаційно-інфраструктурних відносин відповідно до інтересів суспільства. Метою державного управління в інформаційній сфері на сучасному історичному етапі є забезпечення задоволення потреб особи і суспільства загалом в інформації як стратегічному ресурсі його розвитку.

Нині в нашій державі управління інформаційною сферою здійснює 5 основних органів державної влади: 2 регуляторних органи – Національна рада України з питань телебачення і радіомовлення та Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, а також 3 органи виконавчої влади – Державний комітет з телебачення та радіомовлення України, Держінформнауки України та Державна служба спеціального зв'язку та захисту інформації України.

Протидія загрозам інформаційній безпеці на підприємстві передбачає пріоритетний розвиток системи нормативно-правового регулювання відносин у цій сфері. Це зумовлено декількома чинниками: по-перше, інтеграція України в міжнародне співтовариство вимагає закріплення і впровадження міжнародних стандартів з інформаційної безпеки; по-друге, захист національних інтересів та реалізація гарантій прав і свобод громадян передбачає особливу роль органів

державної влади, які несуть основну відповідальність за національну та інформаційну безпеку.

Правова база забезпечення інформаційної безпеки складається із норм міжнародних договорів України, законів України, актів Президента України, постанов уряду та нормативних актів органів державної влади, які регулюють відносини у цій сфері.

Під нормативно правовим регулюванням інформаційної безпеки України розуміється форма владного впливу на суспільні інформаційні відносини, що здійснюються державою з метою їх упорядкування, закріплення і забезпечення [48; с.56].

Так, нормативно-правове регулювання інформаційної безпеки ту сфері прав та свобод здійснюються Конституцією України і базовими законами України «Про інформацію», «Про науково-технічну інформацію», «Про Національну програму інформатизації», «Про концепцію національної програми інформатизації», «Про поштовий зв'язок» та ін.

Зазначені нормативно-правові акти регулюють питання забезпечення інформаційної безпеки, питання захисту інформації, охорони державної таємниці, забезпечення захисту конфіденційної інформації, інформаційних ресурсів.

Недоліком нормативно-правового регулювання інформаційної безпеки України є розпорошення його у численних нормативно-правових актах різної юридичної сили. Причому важливі проблеми нормативно закріплюється підзаконними нормативно-правовими актами.

Не менш важливою проблемою для ефективного забезпечення інформаційної безпеки України є неузгодженість нормативно-правових актів як між собою, так із чинною Конституцією.

В.А. Ліпкан зазначає, що інформаційна безпека України є органічною складовою національної. Нормальна життєдіяльність суспільства визначається рівнем розвитку, якістю функціонування і безпекою інформаційного середовища, а також рівнем і станом нормативно-правового забезпечення

даних процесів. Інформаційне законодавство спрямоване на закріплення державної інформаційної політики, яка передбачає забезпечення гарантованого рівня національної безпеки в інформаційній сфері, виключення монополізму в даній області, запобігання розроблення інформаційно деструктивних технологій впливу на антропогенну популяцію, захист авторських і суміжних прав [45, с.194].

Інформаційна безпека забезпечується проведенням єдиної державної політики національної безпеки в інформаційному просторі, системою заходів політичного, економічного, правового характеру, адекватних загрозам та небезпекам національних інтересів особи, суспільства та держави в інформаційній сфері.

Правове забезпечення інформаційної безпеки створюються сукупністю системи правового регулювання забезпечення інформаційної безпеки та процесу формування цієї системи. В.А. Ліпкан зазначає, що функціонування системи забезпечення інформаційної безпеки не обмежується лише нормативно-правовими актами держави, а й включає визначену державну політику в цій сфері[45; с.198].

Концептуальні основи державної політики інформаційної безпеки і безпеки обігу інформації в Україні та міжнародних відносинах включають: 1) розгляд інформаційної безпеки в якості об'єкта управління, що відображено у Законі України «Про національну безпеку України» від 21 червня 2018 року [www.rada.gov.ua]. Виходячи із положень цього закону можна зробити висновок, що сьогодні в основу національної інформаційної безпеки покладена ідея про те, що вона є справою усіх міністерств, відомств та інших суб'єктів України, що функціонально співпрацюють та задіюють існуючий інтелектуальний, організаційний та матеріально-технічний потенціал. Такий підхід дозволяє оцінити і спрогнозувати ефективність діючої управлінської системи щодо попередження й нейтралізації її інформаційній безпеці.

Конституція України в статті 17 надає інформаційній безпеці статусу, обсягу і змісту як окремі функції держави, що виявляється в її законах,

зокрема визнання пріоритету серед інших напрямків державної діяльності [105, с.25]. Основні правила щодо ведення інформаційної діяльності, тобто одержання, використання, поширення та зберігання інформації і захисту прав суб'єктів інформаційних відносин містяться у статтях 31, 32, 34, 41, 54 Конституції України, яка гарантує свободу в цій сфері. Остання може бути обмежена законом лише в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [33].

2) У процесі розширення міждержавного співробітництва захист інформаційних ресурсів України розглядається як підсистема загальної системи захисту інформації. Отже, ефективно діюча національна система забезпечення інформаційної безпеки є важливою передумовою міжнародних інтеграційних процесів.

3) Інформаційна сфера розглядається як системоутворюючий фактор соціальної системи суспільства, а її безпека як впливовий фактор у всіх сферах його життя. Це означає, що вимоги інформаційної безпеки повинні бути включені в усі рівні законодавства. Звідси можна виділити певну структуру нормативно-правових актів, спрямованих врегулювати відносини інформаційної безпеки суспільства:

а) конституційне законодавство;

б) загальні закони, кодекси, які включають норми з питань інформаційної безпеки;

в) закони управлінського характеру, що стосується окремих структур національного господарства, системи державних органів та визначають їх статус;

г) спеціальні закони (як, наприклад, Закон України «Про інформацію»), що регулюють конкретні процеси в сфері правового забезпечення інформаційної безпеки;

д) підзаконні нормативні акти із забезпечення інформаційної безпеки;

е) законодавство України, що містить норми про відповідальність за порушення у сфері інформаційної безпеки. Так, важливим етапом розвитку законодавства у сфері правової охорони комерційної таємниці стало введення в дію 1 січня 1997 р. Закону України «Про захист від недобросовісної конкуренції», який містить норми, що означають такі прояви недобросовісної конкуренції як неправомірне збирання, розголошення, схиляння до розголошення та неправомірне використання комерційної таємниці, а також встановлює відповідальність за прояви недобросовісної конкуренції та правові засади захисту від недобросовісної конкуренції. Але закон встановлює заходи юридичної відповідальності лише для юридичних осіб (ст. 21, 22 Закону). Відповідальність фізичних осіб, як суб'єктів підприємницької діяльності, так і тих, хто не є підприємцями за вчинення дій, визначених як недобросовісна конкуренція у формі порушення прав на комерційну таємницю, виключена зі сфери його дії і введена в законодавство про адміністративні правопорушення.

Кримінальна відповідальність за порушення прав на комерційну таємницю була встановлена Кримінальним кодексом України від 2001 р.

Адміністративна відповідальність за порушення щодо комерційної таємниці, встановлюється кодексом України про адміністративні правопорушення. Протоколи про адміністративні правопорушення передбачені статтею 164-3 КУпАП, мають право складати посадові особи органів Антимонопольного комітету України, а самі справи про правопорушення розглядають суди. [105; с. 28]

Отже, правову основу забезпечення інформаційної безпеки в Україні складають Конституція, закони, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також підзаконні нормативно-правові акти, видані на їх виконання.

Слід зауважити, що закон України «Про національну безпеку України» від 21 червня 2018 року є загальним законом, що містить норми з питань інформаційної безпеки. Його аналіз дає підстави зробити наступні висновки:

1) закон визначає основи та принципи національної безпеки і засади державної політики в цьому напрямі;

2) у зв'язку з прийняттям цього закону втратили чинність ряд законів: Закон України «Про основи національної безпеки України» 2003 р., Закон України «Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави» 2003 р., Закон України «Про організацію оборонного планування» 2005 р;

3) до позитивних аспектів закону можна віднести:

- закріплення захисту людини і громадянина у якості мети державної політики у сфері національної безпеки;
- в якості основного принципу у сфері безпеки визначається дотримання міжнародно-правових зобов'язань України;
- забезпечення верховенства права як одне із завдань, що викреслюється в контексті поняття «демократичний цивільний контроль»;

4) дискусійними залишаються:

- наведені у законі визначення «державна безпека» , «національна безпека», які не відповідають ст. 3 Конституції України, де найвищою соціальною цінністю виступають людина, її життя, здоров'я, недоторканість і безпека, ні ч.1ст.3 зазначеного Закону;
- положення статті 5 закону, котрі відсилають до статей 106 -107 Конституції України, стосуються здійснення Президентом України контролю за сектором безпеки і розширюють його повноваження, що є неконституційним. Рівномірною мірою це стосується статті 13 Закону.

В цілому ж можна зробити висновок, що закон є прийнятним, але окремі його положення потребують узгодження з іншими законодавчими актами (зокрема, із Конституцією України). Із змісту закону інформаційна безпека постає складовою національної безпеки.

Інформаційні правовідносини характеризується своєю динамічністю і сьогодні можна відмітити недостатність правового врегулювання правової бази щодо інформаційної безпеки. Така ситуація спотворює низку перешкод на шляху повноцінної реалізації державою свого обов'язку щодо забезпечення інформаційної безпеки. На нашу думку, постала нагальна потреба в розробленні єдиного комплексного законодавчого акта, який би забезпечив:

- створення єдиної стратегії державної політики у сфері інформаційної безпеки;
- визначення правового статусу суб'єктів інформаційних відносин, встановлення їх відповідальності за дотримання національного законодавства в цій сфері;
- створення системи підготовки кадрів, які використовуються в галузі забезпечення інформаційної безпеки [64; с. 46].

РОЗДІЛ 2. МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

2.1. Організація захисту інформації на підприємстві

Динаміка розвитку та використання інформаційних технологій фактично в усіх сферах діяльності людини спонукає до розгляду та удосконалення науковими дослідниками, спеціалістами питання організації захисту інформації в усіх сферах суспільних взаємовідносин, в тому числі, під час здійснення підприємницької діяльності.

В будь-якій сфері, що стрімко розвивається, практика застосування нових механізмів, технологій виявляє прогалини, які необхідно заповнювати як в нормативному, організаційному так і в технічному рівні. При затягнутій системі прийняття та впровадження рішень державними органами найбільш «оперативними» у використанні прогалин зазвичай виявляються недобросовісні учасники ринку, які уміло використовують їх з метою отримання фінансової або іншої вигоди.

Необхідність застосування на підприємстві заходів з безпеки загалом та інформаційної безпеки як її складової є очевидною для всіх підприємств не дивлячись на їх розміри та сфери діяльності, оскільки шкоду підприємству можуть нанести навіть незумисні дії (наприклад, дії некваліфікованого персоналу), чи дії не спрямовані проти конкретного підприємства (масовані хакерські атаки, spam розсилки, інше). Якщо зупинення або ж мінімізацію збитків від незумисних дій можливо досягти задіявши досить обмежені людські, матеріально-технічні чи фінансові ресурси, то для протидії цілеспрямованим атакам на інформаційний ресурс підприємству необхідно створення ефективної системи захисту.

Беззаперечним є і той факт, що вирішення складного завдання потребує комплексного, системного підходу з використанням усіх заходів, засобів та матеріально-технічного ресурсу. Особливого значення питання збереження інформаційного ресурсу набуло в сучасному світі, коли значно зросла питома вага використання інформації чи технології її обробки, передачі, зберігання у

виробничому процесі. Для прикладу, можемо уявити наслідки втрати чи спотворення інформації для логістичних компаній. Порушення строків чи унеможливлення виконання договірних зобов'язань, втрата репутації та довіри на ринку, партнерів, контрагентів і, можливо, припинення діяльності. Крім цього, замовники послуг можуть звернутися до господарського суду з позовами про відшкодування завданих матеріальних або моральних збитків.

Отже, недбале ставлення до організації захисту інформації на підприємстві призводить не тільки до порушення виробничих процесів на підприємстві, а і ставить під сумнів досягнення основної статутної мети їх створення – отримання прибутку.

Крім цього, без організації ЗІ на підприємстві, що буде включати: (категоріювання) інформації, встановлення спеціального режиму роботи з окремими категоріями інформації, визначення місць зберігання, умов доступу, кола осіб, що наділяються правом доступу до інформації і юридичному закріплення цих та інших заходів стає неможливим обґрунтування претензії, позовів до господарського суду, щодо дій недобросовісних користувачів інформації підприємства.

Теоретичні дослідження та практика побудови системи захисту інформації на підприємстві дають доволі чітку уяву про її складові елементи та процес організації.

Досить інформативно структуру зазначеного процесу викладено в роботах Зубок М.І. [25; с. 86]

Структурні елементи процесу організації інформаційної безпеки на підприємстві та послідовність їх реалізації, викладену Зубок М.І., зображено на рис.2.1.

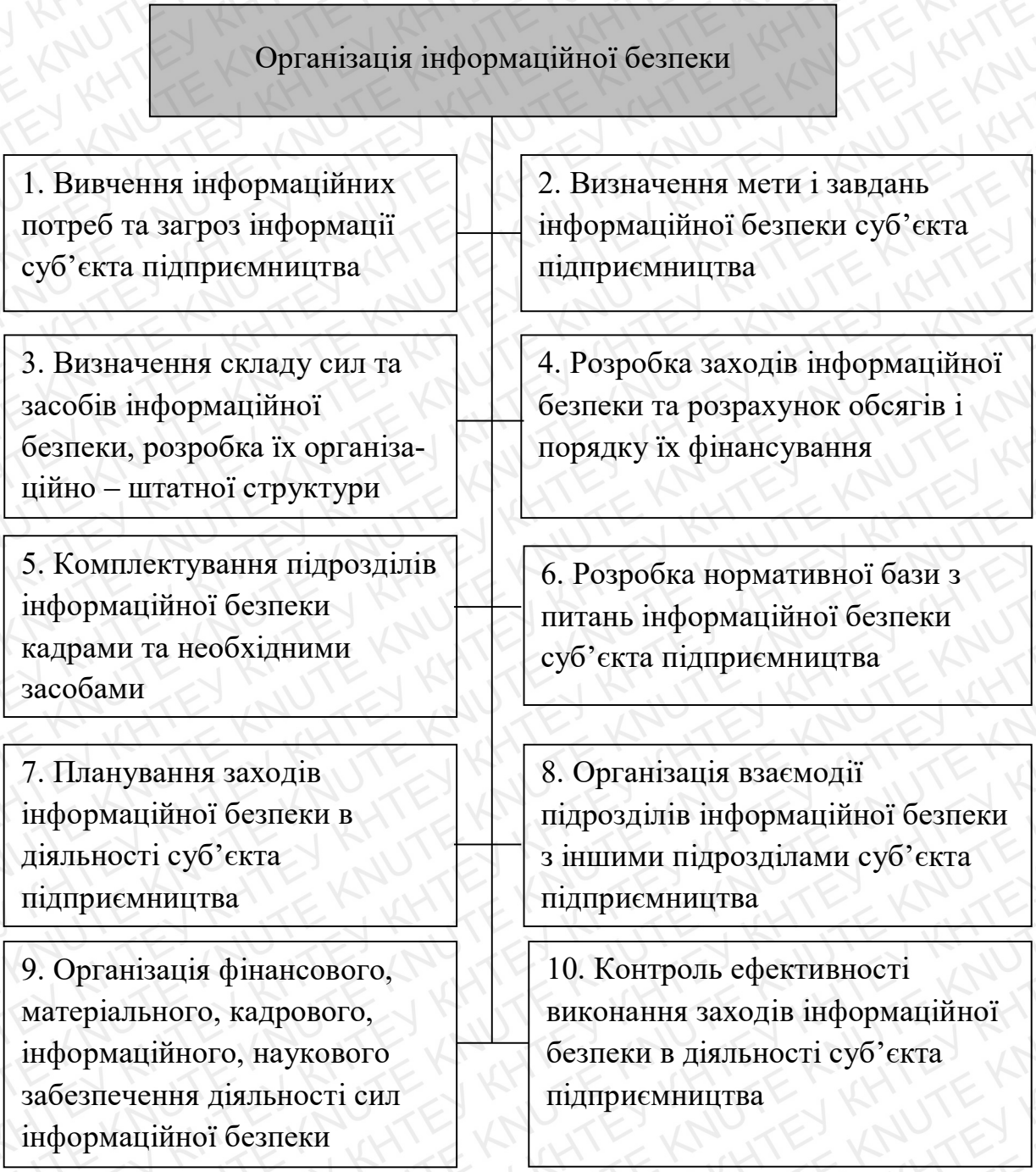

Рис.2.1 Структура процесу організації інформаційної безпеки суб'єкта підприємництва [25; с. 86].

Вивчення інформаційних потреб і загроз (вразливості інформації) є початковим елементом організації інформаційної безпеки. За результатами проведеного аналізу усвідомлюється необхідність та приймається рішення про побудову системи ЗІ на підприємстві. Аналіз вразливості дозволяє зробити три ключових висновки:

- Цінність інформації. Чи є вона вагомим ресурсом підприємства задіяним у виробничому процесі та чи призведе її витік, пошкодження чи втрата, до порушення діяльності.
- Захищеність інформації. Який поточний стан зберігання, використання та збереження інформації. Вірогідність її втрати, спотворення чи несанкціонованого доступу.
- Політика захисту інформації. Наявність, стан дотримання та ефективність захисту інформації на підприємстві.

Проведений аналіз дає можливість сформулювати вихідні дані про наявність на підприємстві інформації яка потребує особливої уваги та захисту, її цінність у виробничому процесі та здійснити оцінку потенційних ризиків і загроз. З урахуванням аналізу та за наявності матеріально-технічних, фінансових і кадрових ресурсів керівництвом підприємства приймаються рішення та формуються завдання, кінцевою метою яких є створення умов існування інформаційних ресурсів при яких забезпечується їх цілісність.

Загальна сукупність заходів для протидії загрозам інформаційної безпеки (ІБ), захисту і збереження інформаційного ресурсу підприємства визначається в базовому документі - «Політика інформаційної безпеки»(ПІБ). Зазначений документ розробляється на підставі чинного законодавства України у сфері захисту інформації, та рекомендацій державних і міжнародних стандартів. Наприклад, для банківської сфери це: стандарт Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги» (ISO/IES 27001:2005, MOD); СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності: звід правил для управління інформаційною безпекою» (ISO/IES 27002:2005, MOD), а також міжнародний стандарт ISO/IEC 27001:2005 та ISO/IEC 27002:2005.

ПІБ – це набір, вироблених на підприємстві правил і вимог з інформаційної безпеки, що регламентують усі сфери його діяльності та забезпечують безпечне використання інформаційних ресурсів за допомогою

комплексного застосування організаційних, адміністративних, правових, програмних, апаратних, фізичних заходів, методів, засобів.

За визначенням, наведеним Зубок М.І «політика інформаційної безпеки – це прийнята у суб'єкта підприємництва сукупність норм, правил, рекомендацій згідно яких будується система його інформаційної безпеки та управління нею. Вона реалізується за допомогою організаційних заходів і програмно-технічних засобів, які визначають архітектуру системи захисту та за допомогою засобів управління механізмами захисту»[25; с. 116].

Сьогодні, українські компанії широко використовують позитивний досвід зарубіжних країн у сфері захисту інформації. Британський інститут стандартів (BSI) за участю комерційних організацій, таких як Shell, National Westminster Bank, Midland Bank, Unilever, British Telecommunications, Marks & Spencer, Logica і ін. розробив стандарт інформаційної безпеки BS 7799, який в 1995 р був прийнятий в як національний стандарт управління інформаційною безпекою організації незалежно від сфери діяльності компанії. Відповідно до цього стандарту будь-яка служба безпеки, IT-відділ, керівництво компанії повинні починати працювати відповідно до загального регламенту. Неважливо, йдеться про захист паперового документообігу або електронних даних. В даний час Британський стандарт BS 7799 підтримується в 27 країнах світу, в числі яких країни Британської Співдружності, а також Швеція і Нідерланди. У 2000 р міжнародний інститут стандартів ISO на базі британського BS 7799 розробив і випустив міжнародний стандарт менеджменту безпеки ISO / IEC 17799. Сьогодні можна стверджувати, що BS 7799 і ISO 17799 це один і той же стандарт, який має на сьогоднішній день світове визнання і статус міжнародного стандарту ISO.

Британський стандарт BS 7799:1995, рекомендує включати в документ, що характеризує політику безпеки організації, такі розділи:

- вступний, підтверджуючий заклопотаність вищого керівництва проблемами інформаційної безпеки;

- організаційний, що містить опис підрозділів, комісій, груп і т.д., що відповідають за роботи в галузі інформаційної безпеки;
- класифікаційний, що описує наявні в організації матеріальні та інформаційні ресурси і необхідний рівень їх захисту;
- штатний, що характеризує заходи безпеки, які застосовуються до персоналу (опис посад з точки зору інформаційної безпеки, організація навчання і перепідготовки персоналу, порядок реагування на порушення режиму безпеки і т.п.);
- розділ, що висвітлює питання фізичного захисту;
- керуючий розділ, що описує підхід до управління комп'ютерами та комп'ютерними мережами;
- розділ, що описує правила розмежування доступу до виробничої інформації;
- розділ, що характеризує порядок розробки та супроводу систем;
- розділ, що описує заходи, спрямовані на забезпечення безперервної роботи організації;
- юридичний розділ, що підтверджує відповідність політики безпеки чинному законодавству [3, с.13]

Найбільшої ефективності захисту можливо досягти за допомогою виконання комплексу завдань з використанням всіх можливих заходів, передбачених ПІБ.

За частотою застосування заходи бувають:

- разові – наприклад, створення нормативно-правової бази, категоріювання інформації, заходи під час проектування та впровадження об’єктів ІІ, створення підрозділів ІІ, встановлення режиму роботи, розробка політики безпеки, інші;
- періодичні (за потребою) – наприклад, кадрові зміни, ремонти і модифікація об’єктів ІІ, заходи в ході окремих мероприємств, інші;
- постійні – наприклад, забезпечення достатнього рівня фізичного захисту об’єктів ІБ, контроль за роботою системи ІБ, аналіз звітів,

виявлених недоліків, оцінка ефективності системи.

Всі заходи та засоби по захисту інформації можна поділити на декілька груп:

1. Організаційні(адміністративні).
2. Правові.
3. Інженерно-технічні.
4. Програмно-апаратні.
5. Криптографічні.
6. Фізичні.

Окремим етапом в організації захисту інформації в діяльності підприємства є визначення режиму функціонування інформації. Як правило обирається варіант трьох видів режиму функціонування інформації:

- повністю закритий;
- частково закритий;
- періодично закритий.

Перші два види відрізняються колом осіб, що мають доступ до інформації, та обсягом інформації відповідно. Третій режим застосовується у випадках розширення діяльності на нові території, ринки та сфери.

Способи захисту інформації, які застосовує підприємство в умовах обраного режиму функціонування поділяють на активні (протидія) та пасивні (захист).

Активними можна вважати періодичну атестацію приміщень, в яких зосереджена цінна для суб'єктів підприємництва інформація або проводиться робота з нею, а також періодичне обстеження засобів обробки і передачі інформації. Сюди ж доцільно віднести періодичні перевірки наявності документів та вимірювання електромагнітних випромінювань і наводок. Обов'язковим має бути встановлення контролю персоналу, допущеного до роботи з інформацією обмеженого доступу суб'єктів підприємництва.

У окремих випадках, з метою протидії посяганням на інформацію суб'єктів підприємництва, останні можуть вдаватись до дезінформації осіб,

які генерують такі загрози щодо місць знаходження інформації, її важливості, провокувати їх на дії через які вони будуть компрометувати себе.

Серед способів захисту інформації може бути її нормування, розмежування доступу до різної за цінністю інформації, поставлення акустичних, електромагнітних та технічних завад, запровадження пропускного режиму, спеціальна охорона місць зберігання інформації і т. д.

До технічних засобів регулювання доступу можна віднести кодовані замки на вході в приміщення де знаходиться відповідна інформація, встановлення засобів та систем пропуску на територію суб'єкта підприємництва, спеціальні прилади та пристрої, що регулюють доступ до інформації, яка зберігається у комп'ютерах. За допомогою програмних засобів розмежовується доступ до інформації в інформаційних комп'ютерних системах і мережах. Правові засоби є загальними, які встановлюють як порядок роботи з інформаційними ресурсами суб'єкта підприємництва, так і умови та правила використання технічних та програмних засобів захисту інформації.

До *пасивних* засобів можна віднести контроль і обмеження доступу на об'єкти, звукоізоляцію приміщень, встановлення фільтрів-обмежувачів, лінійних фільтрів та інші [25; с.98].

Для забезпечення організаційного й правового захисту інформації необхідно розробити пакет документів, щодо регламентації ЗІ на підприємстві та вжити заходів, щодо доведення до персоналу та інших потенційних користувачів встановлених правил та обмежень.

З юридичної сторони, необхідно перевірити наявність і за необхідністю доповнити установчі документи підприємства окремим розділом, щодо права самостійно встановлювати обсяг відомостей, що становлять комерційну й іншу охоронювану законом таємницю й порядок її захисту. Також закріпити право вимагати від персоналу, партнерів, контрагентів та інших фізичних і юридичних осіб, установ і організацій забезпечення нерозголошення конфіденційних відомостей підприємства. Така можливість закріплена

законодавчо в главі 46 Цивільного кодексу України, ст. 30 Закону України «Про інформацію», ст. 162 ГКУ.

Документальне оформлення правового статусу комерційної таємниці та конфіденційної інформації на підприємстві надає можливість її захисту як у випадку зумисного чи незумисного розголошення працівниками підприємства, так і вчинення незаконних дій інших осіб щодо її викрадення.

Одним із головних документів в системі ЗІ є *Положення про конфіденційну інформацію підприємства.* Воно розробляється з метою охорони і захисту конфіденційності інформації (КІ), що становить комерційну таємницю, власником якої є підприємство та регулює доступ до даної інформації, порядок надання, передачі, встановлює відповідальність за її розголошення чи порушення встановленого порядку роботи з нею.

Формування переліку відомостей, що становлять комерційну таємницю та конфіденційну інформацію підприємства проводиться відповідно до ст. 505 ЦК України та ч. 2 ст. 30 Закону України «Про інформацію».

Перелік відомостей підприємства, що містять КІ, приймається окремим документом, чи як додаток до попереднього положення. В ньому визначаються всі відомості, що становлять комерційну таємницю підприємства у всіх сферах діяльності: виробництва, управління, економіки, фінансів, планів, документообігу, кадрів та інших за необхідністю. В переліку описані всі групи й види КІ, яка підлягає особливому режиму поводження. Це важливо не тільки з точки зору її збереження, а і захисту від неправомірного використання.

Слід зауважити про відомості, які не можуть становити комерційну таємницю. Постановою Кабінету Міністрів України від 09.08.93 р. № 611 «Про перелік відомостей, що не становлять комерційної таємниці», встановлено, що комерційну таємницю не становлять: установчі документи; документи, що дозволяють займатися підприємницькою, господарською діяльністю чи її окремими видами; інформація у всіх встановлених формах державної звітності; дані, необхідні для нарахування і сплати податків та інших обов'язкових платежів; документи про сплату податків та обов'язкових платежів; документи

про платоспроможність; відомості про участь посадових осіб підприємств в кооперативах, малих підприємствах, союзах, об'єднаннях та інших організаціях, що займаються підприємницькою діяльністю; відомості, що у відповідності з діючим законодавством підлягають оголошенню. Ці відомості підприємства зобов'язані надати органам державної виконавчої влади, контролюючим та правоохоронним органам України, а також іншим юридичним особам на їх вимогу [88].

Формування переліку носить важливе значення в організації захисту інформації. По-перше, працівник повинен знати і розуміти які відомості потребують чіткого дотримання встановлених вимог до процесу їх обробки, використання, зберігання, пересилання чи навіть утилізації. При цьому, перелік має бути конкретним, а не абстрактним. По-друге, юридичне закріплення режимного статусу відомостей дає підстави для захисту порушених прав у судовому порядку. Для створення переліку відомостей на підприємстві створюється комісія, яка отримує пропозиції про включення до нього від керівників всіх структурних одиниць підприємства та готує підсумковий документ у тісній співпраці з юридичним підрозділом і службою безпеки. Результати роботи комісії, затверджуються наказом керівника підприємства.

Зазвичай, рівень контролю над доступом до КІ компанії залежить від класифікації її за рівнем конфіденційності, який розподіляються орієнтовно на:

- «ДСК» для службового користування - найнижчий гриф конфіденційності, що присвоюється на телефонні довідники, журнали реєстрації, службове листування, внутрішні розпорядчі документи й т. д.
- "КОНФІДЕНЦІЙНО" – угоди; відомості про персонал, контрагентів; фінансово-економічну діяльність і т.д.
- "СУВОРО КОНФІДЕНЦІЙНО" - документи про найважливіші аспекти комерційної діяльності підприємства, його стратегію, фінансове становище.

Рівень конфіденційності та термін дії кожного документа визначає його розробник за погодженням із керівником підрозділу захисту інформації.

На підприємстві має бути проведено категоріювання обєктів, яке здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об'єкті. Загальні вимоги з категоріювання, ознаку, за якою здійснюється категоріювання, а також порядок категоріювання об'єктів інформаційної діяльності, в тому числі об'єктів електронно-обчислювальної техніки (далі – об'єкти), де циркулює (обробляється технічними засобами та/або озвучується) інформація з обмеженим доступом, що не становить державної таємниці встановлені Положенням про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці, яке розроблено відповідно до Закону України "Про Державну службу спеціального зв'язку та захисту інформації України" та Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27.09.1999 № 1229 [90].

Об'єктами категоріювання є об'єкти інформаційної діяльності. Категоріювання здійснюється за ознакою: ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єктах інформаційної діяльності.

Об'єктам, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, встановлюється четверта (IV) категорія.

За рішенням розпорядників (користувачів) інформації або за рішенням власників (розпорядників, користувачів) об'єктів, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, об'єктам може встановлюватися ІІІ категорія.

Об'єкти, яким встановлено відповідну категорію, вносяться до Переліку категорійованих об'єктів, який ведеться власником (розпорядником, користувачем) об'єктів інформаційної діяльності.

Порядок категоріювання об'єктів.

Категоріювання об’єктів здійснює їх власник (розпорядник, користувач).

Категоріювання об’єктів проводиться комісією з категоріювання установи-власника (розпорядника, користувача) об’єкта.

Комісія з категоріювання визначає ступень обмеження доступу до інформації, яка оброблятиметься технічними засобами та/або озвучуватиметься на об’єкті, та з урахуванням цього ступеня встановлює категорію об’єкта. Встановлена категорія зазначається в Акті категоріювання об’єкта, який складається комісією з категоріювання за результатами її роботи.

Акт категоріювання об’єкта є чинним протягом 5 років з моменту проведення категоріювання, якщо не змінилась ознака, за якою була встановлена категорія об’єкта.

Первинне категоріювання здійснюється у разі створення ОІД, де буде оброблятися технічними засобами та/або озвучуватися інформація з обмеженим доступом, що не становить державної таємниці. Чергове категоріювання здійснюється не рідше ніж один раз на п’ять років. Позачергове категоріювання здійснюється у разі зміни ознаки, за якою була встановлена категорія об’єкта [80].

Інструкція із захисту КІ в інформаційній системі підприємства визначає обов’язковий для підрозділів, працівників порядок обліку, зберігання, використання та знищення документів, справ, видань, магнітних та інших матеріальних носіїв інформації, які містять КІ, що є власністю підприємства.

Положення про конфіденційне діловодство визначає порядок роботи з документами, які містять КІ.

Важливим організаційним питанням є доведення до працівників, користувачів інформації встановлених вимог та правил поводження з КІ. Чинним законодавством не передбачено підписання працівником угоди про нерозголошення КІ, однак судова практика вказує, що підписання трудового контракту чи ознайомлення з наказом про прийом на роботу засвідчує згоду працівника з умовами роботи, встановленими підприємством, в тому числі

умови поводження з КІ. Слід організувати ознайомлення працівників з положеннями розпорядчих документів, інструкцій, вимог та інших у сфері ЗІ.

Документами, які регулюють питання поводження з КІ у *взаємовідносинах з працівниками*, крім зазначених вище положень та переліків є:

- трудовий договір, контракт із керівником і колективного договору;
- угода зі працівником про нерозголошення КІ підприємства;
- зобов'язання працівника про нерозголошення КІ після закінчення трудових відносин;
- посадові інструкції;
- відомість про ознайомлення співробітників підприємства з положеннями та інструкціями із захисту КІ;
- правила внутрішнього трудового розпорядку підприємства (щодо регламентації засобів фізичного захисту інформації й питань режиму);
- план проведення занять із штатними працівниками щодо збереження й нерозголошення КІ.

Окрему увагу слід звернути на підбір та постійну роботу з персоналом підприємства. Проведення навчань співробітників, підготовка для них методичних положень, інструкцій, пам’яток, пов’язаних з поводженням з комерційною таємницею, створення матеріальних і моральних стимулів, що спрямовані на збереження комерційної таємниці повинні стати невід’ємною частиною заходів із збереження конфіденційної інформації на підприємстві.

Для *ознайомлення та навчання співробітників* розробляється «Рекомендаційний план виховання і навчання співробітників підприємства з питань збереження комерційної таємниці підприємства». Орієнтовний зміст плану має включати наступні теми:

- Ринкова економіка і необхідність захисту конфіденційної інформації. Поняття комерційної таємниці, її ознаки.
- Практика (досвід) захисту комерційних секретів у країнах із традиційною ринковою економікою.

- Необхідність і значення захисту комерційних секретів підприємства в умовах ринку.
- Вивчення положення про комерційну таємницю підприємства і правил її збереження.
- Правові основи захисту комерційної таємниці.
- Методика визначення відомостей, що становлять комерційну таємницю підприємства.
- Категорії відомостей, що підлягають захисту на підприємстві. Вивчення переліку відомостей, що становлять комерційну таємницю
- Дозвільна система доступу до відомостей і документів, що становлять комерційну таємницю.
- Обов'язки, права і відповідальність працівників підприємства при користуванні документами і відомостями, що становлять комерційну таємницю. Види відповідальності за розголошення комерційних секретів.
- Основні причини й обставини можливого витоку конфіденційної інформації.
- Вимоги до укладання договору, контракту, угоди про господарську діяльність, що містять конфіденційну інформацію. Порядок забезпечення режиму в роботі з іноземними юридичними і фізичними особами, представниками органів державного управління, партнерами, клієнтами і засобами масової інформації.
- Роль підрозділу безпеки в організації і проведенні роботи зі збереження комерційних секретів.
- Порядок забезпечення режиму при обробці комерційних секретів на ЕОМ і користування ними.

Необхідно також визначити порядок збереження комерційної інформації при укладанні договорів та проведенні ділових переговорів.

У взаємовідносинах з контрагентами підприємства усталена практика внесення розділів про дотримання конфіденційності до договірної

документації. Стандартними є договірне зобов'язання не розголошувати інформацію, яка стала відома в ході укладання та виконання договірних зобов’язань в будь-який спосіб третім особам, крім випадків визначених законодавством та відшкодувати іншій стороні в повному обсязі всі збитки, заподіяні невиконанням цього пункту. Термін дії такого зобов’язання зазвичай тотожний терміну дії договору, а іноді і протягом обумовленого сторонами строку після припинення дії договору.

Створити на підприємстві відповідно до закону «Про інформацію» *порядок поводження з інформацією обмеженого користування*, який виключає можливість втрати інформації при розроблення рекламних матеріалів, під час проведення чи участі в наукових конференціях, семінарах, виступах в пресі.

Окремим документом необхідно визначити *порядок взаємодії з представниками правоохоронних органів*, виконавчої влади, які відповідно до законодавства можуть мати доступ до комерційної таємниці при виконанні ними своїх завдань. Дотримання даної рекомендації дозволить представникам підприємства почувати себе впевнено при проведенні перевірок контролюючими органами. Перевіряючі повинні будуть дотриматися всіх процедур, які встановлені на підприємстві для одержання доступу до комерційної таємниці

Організація спеціального діловодства з метою врегулювання порядку роботи та поводження з документами, яким надано спеціальний режим захисту.

На сьогодні, як і взагалі у сфері інформаційної безпеки суб’єктів підприємництва, так і в питаннях правового її регулювання нормативно-правовими документами самих суб’єктів стійкої позиції немає.

Беручи до уваги мету, завдання та зміст інформаційної безпеки суб’єктів підприємництва, структуру процесу її організації та напрацьований досвід, можна рекомендувати наступний перелік таких нормативно-правових документів:

- Положення про комерційну таємницю та правила її зберігання на підприємстві (у банку).

- Положення про конфіденційну інформацію підприємства (банку).
- Інструкція про порядок підготовки, обліку, зберігання та знищення документів, справ, видань і матеріалів, що містять комерційну таємницю та конфіденційну інформацію підприємства (банку).
- Положення про захист електронної інформації та електронних документів на підприємстві (у банках питання захисту електронної інформації здійснюється відповідно до нормативно-правових документів НБУ).
- Інструкція про порядок виконання документів, що надходять до підприємства (банку) від правоохоронних органів, судів та інших державних установ.
- Положення про архів і архівну діяльність підприємства (банку).
- Інструкція про проведення службових розслідувань на підприємстві (у банку).
- Положення про інформаційно-аналітичну роботу на підприємстві (у банку).
- Інструкція з службового діловодства.
- Інструкція з спеціального діловодства.
- Правила використання, поширення та зберігання інформації підприємства (банку) у процесі його діяльності.
- Методики розробки інформаційних документів підприємства (банку) та надання інформаційних послуг.
- Пам’ятки працівникам підприємства, банку по збереженню інформації з обмеженим доступом; інші документи.

Незважаючи на значний перелік документів, всі вони утворюють правове поле суб’єкта підприємництва у сфері забезпечення його інформаційної безпеки, обґрунтовують поведінку суб’єкта у інформаційному середовищі [25; с.136].

Контроль за впровадженням і реалізацією організаційно-правових заходів ЗІ покладається на підрозділ захисту інформації (ПЗІ) шляхом обмеження кола

осіб, які мають доступ до КІ, фізичної збереженості документів, обробки інформації із грифом конфіденційності, внесення вимог щодо конфіденційності конкретної інформації в договори із внутрішніми й зовнішніми партнерами та інших заходів за рішенням керівництва. Допуск працівників до відомостей, що містять КІ, здійснюється керівниками підприємства і ПЗІ.

2.2. Організація і функції підрозділу захисту інформації

Для впровадження заходів по виконанню завдань управління комплексною системою захисту інформації та контролю за її роботою на підприємстві створюється підрозділ захисту інформації(ПЗІ).

ПЗІ реалізує політику інформаційної безпеки підприємства на всіх етапах життєдіяльності комплексної системи захисту інформації (КСЗІ) починаючи з етапу проектування, впровадження та оновлення (удосконалення) КСЗІ, обслуговування при експлуатації, забезпеченні працездатності та контролю за станом забезпечення захищеності інформації в КСЗІ.

У своїй діяльності ПЗІ керується чинними нормативно-правовими актами та нормативними документами у сфері захисту інформації, такими як:

- Закон України «Про державну таємницю»;
- Закон України «Про захист інформації в автоматизованих системах»;
- Положення про технічний захист інформації в Україні;
- інші нормативно-правові акти, що регулюють правовідносини у сфері захисту інформації, державні і галузеві стандарти, розпорядчі та інші документи уповноважених органів влади.
- розпорядчими документами підприємства, Статутом підприємства та Положенням про підрозділ, розробленим і затвердженим на підприємстві.

Підрозділ створюється як окрема штатна одиниця і підпорядковується виключно керівнику підприємства або особі, яка призначена відповідальною за забезпечення інформаційної безпеки на підприємстві. Організаційна структура підрозділу, кількість співробітників повинні бути обґрунтованими і достатніми

для виконання заходів, передбачених політикою інформаційної безпеки підприємства.

Залежно від обсягів і особливостей завдань ПЗІ до її складу можуть входити спеціалісти різних напрямів роботи з питань:

- адміністрування та контролю засобів захисту;
- управління системами доступу та базами даних захисту;
- захисту каналів зв'язку і комутаційного обладнання, налагодження і управління активним мережевим обладнанням;
- захищених технологій обробки інформації;
- захисту інформації від витоку технічними каналами.

Досягнення ефективності роботи підрозділу залежить від якісної комплектації спеціалістами та працівниками, які мають освіту за напрямом підготовки «Інформаційна безпека» або інженерно-технічну освіту фахового спрямування, відповідно до обраного виду роботи, з додатковою підготовкою на курсах перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ чи стажем роботи у галузі ТЗІ за обраним видом роботи.

Для забезпечення роботи ПЗІ необхідно розробити та затвердити Положення про підрозділ захисту інформації та посадові інструкції працівників підрозділ.

Прийняття стратегічних рішень, щодо забезпечення дієвості системи захисту інформації належить до компетенції керівництва підприємства. ПЗІ є основним підрозділом який реалізує політику підприємства в сфері захисту інформації, забезпечую безперебійне функціонування КСЗІ та діє відповідно до прийнятих "Плану захисту інформації", календарних, перспективних та інших планів робіт, затверджених керівником (уповноваженою особою) підприємства.

Функції ПЗІ під час створення комплексної системи захисту інформації. На першому етапі організації системи ЗІ, який описаний в розділі 2.1 ПЗІ приймає безпосередню участь у визначенні переліків відомостей, які підлягають захисту в процесі обробки, класифікації інформації за вимогами до її конфіденційності або важливості для організації, необхідних рівнів

захищеності інформації, визначення порядку введення (виведення), використання та розпорядження інформацією в комплексній системі (КС) за результатами яких розробляються положення та інструкції у сфері ЗІ описані в розділ 2.1.;

– розробка та коригування моделі загроз і моделі захисту інформації в КС, політики безпеки інформації в КС. Для виконання цієї функції ПЗІ відпрацьовує механізми оперативного реагування на загрози, з використання правових, організаційних, інженерно-технічних засобів і методів для виявлення й знешкодження джерел загроз ЗІ. Всі ці заходи відображаються в базовому документі підприємства в сфері захисту інформації – Політика інформаційної безпеки підприємства;

– за результатами аналізу загроз та обраних засобів і методів захисту визначаються і формуються вимог до КСЗІ;

– ПЗІ приймає безпосередньо участь в організації і координації робіт з проектування та розробки КСЗІ, проектних роботах зі створення КСЗІ починаючи з відбору проектних та підрядних організацій та установ;

– підготовка технічних пропозицій, рекомендацій щодо запобігання витоку інформації технічними каналами та попередження спроб несанкціонованого доступу до інформації під час створення КСЗІ;

– організація робіт і участь у випробуваннях КСЗІ, у проведенні її експертизи;

– вибір організацій-виконавців робіт зі створення КСЗІ, здійснення контролю за дотриманням встановленого порядку проведення робіт з захисту інформації, у взаємодії з РСО, службою охорони підприємства, погодження основних технічних і розпорядчих документів, що супроводжують процес створення КСЗІ (технічне завдання, технічний і робочий проекти, програма і методика випробувань, плани робіт та ін.);

– участь у розробці нормативних документів, чинних у межах підприємства і КС, які встановлюють дисциплінарну відповідальність за

порушення вимог з безпеки інформації та встановлених правил експлуатації КСЗІ;

– участь у розробці нормативних документів, чинних у межах підприємства і КС, які встановлюють правила доступу користувачів до ресурсів КС, визначають порядок, норми, правила з захисту інформації та здійснення контролю за їх дотриманням (інструкцій, положень, наказів, рекомендацій та ін.) [106].

Функції ПЗІ під час експлуатації комплексної системи захисту інформації:

– організація процесу керування КСЗІ;

– розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій;

– вжиття заходів у разі виявлення спроб НСД до ресурсів КС, порушення правил експлуатації засобів захисту інформації або інших дестабілізувальних факторів;

– забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;

– організація керування доступом до ресурсів КС (розподілення між користувачами необхідних реквізитів захисту інформації – паролів, привілеїв, ключів та ін.);

– супроводження і актуалізація бази даних захисту інформації (матриці доступу, класифікаційні мітки об’єктів, ідентифікатори користувачів тощо);

– спостереження (реєстрація і аудит подій в КС, моніторинг подій тощо) за функціонуванням КСЗІ та її компонентів;

– підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в КС, впровадження нових технологій захисту і модернізації КСЗІ;

– організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій КС або КСЗІ;

– участь в роботах з модернізації КС – узгодження пропозицій з введення до складу КС нових компонентів, нових функціональних завдань і режимів обробки інформації, заміни засобів обробки інформації тощо;

– забезпечення супроводу та актуалізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їхнього зберігання і тестування;

– проведення аналітичного оцінювання поточного стану безпеки інформації в КС (прогнозування виникнення нових загроз і їх врахування в моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації і реалізованої політики безпеки поточній моделі загроз та ін.);

– інформування власників інформації про технічні можливості захисту інформації в КС і типові правила, встановлені для персоналу і користувачів КС;

– негайне втручання в процес роботи КС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника;

– регулярне подання звітів керівництву підприємства-власника (розпорядника) КС про виконання користувачами КС вимог з захисту інформації;

– аналіз відомостей щодо технічних засобів захисту інформації нового покоління, обґрунтування пропозицій щодо придбання засобів для підприємства;

– контроль за виконанням персоналом і користувачами КС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації, також контроль за забезпеченням режиму обмеження доступу у разі обробки в КС інформації, що становить державну таємницю;

– контроль за забезпеченням охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що підлягають захисту;

– розробка і реалізація спільно з РСО підприємства комплексних заходів з безпеки інформації під час проведення заходів з науково-технічного, економічного, інформаційного співробітництва з іноземними фірмами, а також під час проведення нарад, переговорів та ін., здійснення їхнього технічного та інформаційного забезпечення [106].

2.3. Специфіка технічного захисту інформації

Одним із елементів захисту інформації на підприємстві є технічний захист інформації (ТЗІ).

Технічний захист інформації – це підсистема складної системи, якою є інформаційна безпека. Підрозділи охорони і правового захисту комерційної таємниці суб'єкта господарювання та технічного захисту інформації є штучними організаційними структурами, котрі мають стосунки і взаємозв'язки між собою як ланки функціонування одного рівня складної організаційної системи інформаційної безпеки.

Мета технічного захисту інформації, що становить комерційну таємницю, - запобігання відтоку або порушення цілісності інформації з обмеженим доступом. Вона може бути досягнута шляхом створення механізмів захисту від незаконного проникнення в комп'ютерні системи і мережі, автоматизовані системи, здатного спричинити перекручення або знищення інформації чи то носіїв інформації. Крім того, на практиці застосовуються методи протидії електронним засобам доступу (ЕЗД), що їх використовують злочинці з метою здійснення незаконного переказу грошей не уповноваженою на то особою. В місцях проведення ділових переговорів необхідно встановлювати відповідний режим. У зв'язку з цим приміщення, яке надає одна із сторін, підлягає огляду з застосуванням технічних засобів з метою можливого виявлення засобів несанкціонованого зняття інформації.

Специфіка технічного захисту інформації, крім іншого, полягає в застосуванні спеціальних технічних засобів захисту інформації, які проходять відповідну сертифікацію та щодо яких встановлений чіткий порядок

використання. Крім того, окремі види захисту, як то, наприклад, криптографічний захист – діяльність, що підлягає ліцензуванню. Отже, при виконанні всього комплексу завдань підприємство повинно працювати з відповідними державними та недержавними підприємствами й організаціями, що виконують завдання та працюють у галузі захисту інформації, в тому числі: зі Службою безпеки України, державним підприємствами, приватними підприємствами, що ліцензовані на здійснення окремих видів діяльності в сфері захисту інформації.

Сама по собі інформація може існувати та переноситися у вигляді фізичних полів або речовиною (матеріальним носієм інформації). Наприклад, це може бути акустична хвиля (звук), електромагнітні випромінювання, електричні сигнали, лист паперу з текстом, флешпам'ять, DVD-диск тощо.

Іншими словами, інформація може переноситись тільки в електромагнітному (електричному, магнітному), акустичному та матеріальному вигляді.

По фізичній природі носієм інформації можуть бути:

- світло - електромагнітні хвилі оптичного діапазону (у т.ч. інфрачервоного та ультрафіолетового;
- акустичні (звукові) хвилі;
- електромагнітні хвилі;
- електричні сигнали у провідниках;
- матеріальний носій інформації.

Класифікація шляхів витоку інформації від його носія до недобросовісного користувача за фізичною природою носія(каналу витоку).

Канали витоку інформації:

- акустичний;
- візуально-оптичний;
- електричний;
- електромагнітний;

- матеріальний.

Всі, крім матеріального каналу витоку відносяться до т.з. технічних каналів витоку інформації. При цьому, технічні канали витоку інформації можуть бути як природними так й штучними (спеціально створеними зловмисниками) [18; с.178].

Таким чином, питання ТЗІ поділяють на два великих класи завдань:

- захист інформації від несанкціонованого доступу (НСД);
- захист інформації від витоку технічними каналами.

У залежності від способу циркуляції інформації технічний захист інформації умовно можна розділити на два напрямки:

- технічний захист мовної інформації;
- технічний захист електронної інформації.

Середовищем поширення носіїв ІзОД можуть бути лінії зв'язку, сигналізації, керування, енергетичні мережі, прикінцеве і проміжне обладнання, інженерні комунікації і споруди, захисні будівельні конструкції, а також світлопроникні елементи будинків і споруд (отвори), повітряне, водне та інші середовища, ґрунт, рослинність тощо.

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» (ст. 8) для створення комплексної системи захисту інформації використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Також згідно з Положенням про технічний захист інформації в Україні (пункт 17), затвердженим Указом Президента України від 27 вересня 1999 року № 1229/99, під час розроблення і впровадження заходів з технічного захисту інформації використовуються засоби, дозволені Адміністрацією Держспецзв'язку України для застосування та включені до відповідних переліків.

Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та

інформації формується відповідно до п. 17 Положення про технічний захист інформації в Україні і призначений для використання суб'єктами системи ТЗІ під час розроблення, модернізації та впровадження комплексів ТЗІ на об’єктах інформаційної діяльності та КСЗІ в автоматизованих системах (АС). Перелік містить номенклатуру засобів ТЗІ (технічних засобів, основним функціональним призначенням яких є захист інформації від загроз витоку, порушення цілісності та блокування; технічних засобів, в яких додатково до основного призначення передбачено функції захисту інформації; засобів, які призначені, спеціально розроблені або пристосовані для пошуку закладних пристроїв і які створюють загрозу для інформації; засобів, які спеціально розроблені або пристосовані для оцінювання захищеності інформації), відповідність яких вимогам нормативних документів з питань ТЗІ засвідчено сертифікатом відповідності або позитивним експертним висновком, одержаними у порядку, який встановлено нормативно-правовими актами: Правилами проведення робіт із сертифікації засобів захисту інформації, затвердженими спільним наказом Адміністрації Держспецзв'язку та Держспоживстандарту України від 25.04.2007 р. № 75/91 і зареєстрованими в Міністерстві юстиції України 14.05.2007 р. за № 498/13765, та Положенням про державну експертизу в сфері технічного захисту інформації, затвердженим наказом Адміністрації Держспецзв'язку України від 16.05.2007 р. № 93 і зареєстрованим в Міністерстві юстиції України 16.07.2007 р. за № 820/14087.

Використання засобів цього Переліку під час створення, модернізації та впровадження комплексів ТЗІ не звільняє від необхідності оцінювання відповідності досягнутого рівня захисту інформації встановленому вимогами нормативних документів з ТЗІ, яке здійснюється шляхом атестації комплексів ТЗІ на ОІД або експертизи КСЗІ в АС.

Відповідно до ДСТУ 3396.2-97 (Захист інформації. Технічний захист інформації. Терміни та визначення): «Технічний захист інформації (ТЗІ) - діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами».

Відповідно до вимог зазначеного Держстандарту, для визначення повноти та якості робіт з ТЗІ слід провести атестацію. Атестація виконується організаціями, які мають ліцензії на право діяльності в галузі ТЗІ.

Атестація системи технічного захисту інформації – атестаційні (первинні, періодичні) випробування захищеності інформації на об'єкті від технічних розвідок та спеціальних впливів на відповідність вимогам нормативних документів з технічного захисту інформації. Об`єктами атестації є система забезпечення інформаційної діяльності та її окремі елементи, де циркулює інформація, що підлягає технічному захисту. У ході атестації потрібно:

- установити відповідність об`єкта, що атестується, вимогам ТЗІ;

- оцінити якість та надійність заходів захисту інформації;

- оцінити повноту та достатність технічної документації для об`єкта атестації;

- визначити необхідність внесення змін і доповнень до організаційно-розпорядчих документів тощо.

Порядок атестації встановлюється нормативними документами системи НД ТЗІ 2.1-002-07. Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення НД ТЗІ 2.1-002-07.

Зазначимо окремі правила та заходи, яких доцільно дотримуватись при організації ЗІ на підприємстві з метою уникнення витоку інформації технічними каналами.

Захист інформації від витоку акустичним, віброакустичним та оптоелектронним каналами.

Усі заходи захисту інформації від витоку акустичним, віброакустичним та оптоелектронним каналами зводяться до зниження рівня акустичних/віброакустичних сигналів (озвучення інформації) до певного співвідношення сигнал/завада. Ступень захисту інформації визначається відповідними нормами.

Необхідного співвідношення сигнал/завада можна досягнути пасивними або активними заходами.

Пасивні заходи захисту інформації спрямовані на підвищення звукоізоляції огороджувальних конструкції (далі – ОК) ОІД (встановлення металопластикових вікон, ущільнювачів дверей, створення «плаваючої підлоги», встановлення акустичних фільтрів у повітроводи тощо).

Активні заходи захисту інформації спрямовані зниження співвідношення сигнал/завада до норми шляхом створення акустичної/віброакустичної завади на межі огороджувальних конструкцій ОІД.

Захист інформації від витоку через закладні пристрої.

Автономні пристрої, які конструктивно об'єднують мікрофони і передавачі, називають закладними пристроями (ЗП) перехоплення мовної інформації.

Перехоплена ЗП мовна інформація може передаватися по радіоканалу, мережі електроживлення, оптичному каналу, з'єднувальним лініям ДТЗС, стороннім провідникам, інженерним комунікаціям в ультразвуковом діапазоні частот, телефонної лінії з викликом від зовнішнього телефонного абонента.

Прийом інформації, що передається ЗП, здійснюється, як правило, на спеціальні приймальні пристрої, які працюють у відповідному діапазоні довжин хвиль. Однак існують винятки з цього правила. Так, у випадку передачі інформації по телефонній лінії з викликом від зовнішнього абонента прийом можна здійснювати зі звичайного телефонного апарату.

Використання портативних диктофонів і ЗП, як правило, вимагає проникнення в контрольоване приміщення. Але, у деяких випадках проникати до приміщення не обов’язково, наприклад при застосування стетоскопів.

Використання ЗП вимагає проникнення до контрольованого приміщення (контрольовану зону). Коли це не вдається, для перехоплення мовної інформації використовуються спрямовані мікрофони.

Виявлення ЗП являє собою специфічний вид робіт тому він виділяється в окрему категорію робіт з технічного захисту інформації.

Вимоги, спрямовані запобіганню витоку ІзОД каналом паразитних електромагнітних випромінювань і наведень:

1. Телекомунікаційні мережі та мережі електроживлення прокладати в металевих рукавах з обов'язковим заземленням.

2. Транзитні трубопроводи, повітроводи та інші металеві елементи інженерних комунікацій не повинні проходити через ОІД, але якщо цього не уникнути, то вони обладнуються вставками з ізоляційного матеріалу.

3. Виключити транзитне проходження будь-яких кабелів (комп'ютерної мережі, сигналізації, голосового оповіщення, силових мереж тощо) через ОІД, а також спільний пробіг в одному каналі кабельних ліній різного призначення (силові та сигнальні). Відстань між ними повинна складати не менше 0,8 м.

Вимоги, спрямовані на забезпечення протипожежної безпеки на ОІД:

1. Опорядження стін, матеріали підвісних стель, розсіювачі світильників повинні бути із негорючих матеріалів.

2. Як засоби шумопоглинання повинні застосовуватися негорючі (НГ) або низької горючості (Г1) спеціальні перфоровані плити, панелі, мінеральна вата з максимальним коефіцієнтом звукопоглинання у межах частот 31,5 - 8000 Гц або інші матеріали аналогічного призначення, дозволені для оздоблення приміщень органами державного санітарно-епідеміологічного нагляду.

3. Об'єкт оснащується автоматичною пожежною сигналізацією. Тип та вид пожежної сигналізації має відповідати встановленим вимогам і мати відповідний сертифікат.

Підготовчі роботи для обладнання ОІД технічними системами захисту інформації для подальшого створення комплексів ТЗІ (такі роботи виконуються ліцензіатами у галузі технічного захисту інформації, які у подальшому зможуть обладнати об'єкт засобами захисту та атестувати його.

Вимоги, спрямовані запобіганню несанкціонованого доступу до об'єкту або до окремих його елементів:

1. Вхідні двері зали для проведення секретних нарад з коридору обладнуються надійним замком, а також пристроєм, що сигналізує про доступ

до об'єкту (чашка для опечатування, лічильник відкривання дверей, петлі для опломбування або використання плашок для опечатування тощо).

2. Кришки оглядових люків, інші елементи доступу до ніш, шахт тощо, в яких прокладені комунікації, обладнуються засобами замикання та пристроями для опломбовування.

3. Об’єкт оснащується охоронною сигналізацією, яка повинна бути виведена на пульт централізованого спостереження підрозділу охорони. Для живлення охоронної сигналізації в аварійних випадках має передбачатися автономне джерело живлення. Переключення на автономне джерело живлення має бути автоматичним.

Типи та види охоронної сигналізації повинні відповідати встановленим вимогам і мати відповідний сертифікат.

Захист від НСД може бути здійснений у різних складових інформаційної системи:

- прикладне й системне ПЗ:

- системи розмежування доступу до інформації;

- системи ідентифікації та автентифікації;

- системи аудиту й моніторингу;

- системи антивірусного захисту.

- апаратна частина серверів та робочих станцій:

- апаратні ключі;

- системи сигналізації;

- засоби блокування пристроїв та інтерфейсів вводу-виводу інформації.

- комунікаційне обладнання і канали зв'язку:

- міжмережеві екрани (Firewall) - для блокування атак із зовнішнього середовища:

1) Cisco PIX Firewall;

2) Symantec Enterprise FirewallTM;

3) Contivity Secure Gateway та Alteon Switched Firewall від компанії Nortel Networks. Вони керують проходженням мережевого трафіка відповідно

до правил (policies) захисту. Міжмережеві екрани зазвичай установлюють на вході мережі і поділяють на внутрішні (приватні) й зовнішні (загального доступу);

- системи виявлення вторгнень (IDS - Intrusion Detection System) - для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу "відмова в обслуговуванні" (Cisco Secure IDS, Intruder Alert та NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим впливам, що дає змогу значно зменшити час простою внаслідок атаки і витрати на підтримку працездатності мережі;

- засоби створення віртуальних приватних мереж (VPN -Virtual Private Network) - для організації захищених каналів передавання даних через незахищене середовище: Symantec Enterprise VPN; Cisco IOS VPN; Cisco VPN concentrator. Ці віртуальні приватні мережі забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування;

- засоби аналізу захищеності - для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації: Symantec Enterprise Security Manager; Symantec NetRecon. їх застосування дає змогу уникнути можливих атак на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

Для оцінювання стану технічного захисту інформації, що опрацьовується або циркулює в автоматизованих системах, комп'ютерних мережах, системах зв'язку, та підготовки обґрунтованих висновків для прийняття відповідних рішень проводять експертизу у сфері технічного захисту інформації [16; с.137].

Для кращого розуміння специфіки технічного захисту необхідно проаналізувати окремі стандарти діяльності в цій сфері, а саме:

- *Концепція технічного захисту інформації в Україні*. Затверджено Постановою Кабінету Міністрів України від 08.10.97 р. № 1126. Визначає

основи державної політики в галузі технічного захисту інформації інженерно технічними засобами, встановлює єдність принципів формування та проведення такої політики в усіх сферах життєдіяльності людини, суспільства та держави і соціальної, політичної, економічної, військової, екологічної, науково-технічної, інформаційної тощо.

- *Положення про технічний захист інформації в Україні.* Затверджено Указом Президента України від 27.09.99 р.№ 1229. Визначає правові та організаційні принципи технічного захисту важливої для держави, суспільства та особи інформації, охорона якої забезпечується державою відповідно до чинного законодавства.

- *Положення про контроль за функціонуванням системи технічної інформації.* Затверджено наказом ДСТСЗІ СБ України від 22.12.99 р.№ 61. Зареєстровано в Міністерстві юстиції України11.01.2000 р. за № 10/4231. Визначає правові та організаційні методи контролю за функціонуванням системи технічного захисту інформації, що регламентуються Положенням про технічний захист інформації в Україні. Поширюється на всі суб'єкти системи технічного захисту інформації.

- *Положення про державну експертизу в сфері технічного захисту інформації.* Затверджено наказом ДСТСЗІ СБ України від 29.12.99 р.№ 62. Зареєстровано в Міністерстві юстиції України 24.01.2000 р. за № 40/4261. Визначає суб'єктів та об'єкти державної експертизи в сфері технічного захисту інформації, їх права та обов'язки. Експертиза проводиться з метою оцінки захищеності інформації, яка обробляється або циркулює в автоматизованих системах, комп'ютерних мережах, мережах зв'язку, приміщеннях, інженерно технічних спорудах тощо. Дія цього Положення поширюється на всіх юридичних та фізичних осіб, які належать до числа суб'єктів експертизи.

- *Захист інформації. Технічний захист інформації. Основні положення.* Затверджено наказом Держстандарту України від 11.10.96 р. № 423. Чинний від 01.01.97 р. Встановлює об'єкт, мету, основні організаційно-технічні положення щодо забезпечення технічно го захисту інформації. Поширюється на підприємства, організації та установи усіх форм власності, органи державної влади усіх рівнів, які володіють, використовують та розпоряджаються інформацією з обмеженим доступом.

- *Захист інформації. Технічний захист інформації. Порядок проведення робіт.* Затверджено наказом Держстандарту України від 19.12.96 р. № 511. Чинний від 01.07.97 р. Встановлює вимоги до порядку проведення робіт з технічного захисту інформації. Поширюється на підприємства, організації та установи усіх форм власності, органи державної влади усіх рівнів, які володіють, використовують та розпоряджаються інформацією з обмеженим доступом.

- *Захист інформації. Технічний захист інформації. Терміни та визначення.* Затверджено наказам Держстандарту України від 11.04.97 р. № 200. Чинний від 01.01.98 р. Встановлює терміни та визначення понять у сфері технічного захисту інформації. Поширюється на підприємства, організації та установи усіх форм власності, органи державної влади усіх рівнів, які володіють, використовують та розпоряджаються інформацією з обмеженим доступом. У стандарті наведено абетковий покажчик українською, російською та англійською мовами.

- *Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.* Затверджені наказом Держкоммістобудування України від 02.09.96 р. № 3156. Чинні від 01.01.97 р. Встановлюють вимоги до забезпечення технічного захисту інформації під час організації проектування, будівництва підприємств, будівель та споруд. Призначені для суб'єктів інвестиційної діяльності України та її представництв за кордоном під час виконання проектних та будівельних робіт з урахуванням вимог технічного захисту інформації з обмеженим доступом.

- *Технічний захист інформації на програмно керованих АТС загального користування. Основні положення.* Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р.№ 26. Чинний від 01.07.1999 р. Встановлює об'єкт, мету та основні організаційно-технічні положення технічного захисту інформації на АТС, що призначені для функціонування у проводових телефонних мережах загального користування. Призначено для замовників, розробників, виготовлювачів, постачальників та експлуатаційників АТС і систем захисту інформації в них.

- *Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.* Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22. Чинний від 01.07.1999 р. Визначає методологічні основи (концепцію) розв'язання завдань захисту інформації в

комп'ютерних системах та створення нормативних і методологічних документів, що регламентують питання:

- визначення вимог щодо захисту комп'ютерних мереж від несанкціонованого доступу;
- створення захищених комп'ютерних систем і засобів їх за хисту від несанкціонованого доступу;
- оцінки захищеності комп'ютерних систем та їх придатності для вирішення завдань користувача.

Призначений для замовників, розробників, виготовлювачів, постачальників та експлуатаційників АТС і систем захисту інформації в них.

- *Типове положення про службу захисту інформації в автоматизованій системі.* Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 р.№ 53. Чинний від 15.12.2000 р. Встановлює вимоги до структури та змісту нормативного документа, що регламентує діяльність служби захисту інформації в автоматизованій системі(АС). Призначено для суб'єктів відносин, діяльність яких пов'язана з обробкою в АС інформації, що підлягає захисту згідно з нормативно-правовими актами, а також для розробників комплексних систем захисту інформації в АС. Встановлює єдиний підхід до визначення і формування завдань, функцій, структури, повноважень служби захисту інформації, а також організації робіт з захисту інформації впродовж усього життєвого циклу АС в установах усіх форм власності.

- *Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.* Затверджено наказом ДСТСЗІ СБ України від 09.02.01 р. № 2. Чинний від 20.02.01 р. Встановлює загальні вимоги до організації атестації комплексів щодо повноти та якості робіт з ТЗІ. Призначений для державних органів, органів місцевого самоврядування, органів управління Збройних Сил України, інших військових формувань, підприємств, організацій, установ, діяльність яких пов'язана з інформацією, необхідність охорони якої визначено законодавством України, а також виконавців робіт з ТЗІ.

- *Радіовиявлювачі вимірювальні. Методи та засоби випробувань.* Затверджено наказом ДСТСЗІ СБ України від 27.02.01 р. № 5. Чинний від 01.03.01 р. Поширюється на радіовиявлювачі вимірювальні і встановлює єдині умови та методи їх випробувань на відповідність вимогам

призначення. Вимоги НД є обов'язковими для юридичних та фізичних осіб, які здійснюють свою діяльність згідно з чинним законодавством в галузі ТЗІ.

- *Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань.* Затверджено наказом ДСТСЗІ СБ України від 06.04.01 р. № 11. Чинний з 10.04.01 р. Визначає методи випробувань засобів технічного захисту мовної інформації з обмеженим доступом (ЗТЗІ) від її відтоку через кінцеве обладнання симетричної ланцюгової абонентської телефонної лінії. Обов'язковий для замовників, розробників, виготовлювачів, постачальників ЗТЗІ та для випробувальних лабораторій (центрів), що здійснюють оцінку їх якості.

- *НД ТЗІ 2.3–003–2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів.* Методика випробувань. Затверджено наказам ДСТСЗІ СБ України від 06.04.01 р.№ 11. Чинний з 10.04.01 р. Визначає методи випробувань засобів технічного захисту мовної інформації з обмеженим доступом (ЗТЗІ) від її відтоку через кінцеве обладнання симетричної аналогової абонентської телефонної лінії. Методика охоплює проведення випробувань тільки тих параметрів ЗТЗІ, що стосуються захисту інформації. Обов'язковий для замовників, розробників, виготовлювачів, постачальників ЗТЗІ та для випробувальних лабораторій (центрів), що здійснюють оцінку їх якості.

- *Технічний захист інформації на програмно керованих АТС загального користування. Специфікації гарантій захисту.* Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р.№ 26. Чинний від 01.07.99 р. Встановлює вимоги до гарантій захисту інформації, що циркулює в програмно керованих АТС загального користування. Призначений для замовників, розробників, виготовлювачів, постачальників та експлуатаційників АТС і систем захисту інформації в них. Технічний захист інформації на програмно керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації її захисту. Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.Чинний від 01.07.99 р. Встановлює вимоги до довірчих оцінок коректності реалізації захисту інформації, що циркулює в програмно керованих АТС

загального користування. Призначений для замовників, розробників, виготовлювачів, постачальників та експлуатаційників АТС і систем захисту інформації в них.

- *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу*. Затверджено наказам ДСТСЗІ СБ України від 28.04.99 р.№ 22. Чинний від 01.07.99 р. Встановлює критерії оцінки захищеності інформації, що оброблюється в комп'ютерних системах, від несанкціонованого доступу. Містить специфікації функціональних критеріїв (послуг безпеки) та специфікації критеріїв гарантій коректності реалізації послуг. Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно орієнтовані системи та ін. Призначені для замовників, розробників, виготовлювачів, постачальників та експлуатаційників АТС і систем захисту інформації в них.

- *Методичні вказівки з використання засобів копіювально-розмножувальної техніки.* Затверджено наказом ДСТСЗІ СБ України від 26.07.99 р.№ 34. Чинний від 01.08.99 р. Містить вимоги до захисту та рекомендації щодо використання копіювально-розмножувальних апаратів та інших засобів копіювально-розмножувальної техніки (КРТ) з метою запобігання відтоку інформації з обмеженим доступом каналами побічних електромагнітних випромінювань і наведень. Призначений для підприємств, організацій, що використовують засоби КРТ для обробки інформації, яка підлягає технічному захисту.

- *Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.* Затверджено наказом ДСТСЗІ СБ України від 20.12.2000 р.№ 60. Чинний з 25.12.2000 р. Містить умови для запровадження єдиної системи вимог щодо створення, впровадження, супроводження та модернізації засобів ТЗІ від несанкціонованого доступу (НСД) в комп'ютерних системах установ, організацій і підприємств, а також взаємовідносин суб'єктів ТЗІ з Департаментом. Обов'язковий для виконання всіма суб'єктами системи ТЗІ. Призначено для розробників, виробників (випробувальних організацій), споживачів засобів ТЗІ, де обробляється інформація, захист якої забезпечується державою, а також органів, що здійснюють функції оцінювання засобів ТЗІ.

- *Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.* Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р.№ 22. Чинний від 01.07.99 р. Встановлює вимоги до порядку розробки, складу та змісту технічного завдання на створення комплексної системи захисту інформації, що циркулює в автоматизованих системах. Призначений для замовників та розробників комплексних систем захисту інформації в автоматизованих системах. Розроблено додатково до діючих нормативних документів щодо створення об'єктів інформатики.

РОЗДІЛ 3. ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

3.1. Механізми стратегічного інформаційного протиборства

Економічна сфера здавна слугувала як полем зіткнення протилежних інтересів різних супротивників (ворогуючих держав, виробників-конкурентів), так і об'єктом підриву з їх боку. Форми і способи боротьби, які застосовувалися на цьому терені, були найрізноманітнішими - від промислового шпигунства і фальшування грошей до оголошення економічної блокади, як під час англо-французького протистояння в часи наполеонівських війн. З плином часу в арсеналі економічного протиборства з'являються нові, більш витончені методи підриву, якими є і методи психологічного впливу, тобто засоби інформаційної війни.

Зі вступом суспільства в еру капіталізму засоби з арсеналу інформаційних війн дедалі активніше починають застосовуватися в економічному протиборстві конкуруючих фірм, корпорацій та держав. З одного боку, це обумовлювалось зростанням у суспільному житті ролі виробничої сфери, де загострюється конкуренція між підприємцями, які часто не гребують і жорсткими методами для усунення небажаних конкурентів. З іншого - появою у сфері міждержавного суперництва нових форм і способів підриву потенціалу держави-супротивника, шляхом розхитування, руйнування її економіки [28; с.221].

Гострота взаємовідносин суб’єктів підприємництва зумовлює їх до використання у своїй діяльності не лише інформаційних технологій т. з. мирного співіснування, а і технологій інформаційної конкуренції, інформаційного суперництва та інформаційного протиборства, аж до інформаційної війни. У зв’язку з такими можливостями інформації виникає необхідність звернути увагу на проблеми, які обумовлює інформаційний розвиток та сучасний стан інформатизації суспільства. Проблемний характер інформаційного розвитку проявляється насамперед у формуванні через нього

різного роду досить суттєвих небезпек і загроз. Тут слід говорити не лише про створення інформаційних технологій впливу та комп'ютерних програм для проникнення і руйнування електронної інформації, а і про специфічне використання інформаційних продуктів та специфічну поведінку в інформаційному просторі. Принципи ринкової ідеології згідно з якими в конкуренції перемагає сильніший, зумовили конкуренцію інформаційних можливостей окремих суб'єктів для забезпечення монополізації інформаційної сфери. Поєднання ж вказаних можливостей з можливостями фінансовими формує підґрунтя для економічного зростання певних суб'єктів. Тому заволодіння найбільш впливовими інформаційними каналами та суб'єктами інформаційної інфраструктури є одним із головних завдань у інформаційних відносинах на будь-якому ринку. Саме інформаційні і фінансові можливості роблять сильнішими суб'єктів ринку. У погоні за посиленням таких можливостей у інформаційних відносинах активно використовується дискредитація, дезінформація, компрометація, промислове шпигунство, різного роду ідеологічні та інформаційні диверсії [25; с.142].

На сьогодні не існує чіткого та однозначного виокремлення поняття та змісту інформаційного протиборства в сфері інформаційних відносин суб'єктів підприємницької діяльності. Останні роки, з об'єктивних причин, все більше зустрічаються наукові дослідження, що стосуються інформаційної безпеки держави, суспільства та міжнародних відносин. Разом з тим, аналіз наукової літератури дозволяє констатувати, що механізми, способи і методи впливу в усіх сферах інформаційних відносин фактично тотожні. То ж, для ідентифікації інформаційного протиборства в сфері інформаційних відносин суб'єктів підприємницької діяльності необхідно визначитись із суб'єктами та об'єктами захисту(впливу).

З визначенням Ліпкан В.А, інформаційне протиборство – суперництво соціальних систем (країн, блоків країн) в інформаційній сфері з приводу впливу на ті або інші сфери соціальних відносин і встановлення контролю над

джерелами стратегічних ресурсів, у результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку.

За інтенсивністю, масштабами та засобами, які використовуються, виділяють наступні ступені інформаційного протиборства: інформаційна експансія, інформаційна агресія та інформаційна війна.

Інформаційна експансія – діяльність із досягнення інтересів методом безконфліктного проникнення в інформаційну сферу.

Інформаційна агресія – незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення супротивнику конкретної, відчутної шкоди в окремих областях його діяльності шляхом обмеженого та локального по своїх масштабах застосування сили.

Інформаційна війна найвищий ступінь інформаційного протиборства, шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї) [44; с.184].

За типом прийнято розділяти на:

– інформаційно-технічне протиборство;

– інформаційно-психологічне протиборство.

Ознаки інформаційного, що характеризують його за типом протиборств; метою; характером впливу; джерелом розповсюдження та цільовою аудиторією зображено на рис 3.1

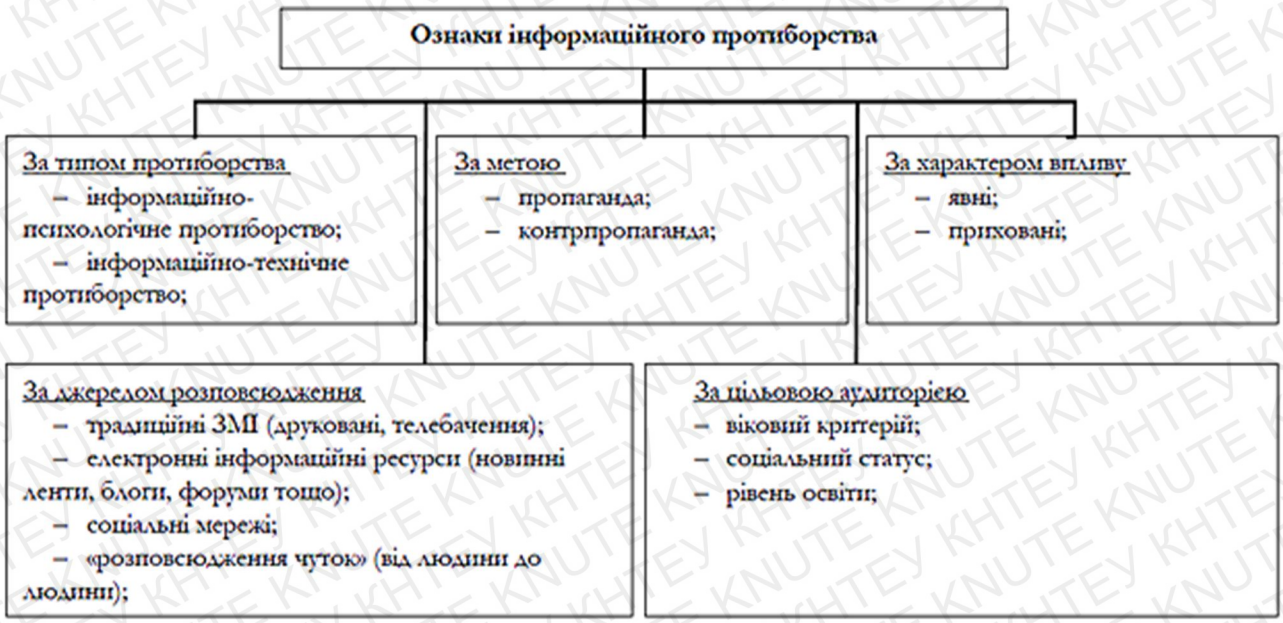

Рис. 3.1. Ознаки інформаційного протиборства

Таким чином, у інформаційних взаємовідносинах суб'єктів підприємництва можуть виникати: загрози, пов'язані з посяганням на їх інформаційні ресурси (переважно ту частину, яка має обмежений доступ) та загрози, що виникають під час формування середовища, умов діяльності таких суб'єктів.

Як свідчить досвід, основними способами реалізації таких загроз є:

- *маніпулювання інформацією* (дезінформація, викривлення інформації, подання в інформаційне середовище неповної або неправдивої інформації);

- *порушення встановленого порядку інформаційного обміну, несанкціонований доступ або необґрунтоване обмеження доступу* до інформаційних ресурсів, протиправне збирання і використання інформації;

- *руйнування та використання з протиправною метою чужих інформаційних ресурсів*;

- *інформаційний тероризм* (поширення комп'ютерних «вірусів», установлення програмних та апаратних закладних пристроїв, упровадження радіоелектронних приладів перехвату інформації, незаконне використання чи порушення роботи інформаційних і телекомунікаційних систем, нав'язування фальшивої інформації, оприлюднення компрометуючої інформації та ін.).

Найбільш поширеними загрозами інформації суб'єктів підприємництва можна вважати: розголошення таємної та конфіденційної інформації, її викрадення, модифікацію чи знищення, незаконне використання інформації, особливо тієї її частини, що становить інтелектуальну власність суб'єктів підприємництва і обумовлює переваги на ринку, несанкціонований доступ до інформації, що охороняється суб'єктом.

Розголошення інформації розуміється як протиправні умисні чи необережні дії посадових або інших осіб, які призвели до несанкціонованого, без службової необхідності, оголошення (поширення) відомостей щодо яких встановлено відповідний порядок їх розкриття. Воно може здійснюватись

шляхом повідомлення, передачі, пересилання, публікації, втрати чи іншим шляхом оприлюднення зазначених відомостей.

Викраденням інформації є таємне вилучення носіїв інформації (документів, електронних носіїв, відео- та аудиозаписів) з метою подальшого їх використання іншою особою чи передачі їх такій особі.

Знищенням є приведення носіїв інформації (документів, електронних носіїв, аудіо-, відеозаписів та інших носіїв, що мають матеріальний характер) в стан непридатний для їх подальшого використання або ж неможливості використання інформації, яка на них зберігалась.

Модифікацією інформації є внесення змін до змісту інформації, яка містилась на певних носіях або ж до самих носіїв (комп'ютерних програм) в результаті чого використання даної інформації стає неможливим взагалі чи така інформація вимагає суттєвого уточнення та аналізу.

Незаконне використання інформації означає використання певних даних, знань, технологій, які на праві власності належать певній юридичній чи фізичній особі без її згоди або з порушенням встановленого порядку їх використання особами, яким така інформація відома у зв'язку з їх службовою чи іншою діяльністю.

Несанкціонованим буде також доступ до інформації з порушенням встановлених правил доступу до неї [25; с.167].

Інформаційно-технічний вплив здійснюється переважно з метою порушення нормальних режимів роботи об'єктів та суб'єктів інформаційного протиборства та виведення з ладу їх комунікаційних систем, електронних інформаційних ресурсів та баз даних. З цією метою додатково для здійснення впливу на електронні інформаційні ресурси та бази даних використовуються програмні засоби деструктивного впливу (комп'ютерні віруси, троянські програми, «логічні бомби» тощо). Крім того ефективним та найбільш поширеним способом блокування таких ресурсів є здійснення кібератак класу DoS на відмову в обслуговуванні. Для порушення нормальної роботи

телекомунікаційних систем, як правило, використовуються різноманітні засоби створення електромагнітних перешкод.

Враховуючи відносну новизну протидії заходам маніпуляції та інформаційно-психологічного впливу в діяльності суб'єктів підприємництва можна бачити, що підрозділи безпеки останніх є досить обмеженими і діють не завжди адекватно тим загрозам, які утворюються від такої ситуації в інформаційному просторі. У даному випадку мова іде саме про ситуації коли технології інформаційно-психологічного впливу створюють передумови для збитків та втрат суб'єктів підприємництва. Розглядаючи питання протидії інформаційно-психологічну впливу слід звернути увагу на те, що він є одним із інструментів інформаційного протиборства або вищої його стадії інформаційної війни суб'єктів ринку. У даному випадку заходи інформаційно-психологічного впливу застосовуються з метою нанесення шкоди суб'єкту щодо якого вони застосовуються. Захист суб'єктів підприємництва від інформаційно-психологічного впливу, як правило, здійснюється шляхом мінімізації ризику отримання негативного результату від нього. Водночас, як показує досвід, тільки заходами мінімізації вказаного ризику суттєвої зміни ситуації не досягається. Тут необхідно значним чином активізувати саме протидію інформаційно-психологічному впливу.

Важливим моментом у цьому випадку є вибір об'єкту протидії. Насамперед, необхідно захистити власний персонал, в першу чергу шляхом впровадження в роботу з ним заходів, спрямованих на руйнування тих інформаційно-психологічних конструкцій, які з'являються у персоналу під чужим впливом. Разом з тим, об'єктом тут мають виступати інформаційне середовище, через яке поширюються заходи інформаційно-психологічного впливу та сам суб'єкт, який є зацікавленою стороною в поширенні такого впливу, а також суб'єкти через які поширюється такий вплив. Тобто, протидія має проводитись не з метою захисту [25; с.179].

Основна мета протидії інформаційно-психологічному впливу – припинення його проведення. Важливим тут буде зрив та нейтралізація заходів

інформаційно-психологічного впливу, що проводяться проти певних суб'єктів підприємництва.

Аналізуючи механізми інформаційного протиборства можна бачити, що моделі інформаційно-психологічного впливу практично однакові в різних сферах людської життєдіяльності. Використовуються лише різні їх модифікації.

Враховуючи, що в центрі інформаційного протиборства чи інформаційної війни знаходиться людина інформаційно-психологічний вплив спрямовується на найбільш вразливі сфери її психіки. Такими сферами є:

- мотиваційна (ціннісні орієнтири, переконання);
- сфера потреб та інтересів, бажань, потягів;
- інтелектуально-пізнавальна (знання, пам'ять, мислення);
- емоційно-вольова (емоції, почуття, настрої, вольові процеси);
- комунікативна (характер і особливості спілкування, взаємини з людьми, між особисті сприйняття);
- функціональна (виконання службових і посадових обов'язків, дисциплінованість) [44; с.181].

Якраз з врахуванням зазначених сфер, завдань та умов і формуються моделі впливу. Крім того, особливостями моделей впливу у інформаційно-психологічній протидії є те, що вони практично завжди виступають руйнівними і спрямовуються на дискредитацію конкретного об'єкта протидії і заходів впливу, що ним проводяться. Хоча в окремих випадках вплив у протидії може носити і стимулюючий характер.

У разі, коли об'єктом протидії впливу обирається інформаційне середовище, суб'єкти підприємництва готують і проводять за відповідними технологіями (моделями) заходи контрпропаганди, спрямовані на руйнування ефекту, якого очікують особи, що ведуть проти зазначених суб'єктів інформаційну війну. З метою посилення протидії інформаційно-психологічному впливу в інформаційному середовищі можуть формуватись групи підтримки, однодумців, громадські об'єднання з клієнтів, акціонерів, інших осіб за допомогою яких здійснюється поширення сформованих

суб'єктами підприємництва моделей протидії в інформаційному середовищі. В окремих випадках можуть проводиться певні акції: мітинги, демонстрації, пікети, громадські вимоги в підтримку вказаних суб'єктів. За таких умов буде здійснюватись не тільки гуртування громадян навколо суб'єктів, а і відповідна трансформація колективної свідомості. Доповненням до цього може бути поширення позитивних для суб'єктів та руйнівних для технологій інформаційно-психологічного впливу чуток та міфів.

Коли ж об'єктом протидії обирається особа, якою ініціюється чи проводиться інформаційно-психологічний вплив, то тут можуть передбачатись інші заходи та формуватись для них відповідні моделі протидії, зокрема:

- виявлення особи, якою ініціюється проведення інформаційно-психологічного впливу на певний суб'єкт підприємництва та осіб через яких здійснюється такий вплив;
- розкриття негативного змісту діяльності зазначених осіб у засобах масової інформації та іншим шляхом в інформаційному середовищі суб'єкта підприємництва;
- звернення до органів влади, правоохоронних органів, Антимонопольного комітету, суду, громадськості з вимогами щодо припинення проведення щодо суб'єкта негативного інформаційно-психологічного впливу;
- залучення до протидії інших суб'єктів (партнерів, клієнтів, акціонерів) та вжиття спільних заходів щодо протидії інформаційно-психологічному впливу;
- формування компрометуючих інформаційних моделей протидії та поширення їх в інформаційному середовищі щодо осіб, якими проводяться дії інформаційно-психологічного впливу на суб'єктів підприємництва [25; с.185].

Серед ризиків інформаційного впливу особливу небезпеку становить ризик потрапляння суб'єктів підприємництва під дію інформаційного тероризму, що є нині доволі ймовірним. Ураховуючи відчутні наслідки, до яких можуть призвести дії інформаційного тероризму, суб'єкти підприємництва не повинні ігнорувати такий вид ризиків і мають виробляти відповідну політику

щодо їх мінімізації. Насамперед має проводитися постійний аналіз та оцінювання умов формування таких ризиків. У процесі аналізу суб'єкти підприємництва повинні визначити, наскільки уразливі до атак інформаційного тероризму їх комунікаційні системи та мережі, особливо засоби, мережі та інформація, які обслуговують платіжну систему банків. Має визначатися ступінь доступності інформаційних систем і мереж для атак інформаційного тероризму. Крім того, вивчається діяльність суб'єктів з погляду її вразливості від інформаційних атак компрометуючими матеріалами, розраховується критична межа, за якої пропаганда та реклама суб'єктів будуть неефективними під впливом заходів інформаційного тероризму. Тобто, межа, за якою інформаційний вплив від актів тероризму призведе до руйнування іміджу суб'єктів підприємництва, їх взаємовідносин з іншими суб'єктами, породжуватиме конфліктні ситуації у виробничих колективах та ін.

Виходячи з результатів аналізу, визначається ступінь уразливості діяльності суб'єктів підприємництва, їх інформаційних мереж і систем щодо атак інформаційного тероризму. Далі робиться припущення про те, які саме ризики інформаційного тероризму найімовірніші для суб'єктів (ризик порушення роботи, руйнування інформаційних мереж і систем, вилучення електронної інформації, викрадення коштів та ін. чи ризики втрати іміджу від атак компрометуючими матеріалами) та можливі періоди чи обставини, за яких такі ризики будуть найімовірнішими.

У процесі оцінювання ризиків інформаційного тероризму визначається,

які наслідки можуть настати для суб'єктів підприємництва через інформаційні атаки терористів як з погляду економічного, так і з погляду їх іміджу. Тут можна формувати певні прогнози щодо таких наслідків (втрата клієнтів, звільнення провідних працівників з роботи, втрата інформації, що має обмежений доступ, викрадення коштів з рахунків суб'єктів та їх клієнтів, руйнування програмного забезпечення роботи інформаційної мережі та інформаційних систем). Стосовно конкретного виміру обсягу шкоди, завданої від актів інформаційного тероризму, то тут поки що відсутні якісь підходи.

Практично неможливо передбачити, а тим більше прорахувати обсяги можливої шкоди від таких дій. Тому під час оцінювання зазначених ризиків обмежуються можливими категоріями наслідків, які можуть наступати у зв'язку з інформаційними атаками терористів.

Під час контролю ризиків інформаційного тероризму виявляють ознаки підготовки терористичних актів, насамперед інформаційних атак. Крім того, вивчаються умови, за яких такі атаки можуть бути найбільш імовірними, та з'ясовуються причини, що впливають на формування таких умов. Якраз виявлення та контроль зазначених умов і причин і є основним предметом роботи з контролю ризиків інформаційного тероризму. Головне завдання контролю полягає в тому, щоб звузити велику різноманітність варіантів дій терористів і контролювати найбільш можливі та небезпечні.

Мінімізація ж зазначених ризиків здійснюється шляхом проведення заходів захисту технічного, програмного, криптографічного, апаратного, адміністративного, правового характеру власних інформаційних мереж і систем, а також заходів формування стійкого іміджу суб'єктів підприємництва на ринку, пропаганди їх послуг і реклами. Крім того, проводиться низка заходів щодо згуртування колективів працівників суб'єктів підприємництва, формування в них фірмового патріотизму. Важливою частиною заходів мінімізації ризиків інформаційного тероризму є заходи з формування довіри до суб'єктів підприємництва та його менеджменту з боку клієнтів, акціонерів, державних органів.

На мінімізацію ризиків інформаційного тероризму мають бути спрямовані заходи з виявлення та перетинання інформаційних каналів, через які можуть бути здійснені інформаційні атаки.

Водночас слід зазначити, що дії, пов'язані з інформаційним тероризмом, є для суб'єктів підприємництва не лише небезпечними, а й такими, від яких побудувати гарантовану систему захисту, яка б виключала можливість проведення актів інформаційного тероризму, дуже складно. Тому суб'єкти підприємництва мають передбачати заходи своєї поведінки в разі здійснення

таких актів, передусім спрямовані на забезпечення виживання в умовах інформаційних атак, а також заходи по ліквідації їх наслідків [25; с.187].

3.2. Міжнародні аспекти інформаційної безпеки в умовах глобалізації

За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір. Сучасні інформаційні технології дають змогу підприємствам реалізовувати власні інтереси, пришвидшують процеси обміну та співпраці. Проте неефективне використання інформації здатне послабити або завдати значної шкоди безпеці конкурентного підприємства, яке не має дієвої системи захисту від негативних інформаційних впливів. Від обсягу, швидкості та якості обробки інформації значною мірою залежить ефективність управлінських рішень, зростає значення методів управління з використанням інформаційних технологій соціальними та економічними процесами, фінансовими і товарними потоками, аналізу та прогнозування розвитку внутрішнього і зовнішніх ринків. Таким чином, інформаційна безпека є невід'ємною складовою ефективної діяльності підприємства.

Сьогодні всі економічно розвинуті країни широко використовують переваги нових інформаційних технологій у виробничій, комерційній та банківській сферах. Це пояснюється тим, що за допомогою традиційних методів неможливо зорієнтуватися в сучасному стрімкому інформаційному потоці й глибоко аналізувати динамічні процеси економічної діяльності підприємств. Найбільш швидко й ефективно розвиваються технології, пов’язані з глобальною комп’ютерною мережею Інтернет, що призвело до появи таких нових категорій, як електронна торгівля, електронний бізнес, електронний уряд тощо [93].

Комісія з питань національної безпеки визначила такі потенційні загрози в інформаційній сфері: відсутність у міжнародного співтовариства об’єктивного уявлення про Україну; інформаційна експансія з боку інших країн; відтік інформації, що містить державну таємницю, а також

конфіденційної інформації, що є власністю держави; повільне входження України до світового інформаційного ринку; незбалансованість державної політики та відсутність необхідної інфраструктури в інформаційній сфері [14; с.3].

Сьогодні в Україні поступово створюються умови для комфортного ведення електронного бізнесу – різко зростає кількість автоматичних телефонних станцій, довжина та якість ліній зв'язку, реально починає працювати програма інформатизації, активно формується нормативно-правова база. Законодавчо врегульовано загальні правові основи одержання, використання, поширення та зберігання інформації, закріплено право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначений статус учасників інформаційних відносин, доступ до інформації та її охорона. У правоохоронних органах створені спеціальні підрозділи боротьби з комп'ютерними злочинами [93].

Сучасну епоху називають ерою інформації або інформаційним суспільством, що характеризується домінуючою роллю інформації та знань, створенням глобального інформаційного простору, в якому завдяки високорозвинутим інформаційно-комунікативним мережам і технологіям забезпечуватиметься стале економічне та соціальне зростання, вільний доступ до світових інформаційних ресурсів, що дозволить людям у повній мірі використовувати свій потенціал та реалізовувати власні прагнення [41].

Процеси глобалізації торкаються дедалі нових сфер діяльності. Інформаційна також стає не тільки найважливішою сферою міжнародної співпраці, а й об'єктом суперництва.

У даний час в Україні значна частина баз даних, що містять конфіденційну інформацію, виконана із застосуванням мінімальних засобів захисту та розмежування доступу і не забезпечує необхідного рівня захисту інформації, адже бази даних – найважливіше джерело інформації. Ситуація збільшується доступністю і “дешевизною” засобів знімання інформації з комп'ютерного устаткування. Таким чином, завдання захисту баз даних набуває

великої актуальності. Потрібні значні фінансові та матеріальні витрати для забезпечення повномасштабного захисту і сертифікації вже наявних і баз даних, що розроблюються, засобів доступу до них і створення необхідного для цього науково-технічного потенціалу. Щоб забезпечити високий ступінь захисту інформації, необхідно, у першу чергу, вирішити такі завдання:

– розробити однакові вимоги, що регламентують безпеку роботи засобів зв'язку й іншої електронної техніки;

– забезпечити державні органи криптографічними матеріалами і відповідною документацією; розробити сервісні послуги при придбанні, монтажі і визначенні порядку використання систем забезпечення безпеки інформації і зв'язку;

– зібрати дані про теперішній стан справ по запобіганню витоку інформації і закриттю каналів зв'язку в державних структурах;

– докласти зусиль щодо допомоги вітчизняній промисловості в розробці систем зв'язку, що володіють високим ступенем захищеності.

Сучасний рівень розвитку демократизації та технічного прогресу зумовив значне розширення доступу до інформації. Насамперед, збільшилось коло осіб здатних отримати необхідну їм інформацію, знизився рівень закритості інформації, значно збільшилась кількість джерел інформації. Глобалізація суспільних та економічних відносин дає можливість отримувати інформацію практично з будь-якого сегменту інформаційного простору.

Однак, слід звернути увагу на загрози, пов’язані з глобалізацією інформаційних і телекомунікаційних технологій. У зв’язку з процесом міжнародної інтеграції та глобалізації обсяги та різноманітність загроз значно розширились. Підприємства, банки можуть зазнавати інформаційного удару щодо своїх інформаційних та фінансових ресурсів із глобального інформаційного простору. Серед найбільш поширених глобальних загроз – комп’ютерний тероризм і комп’ютерне хуліганство. Значне розповсюдження Інтернет-технологій і відносна анонімність користувачів спровокували появу так званих хакерів, крекерів, телефонних фанатиків – людей, які вважають

своїм обов'язком здійснити певні протиправні дії в мережі Інтернет як самовираження на глобальному рівні. Як правило, такі особи є добре обізнаними з комп'ютерними технологіями, є їх фанатами і тому можуть на досить професійному рівні проникати в комп'ютерні системи. Вони є катастрофічно небезпечні для комп'ютерних технологій суб'єктів підприємництва, особливо банків, оскільки не тільки руйнують системи їх захисту, а можуть отримати досить важливу інформацію. Поширене останнім часом комп'ютерне хуліганство зумовило появу фактів, пов'язаних з так званим електронним пограбуванням, насамперед банків. Останні щороку від протиправних дій різного роду хакерів, крекерів, комп'ютерних хуліганів зазнають мільярдні збитки та втрачають величезні обсяги інформації.[25; с.189].

Поняття загрози інформаційної безпеки зародилось майже у той же час, як і поява інформаційного середовища. Спочатку це були прояви крадіжки інформації з комп'ютера, незаконне використання, порча інформації на комп'ютерах. Пізніше з розвитком інформаційних мереж інформаційна небезпека перетворилась в засоби перекачування по мережі неправдивої інформації, вірусів. Зараз питання безпеки відноситься майже до всіх агентів глобального інформаційного середовища. Україна як активний учасник процесів циклу життя інформації не стоїть в стороні від них. Це відбувається як на загальному міжкраїновому рівні, так і в середині кожного окремого підприємства [11].

У сучасних умовах XXI ст. інформаційна безпека корпоративної економіки набуває все вагомішої ролі, а питання її забезпечення стають дедалі гострішими. Стрімке впровадження інформаційних технологій у всі сфери життєдіяльності суспільства та розвиток корпоративної економіки в умовах глобалізаційних процесів актуалізує проблему визначення обґрунтованих та ефективних шляхів забезпечення інформаційної безпеки.

Формування корпоративної економіки в умовах глобалізаційних процесів порушує широке коло проблемних питань, одним із яких є підвищення інформаційної безпеки.

В умовах глобалізаційних процесів корпоративну економіку, на наш погляд, слід розглядати як динаміку злиттів і поглинань, що являє собою трансформаційну стратегію економіки, спрямовану на підвищення її ефективності та конкурентоспроможності на світовому ринку.

Країни, які не можуть забезпечити власну інформаційну безпеку, стають неконкурентоспроможними і, як наслідок, не можуть брати участь у боротьбі за розподіл ринків і ресурсів. Можна стверджувати, що розпад великих держав відбувся не в останню чергу через неспроможність ефективного управління на власній території та невідповідність інформаційної структури новим умовам існування.

Таким чином, у зв'язку зі зростанням динаміки злиттів і поглинань компаній як складової частини стратегії зміни економіки України, спрямованої на підвищення її ефективності та конкурентоспроможності на світовому ринку, проблема інформаційної безпеки потребує постійної і прискіпливої уваги.

Узагальнюючи підходи до розуміння сутності інформаційної безпеки, слід наголосити, що в умовах глобалізаційних процесів інформаційну безпеку корпоративної економіки запропоновано визначати як інтегрований складник процесу забезпечення захисту інформації від внутрішніх і зовнішніх загроз і створення сприятливих умов для ефективного функціонування корпорацій і підвищення їх конкурентоспроможності.

Необхідність забезпечення безпеки активів корпорації зобов'язує їх займатися діяльністю, яка раніше була виключно прерогативою спеціальних державних органів. Забезпечення безпеки приватної діяльності стає важливою необхідністю, є основою функціонування недержавних об'єктів. Отже, охорона корпорацій і забезпечення інформаційної безпеки корпоративної діяльності – стрижнева проблема, що передбачає вживання низки організаційно-правових, техніко-технологічних, інформаційних, адміністративних, виховних,

фінансових і спеціальних заходів, спрямованих на виявлення, попередження і припинення загрози стабільності функціонування і розвитку корпорацій. Цей процес передбачає забезпечення безпеки інформації, охорону приватної власності корпорацій і фізичний захист її персоналу. Сюди варто віднести інтелектуальну власність, що містить інформацію, яка є актив компанії, а також знання і досвід співробітників корпорацій, їх професійні секрети і винаходи.

Корпорації, які прагнуть мати власну службу безпеки, не повинні розглядати витрати на її створення як необґрунтовано високі, оскільки життя та репутація цінуються набагато вище. Проблемою корпорацій є те, що отримання ними надприбутків не сприяє усвідомленню того факту, що багатство неминуче переводить їх у «групу ризику». Як показує сумний досвід, вітчизняні корпорації починають вживати суттєві заходи із забезпечення власної безпеки, безпеки інформації лише після виникнення проблем.

Виділимо важливі проблеми інформаційної безпеки корпоративної економіки. По-перше, до них слід віднести забезпечення захисту і контролю за інформаційним простором від несанкціонованого доступу до інформації, по-друге, удосконалення нормативно-правового поля інформаційної сфери; по-третє, залучення інвестицій для скорочення технічного відставання інформаційних технологій; по-четверте, використання новітнього програмного забезпечення та техніки.

Проведене дослідження засвідчило, що ефективне функціонування інформаційної безпеки корпоративної економіки в умовах глобалізаційних процесів необхідно розглядати як сукупність державної та недержавної системи захисту. Основні її компоненти: законодавча, економічна, програмно-технічна, адміністративно-управлінська.

Складниками єдиної системи забезпечення інформаційної безпеки корпорацій є:

– державна система, представлена правоохоронними органами та спецслужбами (наприклад, Служба безпеки України, Рада національної безпеки і оборони України);

– недержавна система, представлена приватними охоронними, охоронно-технічними підприємствами, комерційними службами безпеки, підприємствами різної форми власності, інформаційними бюро, службами безпеки банків, профільними факультетами, кафедрами вищих навчальних закладів.

До законодавчої компоненти слід віднести: розробку єдиної комплексної системоутворювальної нормативно-правової бази, яка регулювала б функціонування та сприяла стимулюванню розвитку інформаційної безпеки корпоративної економіки.

Адміністративно-управлінська компонента в першу чергу повинна відповідати за:

– створення органів на державному рівні та на рівні корпорації, що координують розвиток системи інформаційної безпеки;

– підвищення уваги керівництва до управління персоналом і фізичним захистом інформації;

– розробку та забезпечення концепції і програми розвитку інформаційної безпеки на всіх рівнях;

– активізацію міжнародного співробітництва у сфері інформаційної безпеки;

– гармонізацію навчання персоналу із відповідними світовими нормами й стандартами.

Для захисту та посилення інформаційної безпеки, на наш погляд, головною є програмно-технічна компонента, що відповідає за:

– розвиток вітчизняної індустрії інформації відповідно до сучасної геополітичної ситуації у світі;

– розробку програмних та апаратних засобів криптографічного захисту інформації, які б захищали інформаційні ресурси від несанкціонованого доступу для забезпечення конфіденційності;

– ліцензування та розробку критеріїв сертифікації технологій;

– інформатизацію та автоматизацію виробничих процесів і робочих місць співробітників.

Необхідний рівень інформаційної безпеки забезпечує сукупність політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення і нейтралізацію тих обставин, факторів і дій, які можуть завдати збитку або перешкодити реалізації інформаційних прав, потреб та інтересів країни і її громадян [61; с.92].

Характер розповсюдження інформаційних технологій, розвитку світового інформаційного простору та нових викликів, які виникають при цьому, вимагає впровадження інтернаціональних підходів до підтримки безпеки, як суто інформаційної, так і у інших її вимірах. З огляду на це, виникає потреба у формуванні міжнародної системи інформаційної безпеки (МСІБ), яка б дозволяла здійснювати ефективні заходи реагування на існуючі і потенціальні виклики, підтримувати нормальне функціонування загальносвітового інформаційного простору.

Слушно звернути увагу на основні елементи МСІБ, що формується, а саме:

1) міжнародні доктринальні документи універсального характеру, присвячені інформатизації, інформаційному суспільству та інформаційній безпеці;

2) міжнародні стандарти у галузі інформаційної безпеки;

3) міжнародні професійні (спеціалізовані) установи, які займаються питаннями інформаційної безпеки у різних галузях;

4) міжнародно-регіональні інститути та структури, які створюються інтеграційними об’єднаннями (на прикладі, ЄС);

5) інститути, що створюються військово-політичними організаціями (на прикладі НАТО);

6) національні доктрини, концепції та стратегії.

Головними міжнародними доктринальними документами є Окінавська Хартія глобального інформаційного суспільства (розвиток та ефективне функціонування електронної ідентифікації, електронного підпису, криптографії та інших засобів забезпечення безпеки та достовірності операцій); Резолюції

Генеральної Асамблеї «Досягнення у сфері інформатизації і комунікацій у контексті міжнародної безпеки» та «Створення глобальної культури кібербезпеки та оцінка національних зусиль щодо захисту найважливіших інформаційних інфраструктур», «Стратегія у галузі ІКТ», «Боротьба зі злочинним використанням інформаційних технологій» тощо. Основні ідеї цих документів виражають прагнення до більш безпечного, стабільного, відкритого глобального інформаційного простору. Також ці документи визначають головні напрями міжнародної політики у сфері безпеки, наприклад, боротьба з кіберзлочинністю, безпека використання мереж, розвиток інфраструктури тощо.

Бурхливий розвиток ІТ у 1990-х рр. зумовив необхідність розвитку стандартизації у сфері інформаційної безпеки. Основними міжнародними стандартами, що прийняті ISO, є: ISO/IEC 27002:2013 «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги» та ISO/IEC 27002:2013 «Інформаційні технології. Методи забезпечення безпеки. Кодекс практики управління інформаційною безпекою» та інші стандарти серії ISO/IEC27002, ISO/IEC27005:2011«Інформаційні технології. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки». Ці стандарти визначають вимоги щодо забезпечення інформаційної безпеки та напрями заходів (криптографія, експлуатаційні процедури, аудит, управління інцидентами тощо). Із розвитком мережі Інтернет також набула поширення група спеціальних стандартів, включно із: сімейством протоколів TCP/IP для передавання даних; Simple Mail Transport Protocol та Post Office Protocol для електронної пошти; Simple Network Management Protocol для управління мережами; Secure Socket Layer для шифрування даних; Security Electronics Transaction для електронних транзакцій, Public Key Infrastructure для управління ключами. Всі вони покликані забезпечити захист даних та інформації при виконанні різних операцій [101].

Таким чином, сучасна геополітика визначає інформаційну безпеку як один із головних напрямів соціально-економічного розвитку держави,

суспільства, бізнесу. Необхідним для забезпечення інформаційної безпеки корпоративної економіки є застосування на практиці комплексну заходів, що поєднує такі засоби впливу, як законодавчий, економічний; програмно-технічний; адміністративно-управлінський. Найскладнішими для реалізації є удосконалення нормативно-правової бази, пошук і виділення необхідних ресурсів для розвитку інформаційної безпеки, а також навчання персоналу відповідним світовим нормам і стандартам, кооперація фахівців із різних галузей [61; с.93].

Разом з тим, глобальність процесів інформаційної взаємодії між суб'єктами ІБ різних держав, трансграничність комп'ютерної злочинності роблять необхідним об'єднання зусиль різних держав у боротьбі з тими загрозами, з якими вони не в змозі впоратися самостійно.

Основні напрями об'єднання спільних зусиль – це узгоджених стратегій і державної політики в галузі забезпечення інформаційної безпеки, а також заходів і механізмів, пов'язаних з їхньою реалізацією; удосконалення й уніфікація нормативної правової бази забезпечення інформаційної безпеки держав, форми й способи реалізації правових норм; розширення взаємодії з міжнародними органами й організаціями при вирішенні науково-технічних і правових питань забезпечення безпеки інформації в міжнародних інформаційних і телекомунікаційних системах; розробка критеріїв і методів оцінки ефективності систем і засобів забезпечення інформаційної безпеки, уніфікацію сертифікації цих систем і засобів; розвиток національних систем підготовки кадрів в галузі інформаційної безпеки й інформаційних технологій і надання взаємодопомоги в цих питаннях; зміцнення взаємодії правоохоронних органів держав стосовно запобігання комп'ютерних (інформаційних) злочинів.

Поширення й використання інформаційних технологій і засобів зачіпає інтереси всього міжнародного співтовариства й тільки широке міжнародне співробітництво здатне забезпечити їхнє безпечне застосування в інтересах кожної держави. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки повинне будуватися на основі збігу національних

інтересів зацікавлених країн в інформаційній сфері, їхніх уявлень про загрози цим інтересам, методи й засоби протидії загрозам[15, с.102].

3.3. Захист інформації підприємства від промислового шпигунства

Конкурентна боротьба за ринки збуту продукції, сфери вкладення капіталів і прагнення до отримання максимальних прибутків змушують керівництво великих корпорацій уважно стежити за діяльності своїх конкурентів. Явище «шпигунство» таке ж давнє як і наша цивілізація. Економічна розвідка є невід'ємною частиною історичного розвитку продуктивних сил, оскільки, відповідно до еволюції, змінювала характер, форми, прояви та способи виробництва і цим сприяла розвитку науки і техніки.

Письменник Анрі Беке у своїй книзі «Боротьба за вогонь» описує один з найдавніших прикладів промислового шпигунства: герої книги - первісні люди – відправлялися до сусіднього племені щоб викрасти секрет добування вогню. Китайська хроніка 15 століття до нашої ери вміщає в собі розповідь про китайську принцесу. Вона в своєму капелюшку, який був прикрашений живими квітами, вивела з Китаю шовкопряди і передала їх своєму нареченому разом із секретом виготовлення шовку. Таким вчинком, китайська принцеса позбавила свою країну монополії в цій галузі.

Багато секретів викрадали у східних країнах, у арабів. Досить довго на португальських кораблях, що огинали Африку, знаходилися різні авантюристи, які купили або викрали у арабів таблиці тригонометричних функцій за допомогою яких вони визначали місцезнаходження корабля. Араби володіли і іншим секретом, за яким довгий час полювали всілякі шпигуни, - секретом запальних ракет, так званих «китайських стріл» (судячи з назви, араби свого часу самі викрали цей секрет у китайців).

З XIV по XVIII століття основним предметом промислового шпигунства були відкриття алхіміків. Наполегливе полювання велося за секретом геометричної закупорки судин (він, до речі, не розкритий і донині); секретом

виробництва золота, кислот для чищення алмазів і, нарешті, пороху (теж вкраденого у китайців).

Наступною віхою розвитку промислового шпигунства можна вважати прийняття у 1791 році у Франції закону про патенти. Це була далеко не перша законодавча міра, спрямована на захист винахідницьких прав. Але особливістю цього закону було те, що вперше заохочувалося промислове шпигунство за межами Франції. Цей закон закріплює «за всяким хто першим привезе у Францію якийсь іноземний промисел, такі ж пільги, якими б користувався його винахідник [98, с.12].

В кінці XVIII століття в Манчестері виникає перша приватна організація, що сприяє промисловому шпигунству, названа «Асоціацією по боротьбі з патентами і монополіями». Приблизно в той же час 1854 року група банкірів, промисловців і філантропів в створила «Спілку заохочення ремесла і торгівлі», яка видавала премії винахідникам які не запатентували свої винаходи. Ця спілка видали 14 тисяч фунтів Томасу Ломбу, щоб він не поновлював свій патент на обробку шовку; 30 тисяч фунтів Дженеру, щоб він не подарував вакцинацію; 5 тисяч фунтів в Самуєлю Кромттону, щоб він не патентував свою прядильну машину. В історії є ще безліч подібних випадків.

Приблизно з 1875 року – часу явної промислової переваги Англії – починається історія розвитку промислового шпигунства в США та в Японії. Наприклад, японцями був вкрадений спосіб шліфування лінз за допомогою їх обробки окисом цезію, завдяки чому їм вдалося наповнити світовий ринок високоякісними і порівняно дешевими фотоапаратами, а також спосіб приготування віскі. Американцям вже вдалося використати спосіб електролітичного виробництва алюмінію.

Друга світова війна стала справжнім Ельдорадо для промислових шпигунів всіх країн. Але тут, мабуть, самим дивним фактом можна вважати невдачу німецьких шпигунів в історію з атомною бомбою. Особливо видатним досягненням стала охорона проекту, організована американським генералом Гровсом. В інститутах, що займаються розробкою атомної бомби, щовечора

під наглядом автоматників спалював весь вміст кошиків зі сміттям; жінок, які переносили з будівлі в будівлю секретні документи, завжди супроводжував озброєний револьвером детектив з відомого агенства «Брінкс». Для дезінформації розпустилися всілякі чутки.

У розвинених країнах в даний час промислове шпигунство набуло значного поширення. Так, наприклад, в США з 1986 року легально існує «Товариство фахівців з добування відомостей про конкурентів» яке налічує близько півтори тисячі постійних членів.

Промислове або комерційне шпигунство досить поширене явище і є окремим видом недобросовісної конкуренції, що являє собою вчинення дій із протиправного добування відомостей, що становлять комерційну цінність для підприємства.

Стаття 16 Закону України «Про захист від недобросовісної конкуренції» визначає, що неправомірним збиранням комерційної інформації вважається збирання протиправним способом відомостей, які становлять відповідно до законодавства України комерційну таємницю, якщо це завдало чи могло завдати шкоди суб'єкту господарювання.

На сучасному етапі розвитку суспільства масштаби економічного шпигунства різко зростають. Інформація про результати чужих прикладних і фундаментальних досліджень дозволяє заощадити власні сили й кошти і зосередити всю увагу на виробництві та маркетингу. Подальший розвиток науково-технічного прогресу, збільшення потоку патентів і жорсткість конкуренції як «війни всіх проти всіх» роблять викрадення чужих таємниць особливо прибутковою, і тому дуже перспективною справою.

Промислове шпигунство щодо бізнесу – це різновид економічного шпигунства, якому властиве звуження масштабів завдань з одержання інформації, що цікавить, від державного – до масштабу однієї або декількох фірм-конкурентів. Отже, для бізнесу промислове шпигунство – лише спосіб конкурентної боротьби.

Промислове шпигунство, зазвичай, має дві мети:

• отримання інформації конкурентів, насамперед конфіденційної, про стратегічні й тактичні наміри їхнього бізнесу;

• здобуття конкурентної переваги на ринку, через витіснення або знищення конкурента.

Ознаки промислового шпигунства досить розгорнуто наведені в роботі Суярової О.О. та відображені на рис. 3.1[99, 25].

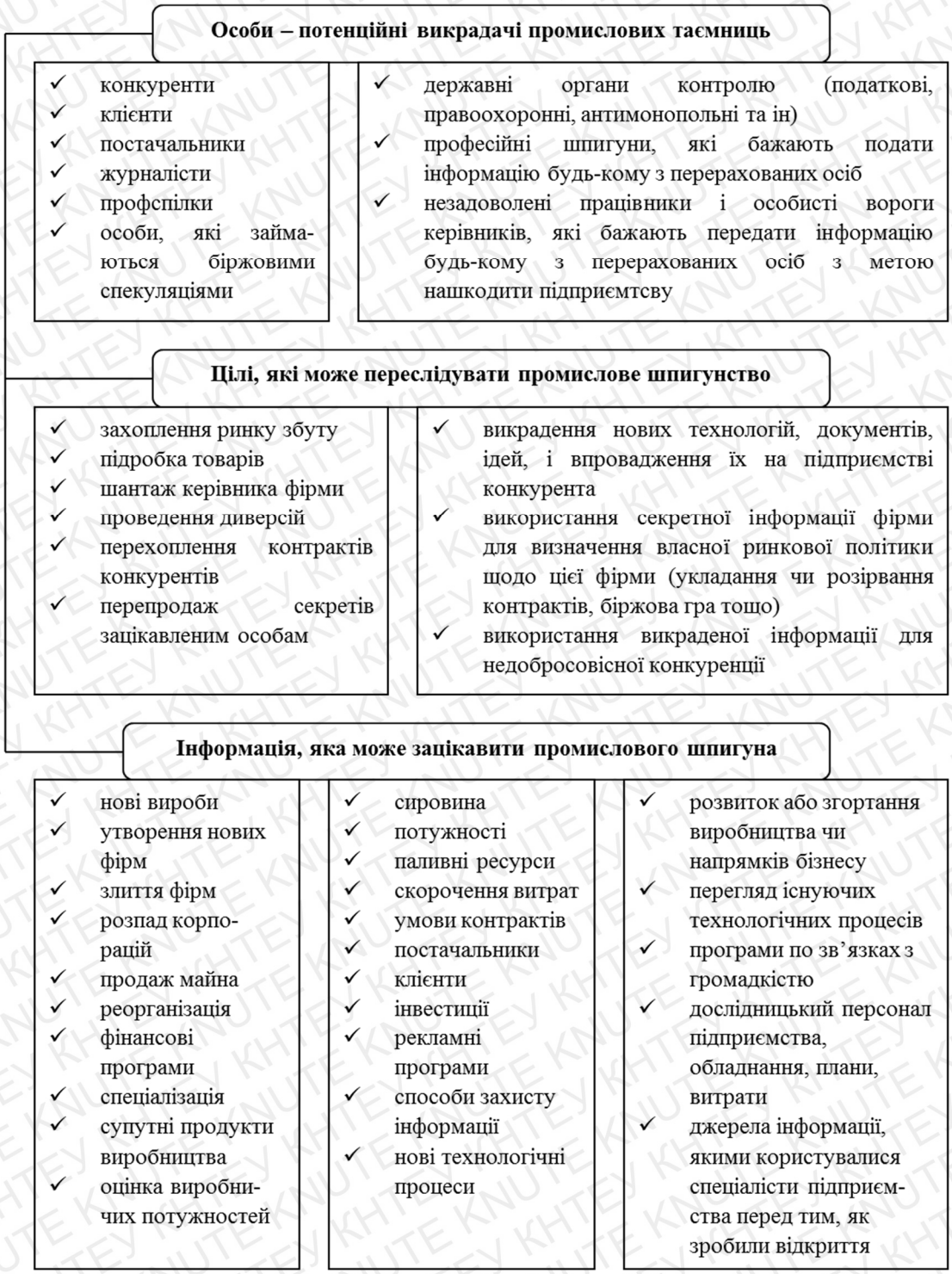

Рисунок 3.1 – Основні ознаки промислового шпигунства

Довідники описують промислове шпигунство як вид недобросовісної конкуренції, діяльність із незаконного добування відомостей, що становлять комерційну цінність [99; с.24].

Слід зазначити, що схожими за своїми задачами, призначенням до промислового шпигунства є ділова (бізнес) розвідка, економічна розвідка, конкурентна розвідка, адже проводяться вони для досягнення ідентичного кінцевого результату – збору інформації. Суттєва різниця між цими поняттями полягає в тому, що промислове шпигунство це здійснення *неправомірних* дій, тобто збирання інформації на яку порушник не має законного права(комерційна таємниця) або ж збирання у спосіб який протирічить вимогам законодавства (перехоплення комп'ютерної інформації, прихована фото- або відеозйомка, підкуп працівника, прослуховування розмов і т. п.) тоді як проведення вищевказаних розвідок може відбуватися в *легальний* спосіб, шляхом обробки, аналізу відкритих джерел, доступної публічної інформації з метою одержання інформації, яка б дала змогу здобути конкурентну перевагу на ринку.

Захист інформації підприємства від промислового шпигунства залежить від методів, що застосовуються недобросовісними користувачами для створення каналів витоку інформації. Методи, які використовують в промисловому шпигунстві прийнято розділяти на *агентурні методи* і *технічні методи*.

Агентурний метод одержання інформації є основою будь-якого виду шпигунства. Найбільш уживаними є два напрями діяльності: вербування і «впровадження» своєї людини.

Інсайдер – особа, яка володіє конфіденційною діловою інформацією в силу свого службового положення [60].

За даними наведеними в світовій статистиці, більше чим в половині випадків у розсекречуванні конфіденційної інформації фірми (промислового шпіонажу) винні співробітники самої фірми, які вербуються конкурентами або спеціальними агенствами, що спеціалізуються на замовленнях такого роду.

При цьому, не обовязково вербувати осіб, які займають керівні ланки в організаційній структурі підприємства. У будь-якому підприємстві є співробітники які за своїми знаннями й досвідом і посадами наближаються до рівня вищої ланки і які здатні самостійно вести свою гру. Результатом вербування може бути те, що вигідні замовлення підуть тим особам, які й організували бізнес-шпигунство на свою користь. Якщо кінцевою метою промислового шпигунства є знищення фірми-конкурента або отримання комерційної таємниці, то варіант із впровадженням має істотне переваги, тому що довіра до своєї людини, звичайно ж, більша.

Об'єктами агентурної розробки можуть бути не тільки, скажімо, «другі» або «треті» особи фірми-конкурента, а й будь-який співробітник якої-небудь, навіть нижчої, ланки. Вони цілком спроможні здійснити приховане встановлення відповідної апаратури («жучків», «комарів» тощо). Для цього необхідно від декількох секунд до двох-трьох хвилин. Щоб встановити обладнання для перехоплення телефонних повідомлень взагалі не потрібно проникати в офіс, а варто лише знайти телефоніста який погодиться знайти потрібний телефонний кабель. Такі «закладки» можуть бути встановлені по лінії телефонного кабелю на відстані до трьох кілометрів від офісу, що значно ускладнює їх виявлення [27, с. 19].

До технічних методів відносяться: встановлення відповідної апаратури для прослуховування в офісах та приміщеннях, «закладки» по лінії телефонного кабелю, «мобільне шпигунство», та інше. Інший напрям промислового шпигунства, що набуває популярності в усьому світі, а також і в Україні, – це отримання конфіденційної інформації за допомогою Інтернету.

Це основні методи промислового шпигунства, які, у свою чергу, поділяються ще на низку способів добування конфіденційної інформації (дезінформування конкурентів, шантаж і підкуп, використання можливостей правоохоронних та контрольних органів тощо).

Для збереження цілісності комерційної таємниці на підприємстві застосовуються відповідні методи захисту:

- правові;
- організаційні;
- технічні.

Правовий захист полягає в оформленні на підприємстві документів, що забезпечують його: - наказ, статут, трудові контракти та угоди, правила внутрішнього розпорядку, які передбачають використання певного комплексу правових засобів, наданих законом і підзаконними актами особам, які законно контролюють таку інформацію. До таких документів слід віднести розробку і прийняття локальних нормативних (корпоративних) актів, що вже були розглянуті в попередніх розділах: Перелік відомостей, які складають комерційну таємницю, Положення про конфіденційну інформацію, комерційну таємницю підприємства та інші. Крім того, організацією розробляється ряд документів для регулювання трудових відносин з працівниками з приводу охорони конфіденційної інформації (комерційної таємниці, ноу-хау), яка була надана йому для виконання трудових функцій.

Організаційний захист передбачає:

- організацію конфіденційного діловодства;
- обмеження доступу до документів з відповідною градацією допуску до них;
- порядок використання технічних засобів і приміщень (при цьому для копіювання та розмноження паперів здійснюється облік паперу, підтверджений свідками або відповідними документами);
- супровід відвідувачів під час їх перебування в службових приміщеннях;
- встановлення порядку ведення переговорів (виявлення наміру відвідувачів, мети їх приходу);
- навчання співробітників заходам захисту, підвищення вимогливості і відповідальності.

До **технічних** відносяться **заходи**, пов'язані з використанням різноманітних технічних засобів, які перешкоджають несанкціонованому

доступу до інформації. Сюди відносяться: кодування повідомлень, які передаються по каналах електронного або факсимільного зв'язку; встановлення різноманітних пристроїв, що перешкоджають зняттю інформації в процесі її проходження по каналах зв'язку; використання апаратів для знищення документів і ряд інших.

Технічний захист використовує:

- засоби охорони територій (контролюючі системи, огорожі з автоматичною системою телевізійного контролю, електронно-оптичні засоби контролю);
- засоби захисту комунікацій (процеси обробки, передачі і збереження інформації за допомогою електроніки – пристроїв з побічними чи паразитними випромінюваннями, а саме: ЕОМ, телетайпи, телефакси з шифрами та кодами, «паразитні наведення» на комп’ютери, датчики пожежної безпеки, запобіжні деталі проти підслуховування для телефонів та ін.).

Застосовуючи весь арсенал засобів для попередження витікання комерційної таємниці, слід вжити і відповідних заходів захисту:

- пошук підслуховуючих пристроїв;
- шифрування ділової кореспонденції;
- захист апаратури від випромінювання з допомогою захисних блоків;
- створення комп’ютерних систем і банку технічних даних по охороні;
- створення внутрішніх перепон акустичним імпульсам (за допомогою екранів).

Такі заходи носять троякий характер:

1) посадові особи і працівники, які мають справу з конфіденційною інформацією (комерційною таємницею, ноу-хау) зобов'язані зберігати її в секреті; особи, які отримали доступ до неї повинні бути попереджені, що така інформація є комерційною таємницею або ноу-хау, і зобов'язані зберігати її в секреті (не розголошувати третім особам), а також нести відповідальність за недотримання конфіденційності. Найчастіше така відповідальність

передбачається в трудовому договорі або укладається окремий договір (про нерозголошення комерційної таємниці або ноу-хау) з працівником;

2) особа, яка законно контролює конфіденційну інформацію (комерційну таємницю, ноу-хау) і повинна передбачити в контракті зі своїми контрагентами, яким надається доступ до неї, обов'язок утримуватись від розголошення її третім особам і передбачити відповідальність за порушення цієї таємниці. Одним із способів фіксації обов'язку щодо збереження конфіденційності є проставлення на відповідних документах грифу «конфіденційно» або «комерційна таємниця»;

3) особа, яка законно контролює конфіденційну інформацію (комерційну таємницю, ноу-хау) повинна прийняти необхідні заходи по недопущенню несанкціонованого доступу третіх осіб до неї, зокрема, що перешкоджають промисловому шпіонажу (контроль за недопущенням установки підслуховуючих пристроїв і т.д.). Недотримання цих умов може бути перешкодою для захисту «законного інтересу» особи, яка законно контролює конфіденційну інформацію (комерційну таємницю, ноу-хау). Можна сказати, що ця умова є обов'язковою для доказування в суді при виникненні спору [99; с.56].

Звичайна, що всі перераховані заходи вживаються на підприємстві з метою, перш за все, профілактики витоку інформації. В цьому сенсі технічні способи захисту інформації є дуже важливим фактором у профілактиці промислового шпигунства. Необхідно не тільки захищатися від можливих атак, а й належним чином зберігати цінну інформацію: обмежувати доступ до неї не тільки третім особам, а й співробітникам; зберігати особливо цінну інформацію в закодованому вигляді; не передавати цінну інформацію жодними засобами зв'язку.

На сьогоднішній день профілактика промислового шпигунства дуже ускладнюється зважаючи на постійний розвиток інформаційних технологій і доступності Інтернету. Хакерські атаки на різні інформаційні системи набули сьогодні воістину колосальних обсягів. Протистояти і захищатися від нових

технологій (пристроїв), спрямованих на зняття інформації, багатьом компаніям просто не по кишені [34].

Створити надійний захист від промислового шпигунства досить складно, і упередити витік інформації на 100 % практично не можливо. При цьому, не всі компанії готові витрачати значні кошти на технічні системи захисту інформації. Особливо це проявляється в економіках, що розвиваються і в тому числі в Україні.

Однак, навіть високотехнологічні підприємства у розвинутих країнах не убезпечені від промислового шпигунства. Із недавніх відомих випадків, що стосуються промислового шпіонажу в розвинутих компаніях можна навести наступні випадки:

1. *«Unilever» та «Procter & Gamble».* Компанія «Procter & Gamble» зізналася в промисловому шпигунстві, яке, як стверджується, здійснювалося протягом шести місяців, та стосувалося продукції по догляду за волоссям компанії-конкурента «Unilever». Особливістю їхнього плану, який «Procter & Gamble» називає «нещасним випадком», є огляд сміття компанії «Unilever» з метою пошуку конфіденційних документів. Однак «Unilever» стверджує, що зазвичай утилізують документи в повному обсязі, а секретні, які становлять загрозу для лідера «Procter & Gamble», є пронумерованими. Компанія «Procter & Gamble» заперечує твердження журналу «Fortune» про даний інцидент. Ці компанії досягли згоди, і «Procter & Gamble» зобов'язалася не використовувати будь-яку інформацію, яку вона отримала нелегальним шляхом, в розробці свого продукту.

2. *«Opel» та «Volkswagen».* Негативним фактором для будь-якої компанії є перехід керівника найвищої ланки управління в іншу компанію. Прикладом цього став перехід керівника та семи його замісників компанії «Volkswagen» у компанію «Opel». Врезультаті «Opel» заявила про промислове шпигунство, а саме - за передбачувану відсутність конфіденційних документів компанії. Увідповідь на це «Volkswagen» виступила із звинуваченнями в наклепі. Чотирирічна судова справа була вирішена, коли компанія «Volkswagen»

погодилася заплатити «General Motors», материнській компанієї «Opel», 100 млн. дол США і розмістити замовлення на понад 1 мільярд доларів у вартості запчастин для автомобілів.

3. *«IBM» та «Hitachi»*. Цей випадок промислового шпигунства, що був названий «Japscam», стосувався прав на комп'ютерні ігри. Компанія «Hitachi» таємно вступила у володіння практичноповним набором «Adirondack», книг компанії «IBM». Звертає на себе увагу той факт, що в них містилася проектна документація «IBM», комерційні таємниці, що містили позначку «Для внутрішнього користування IBM». Після тривалого судового розгляду компанія «Hitachi» заплатила «IBM» 300 млн. дол США.

4. *«Microsoft» та «Oracle»*. Глава компанії «Oracle» здійснював прихований моніторинг за фінансуванням компанії-конкурента «Microsoft».

5. *«Google» та операція «Aurora»*. Компанія «Google» оголосила, що оператори з території Китаю здійснили крадіжку інтелектуальної власності, зокрема, облікових записів електронної пошти від захисників прав людини. Керівники «Google» зазначили, що даний злочин був частиною більш широкої кібератаки від компанії в Китаї, яка стала відома як операція «Aurora». Зловмисники розпочали кібернапад, використовуючи незахищеність браузера Microsoft Internet Explorer, запустивши нову модифікацію трояна «Hydraq». Існувало припущення, що серед «інсайдерів», котрі брали участь у кібернападі, значна частина співробітників Google China, яким було відмовлено в доступі до внутрішніх мереж компанії. Через місяць комп'ютерні експерти американського Національногоагентства безпеки ствердили, що атаки на «Google» походили від двох китайських університетів, чия спеціалізація пов'язана з галузями комп'ютерних наук: «Shanghai Jiao Tong University» та «Shandong Lanxiang Vocational School», останній з котрих має тісні зв'язки з китайською військовою сферою. Деякі коментатори стверджували, що кібернапад був частиною узгодженого китайського промислового шпигунства, спрямованого на отримання високотехнологічної інформації для стимулювання економіки Китаю. Критики вказували на той факт, що ставленням до інтелектуальної

власності іноземних компаній в Китаї є зневажливим, оскільки керівництво таких компаній намагається копіювати або перепроектовувати технології. Через місяць компанія «Google» вирішилаприпинити діяльність по високотехнологічному сектору в Китаї, що призвело до закриття операції «Aurora» [56].

В тих випадках, коли несанкціонований витік конфіденційної інформації вже стався підприємство має бути готовим до правильного, правового і оперативного реагування.

Першочергово необхідно встановити джерело такого витоку, якщо це можливо. У будь-якому випадку, важливо розуміти, яким чином стався такий витік: через співробітників чи через засоби зв'язку.

Якщо витік інформації стався з вини співробітника, необхідно вжити заходів щодо його тимчасового відсторонення та проведення внутрішнього розслідування. Коли витік інформації може загрожувати інтересам третіх осіб, необхідно в терміновому порядку сповістити таких осіб, бажано в письмовому вигляді. Це дозволить тим, чиї інтереси можуть постраждати в результаті такого витоку, також вчасно розробити механізм захисту і вчасно вжити необхідних заходів. Доцільно також звернення із заявою до правоохоронних органів.

Захисту інформації підприємства від промислового шпигунства звичайно ж сприяє і юридичне закріплення в нормативно-правових актах відповідальності недобросовісні дії, щодо конфіденційної інформації.

Так, кримінальна відповідальність за незаконне збирання та умисне розголошення без згоди власника інформації, що становить комерційну таємницю, настає в тому випадку, якщо такий збір та розголошення завдало істотну шкоду суб'єкту господарської діяльності (ст. ст. 231, 232 Кримінального кодексу України). Однак і без умови заподіяння шкоди кримінальна відповідальність передбачена за *несанкціоноване втручання* в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку і за *несанкціоновані збут або розповсюдження інформації* з

обмеженим доступом, яка зберігається в комп'ютерах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.

У випадку встановлення факту незаконного збирання інформації, що становить комерційну таємницю, підприємство може звернутися до Антимонопольного комітету України. При цьому, необхідно надати докази факту, що збір інформації здійснювався незаконними методами. В результаті розгляду справи щодо порушення законодавства про захист від недобросовісної конкуренції Комітет може накласти штраф, а для відшкодування завданих збитків підприємству необхідно звертатися до суду.

Нормативними актами, що регламентують розгляд органами Антимонопольного комітету України справ про захист від недобросовісної конкуренції, є Закон України «Про захист від недобросовісної конкуренції», Закон України «Про захист економічної конкуренції», Правила розгляду заяв і справ про порушення законодавства про захист економічної конкуренції.

Судова практика, щодо покарання винних у збиранні та розголошенні конфіденційної інформації підприємства доволі слабка в Україні, при цьому, визначити розмір збитку від витоку інформації досить непросто. Крім того, якщо промислове шпигунство було здійснене співробітником, довести його вину буває практично неможливо. Іноземні підприємства взагалі, в багатьох випадках, воліють не розголошувати факт промислового шпигунства їх діяльності, оскільки іміджеві втрати іноді значно перевищують розмір збитку від промислового шпіонажу та і судове переслідування за промислове шпигунство в також рідко закінчується на користь позивача.

Судова практика показує, що підприємства не приділяють достатньої уваги нормативному та договірному врегулюванню питань що стосуються конфіденційної інформації, обліку, фіксації та реєстрації фактів надання такої інформації чи доступу до неї, що призводить до складнощів при розгляді судом спору по суті.

Законодавчо не врегульовано порядок визначення розміру та відшкодування збитків завданих неправомірним розголошенням

конфіденційної інформації. Таким чином, доцільно приділити увагу їх визначенню в договірному порядку.

ВИСНОВКИ

Термін «інформація» вперше з'явився в 1387 році в англійській мові, а загальнонауковими поняттями стає із середини XX століття і означає відомості, дані про суб'єкти, об'єкти, явища та процеси.

Правовий статус інформації визначає закон України «Про інформацію». Здійснений в роботі аналіз наукових робіт Северина Л.І., Чередниченка В.С., Шелеста М.Є., Андрєєва В.І., Баранова О.А., Степко О.М., Петрика В.М., Калюжного Р.А., Цимбалюк В.С., показує, що структурні складові забезпечення інформаційної безпеки недостатньо систематизовані. Основу даної системи складають, по-перше, органи, а, по-друге, засоби забезпечення інформаційної безпеки. Вони застосовують комплекс адміністративно-правових, інформаційно-аналітичних, та організаційно-управлінських заходів.

Сучасна теорія і практика виробила багато підходів щодо класифікації інформації. Так, за категоріями, виділяють відкриту, корисну, важливу і конфіденційну інформацію. Для управління і прийняття рішень у сфері підприємництва інформація поділяється на вхідну та вихідну. Інформація, яка характеризує стан фірми містить: організаційно-правові характеристики; виробничі потужності; матеріальні ресурси; трудові ресурси; організаційно-технологічні можливості; економічні характеристики.

Основні види інформації перелічені у статті 10 закону України «Про інформацію», яка може бути: інформацією про фізичну особу; довідково-енциклопедичного характеру; про стан довкілля; про товар (роботу, послугу); науково-технічною; податковою; правовою; статистичною; соціологічною.

Інформація, що виникає в процесі досліджень називається первинною, а та, що є результатом аналітичних узагальнень - вторинною.

Досліджуючи питання ролі та значення правового регулювання інформаційної безпеки, ми дійшли висновку про те, що наразі в Україні іде процес становлення інформаційного суспільства, а тому серед різних напрямів державного управління пріоритетне місце посідає управління інформаційною сферою.

Забезпечити цілеспрямованість зазначених управлінських процесів та створити умови для побудови інформаційного суверенітету України можливо лише за умов створення надійного правового підґрунтя. Правову основу цієї системи складають закони України: «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про інформацію», «Про доступ до публічної інформації».

Прогалиною національного законодавства лишається відсутність легалізації поняття «інформаційна сфера», що, на нашу думку, стає актуальним завданням адміністративно-правової науки.

Нині в Україні управління інформаційною сферою здійснюють п'ять органів державної влади: Національна рада України з питань телебачення і радіомовлення; Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформації; Державний комітет з телебачення та радіомовлення України; Держінформнауки України; Державна служба спеціального зв'язку та захисту інформації України.

Захист інформації на підприємстві включає: категоріювання інформації; встановлення спеціального режиму роботи з окремими категоріями інформації; визначення місць її зберігання та умов доступу; визначення кола осіб, що наділяється правом доступу до інформації; юридичне закріплення цих заходів.

Сукупність заходів для протидії загрозам інформаційній безпеці, захисту і збереження інформаційного ресурсу підприємства визначається в базовому документі підприємства «Політика інформаційної безпеки» (ПІБ). За необхідністю установчі документи підприємства варто доповняти окремим розділом щодо права самостійно встановлювати обсяг відомостей, які становлять комерційну і іншу охоронювану законом таємницю й порядок її захисту.

Положення про конфіденційну інформацію підприємства є базовим документом в системі захисту інформації. Перелік документів підприємства,

що містять конфіденційну інформацію, приймається окремим документом чи як додаток до попереднього положення.

Важливим організаційним питанням є доведення до працівників, користувачів інформації Інструкції із захисту КІ в інформаційній системі підприємства та Положення про конфіденційне діловодство.

У взаємовідносинах з контрагентами підприємства установлена практика внесення розділів про дотримання конфіденційності до договірної документації. Термін дії такого зобов'язання зазвичай тотожний терміну дії договору.

Контроль за впровадженням і реалізацією організаційно-правових заходів ЗІ покладається на підрозділ захисту інформації (ПЗІ). У своїй діяльності ПЗІ керується чинними нормативно-правовими актами, нормативними документами у сфері захисту інформації, Положенням про підрозділ (ПЗІ), розробленим і затвердженим на підприємстві. Підрозділ створюється як окрема штатна одиниця і підпорядковуються виключно керівнику підприємства або особі, яка призначена відповідальною за забезпечення інформаційної безпеки на підприємстві. Досягнення ефективності роботи підрозділу залежить від якісної комплектації працівниками, які мають освіту за напрямом підготовки «Інформаційна безпека», або інженерно-технічну освіту фахового спрямування.

Технічний захист інформації (ТЗІ) – один із елементів захисту інформації в інформаційних системах. Об'єктом технічного захисту є інформація, що становить державну, іншу передбачену законодавством України інформацію, в тому числі інформацію, якій розпорядчими документами по підприємству надано статусу комерційної таємниці та щодо якої встановлений особливі, режимні умови одержання, використання поширення та зберігання. Технічний захист інформації включає два завдання:

1) захист інформації від несанкціонованого доступу;

2) захист інформації від витоку технічними каналами.

Для їх виконання підприємство повинно працювати з відповідними державними та недержавними підприємствами, організаціями, які працюють у галузі захисту інформації, в тому числі зі Службою безпеки України, а також підприємствами, що ліцензовані на здійснення окремих видів діяльності в сфері захисту інформації.

Заволодіння найбільш впливовими інформаційними каналами та суб'єктами інформаційної інфраструктури є одним із головних завдань у відносинах на будь-якому ринку, бо інформаційні і фінансові можливості роблять більш сильними цих суб'єктів. У погоні за посиленням таких можливостей у інформаційних відносинах активно використовується: дискредитація, дезінформація, компрометація, промислове шпигунство, різного роду ідеологічні та інформаційні диверсії.

Найбільш поширеними інформаційними загрозами господарюючих суб'єктів можна вважати: розголошення таємної та конфіденційної інформації; її викрадення, модифікацію чи знищення; незаконне використання інформації, особливо тієї її частини, що становить інтелектуальну власність суб'єктів підприємництва і обумовлює переваги на ринку, несанкціонований доступ до інформації.

Аналізуючи механізми інформаційного протиборства можна зробити висновок, що його центром є людина, а тому інформаційно-психологічний вплив спрямовується на найбільш вразливі сфери психіки: мотиваційну (ціннісні орієнтири); сферу потреб та інтересів; інтелектуальну пізнавальну (знання, пам'ять, мислення); комунікативну (характер і особливості спілкування, взаємовідносини з людьми); функціональну (виконання службових і посадових обов'язків).

У разі, коли об'єктом протидії впливу обирається інформаційне середовище, суб'єкти підприємництва проводять за відповідними моделями заходи контрпропаганди.

Коли ж об'єктом протидії обирається особа, якою здійснюється інформаційно-психологічний вплив, то для них формуються відповідні моделі

протидії: звернення до органів влади, правоохоронних органів, Антимонопольного комітету, суду, громадськості з вимогами припинити проведення щодо суб'єкта негативного інформаційно-психологічного впливу.

Особливу небезпеку серед ризиків інформаційного впливу становить ризик потрапляння суб'єктів підприємництва під дією інформаційного тероризму. Головне завдання контролю полягає в тому, щоб звузити велику різноманітність варіантів дій терористів і контролювати найбільш важливі та небезпечні. Мінімізація зазначених ризиків здійснюється шляхом формування стійкого іміджу суб'єктів підприємництва на ринку, а також проведення заходів захисту криптографічного, апаратного, програмного, адміністративного, правового характеру власних інформаційних мереж і систем. Важливою частиною заходів мінімізації ризиків є формування в колективу працівників фірмового патріотизму, їх згуртування.

Інформаційний простір – головна арена боротьби різних інтересів держав в умовах глобальної інтеграції. Підприємства, банки зазнають інформаційного удару щодо своїх ресурсів із глобальної комп'ютерної мережі Інтернет. Хакери, крекери, телефонні фанатики є добре обізнаними з комп'ютерними технологіями й можуть незаконно проникати в комунікативну систему, отримувати важливу інформацію і завдавати мільярдні збитки банкам та інформаційним ресурсам підприємства.

З розвитком інформаційних мереж інформаційна небезпека перетворилась засоби перекачування по мережі неправдивої інформації, вірусів.

Корпоративна економіка буде знаходитись в інформаційній безпеці за умов залучення інвестицій для скорочення технічного відставання інформаційних технологій; використання новітнього програмного забезпечення та техніки; контролю за інформаційним простором від несанкціонованого доступу до інформації; удосконалення нормативно-правового поля інформаційної сфери.

Характер розвитку світового інформаційного простору вимагає формування міжнародної системи інформаційної безпеки (МСІБ), яка включає:

міжнародні доктринальні документи; міжнародні стандарти в галузі ІБ; міжнародні професійні установи; міжнародно-регіональні інститути (ЄС); інститути, що створюються військово-політичними організаціями (НАТО); національні доктрини, концепції, стратегії.

Головні напрями міжнародної політики у сфері інформаційної безпеки визначають: Окінавська Хартія глобального інформаційного суспільства; Резолюції Генеральної Асамблеї «Досягнення у сфері інформатизації і комунікацій у контексті міжнародної безпеки» та «Створення глобальної культури кібербезпеки та оцінка національних зусиль щодо захисту найважливіших інформаційних інфраструктур», «Боротьба зі злочинним використанням інформаційних технологій».

Окремим видом недобросовісної конкуренція є промислове шпигунство. Залежно від того, які методи використовують в останньому (агентурні чи технічні), буде і здійснюватись захист інформації на підприємстві.

Для захисту інформації від витоку технічними каналами застосовують інженерно-технічні способи захисту (апаратні, програмні криптографічні). З метою захисту інформації на підприємстві відбувається документальне оформлення її статусу («комерційна таємниця», «конфіденційна інформація») з подальшим формуванням переліку відомостей, які її становлять відповідно до ч.2 ст. 505 ЦК та ч. 2 ст. 30 Закону України «Про інформацію». Це дає підстави захищати порушені права у судовому порядку.

Ретельний підбір кадрів для роботи з відомостями категорії «комерційна таємниця» забезпечить її захист. Зобов'язання про нерозголошення інформації краще оформляти записом безпосередньо в тексті трудового договору (контракту), хоча допускається і додатком до трудового договору (контракту).

Отже, промисловому шпигунству можна протидіяти лише у тому разі, якщо інформація яка належить підприємству, набула достатньої правової

охорони, а люди які мають доступ до комерційної таємниці й конфіденційної інформації захищені від відповідних посягань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андреев В. І., Чередниченко В. О., Шелест М.Є. Основи інформаційної безпеки / За ред. проф. Хорошка В. О. вид., доп. і перероб. – К.: Вид. ДУІКТ, 2009. – 292 с.

2. Андрощук Г. Захист комерційної таємниці: економічно-правовий аспект / Г. Андрощук // Інтелектуальна власність. – 1999. – № 9. – С. 8-12.

3. Ахрамович В. М. Адміністративний рівень інформаційної безпеки / В. М. Ахрамович // Сучасний захист інформації. - 2017. - № 1. - С. 10-14. - Режим доступу: http://nbuv.gov.ua/UJRN/szi_2017_1_4

4. Бандурка О. М., Духов В. Є., Петрова К. Я. Основи економічної безпеки: Підручник. – Х.: Вид-во Нац. ун-ту внут. справ, 2003. – 36 с.

5. Баранов О. А. Інфомаційне право України: стан, проблеми, перспективи / О. А. Баранов. – К.: ВД «СофтПрес», 2005. – 316 с.

6. Бачило І. Л., Лопатін В. Н., Федотов М. А. Інформаційне право. – Спб.: Юридичний центр Прес, 2001.

7. Бегун. В.І. Інформаційна безпека: навч. посібник. – К.: КНЕУ, 2008. – 280с.

8. Березин І. Промислове шпигунство, конкурентна розвідка, бенчмаркинг й етика цивілізованого бізнесу // Практичний Маркетинг. - 2005. - 22 липня. - № 101.

9. Березовська І. Р. Поняття і характеристика структурних елементів механізму застосування адміністративно-правових засобів забезпечення інформаційної безпеки України [Електронний ресурс] / І. Р. Березовська // Науковий вісник Національної академії внутрішніх справ. - 2013. - № 2. - С. 31-35. - Режим доступу: http://nbuv.gov.ua/UJRN/Nvknuvs_2013_2_7

10. Бондарчук Ю.В. Безпека бізнесу: організаційно-правові основи / Ю.В. Бондарчук, А.І. Марущак: наук.-практ. посібник. – К.: Вид.дім «Скіф», КНТ, 2008. – 372 с.

11. Валіулліна В. Інформаційна безпека корпоративної економіки в умовах глобалізаційних процесів //Вісник Дніпропетровського університету. 2016. Випуск 63.

12. Василюк В. Система захисту інформації приватного підприємства. Організація служби захисту інформації приватного підприємства//Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (14), 2007 р.

13. Господарський кодекс України від 16.01.2013р. [Електронний ресурс]. – Режим доступу: www.rada.kiev.ua

14. Гуцалюк М.О. Інформаційна безпека України: нові загрози / М.О. Гуцалюк // Бизнес и безопасность. – 2007. – № 5. – С. 2–3.

15. Дзьобань О.П. Інформаційна безпека в умовах глобалізаційних тенденцій: до проблеми осмислення сутності //Гуманітарний вісник ЗДІА випуск 24. 2006.- С 101-108

16. Доступ до інформації та електронне урядування/ Автори-упорядники М.С. Демкова, М.В. Фігель. – К.: Факт, 2004. – 336 с.

17. Е-боротьба в інформаційних війнах та інформаційне право [Текст] / В.М. Брижко [и др.] ; Акад. прав. наук України. Н.-д. центр прав. інформатики. – К. : НДЦПІ АПрН України, 2007. – 233 с.

18. Економічна безпека підприємств, організацій та установ: Навч. посібник / В. Л. Ортинський, І. С. Керницький, З. Б. Живко. – К.: Правова єдність, 2009. – 544 с.

19. Економічна безпека підприємства: навч. посіб./ Т. М. Іванюта, А. О. Зайчковський. – Київ: Центр навч. літ., 2009, - 256 с.

20. Живко З. Б., Живко М. О., Живко І. Ю. Словник сучасних економічних термінів. – Л.: Край, 2007. – с. 58.

21. Живко З.Б., Живко М.О. Регламентація конкурентної розвідки в 5. інформаційно-правовому просторі : Зб. наук. праць / З. Б. Живко, М. О. Живко // Науковий вісник ЛДУВС. – 2007. – Вип. 2. – С. 211-219. – (Серія юридична).

22. Живко М. О. Захист інформації в системі економічної безпеки 2. держави та підприємства : матеріали ІІІ українсько-польської НПК. / М. О. Живко // Регіональне і місцеве самоврядування в нових умовах: партійна публічна адміністрація і безпосередня демократія. – Львів, 2006. – С. 270-277.

23. Забезпечення інформаційної безпеки цифрових програмно-керованих АТС: навчальний посібник / [Кононович В.Г., Стайкуца С.В., Тардаскіна Т.М., Шинкарчук Т.М.]; за ред. чл.-кор. В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – 168 с.

24. Зубок М.І. Інформаційна безпека [Текст] : навч. посібник / М.І. Зубок; Київський національний торговельно-економічний ун-т. – К. : КНТЕУ, 2005. – 133 с.

25. Зубок М.І. Інформаційна безпека в підприємницькій діяльності / М.І. Зубок. – К.: ГНОЗІС, 2015 - 216 с.

26. Зубок М.І. Інформаційно-аналітичне забезпечення підприємницької діяльності: навч. посібник. – К.: КНТЕУ, 2007. – 156с.

27. Івченко О. Промислове (економічне) шпигунство: конкурентна розвідка та контррозвідка // Юридичний журнал. – 20033. – № 7.

28. Інформаційна безпека (соціально-правові аспекти): Підручник / Остроухов В. В., Петрик В. М., Присяжнюк М. М. та ін.; за ред. Є. Д. Скулиша. - К. : КНТ, 2010.-776 с.

29. Інформаційна безпека: навчальний посібник / С.В. Кавун, В.В. Носов, О.В. Манжай. – Ч.2. – Харків : Вид. ХНЕУ, 2008. – 196 с.

30. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / О.Г. Додонов, В.П. Горбулін, Д.В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.

31. Кибертероризм и защита персональних данных. – К.: ООО «Консалтинговая компания «СИДКОН», 2013. – 50с.

32. Кибертероризм, информационные войны и безопасность.-К.: ООО «Консалтинговая компания «СИДКОН». – 2014. – 60с.

33. Климник І.І., Харитонов О.В. «Правова характеристика забезпечення інформаційної таємниці на підприємстві в умовах ринкової економіки», монографія, Харків, ХНУМГ, 2014, С.14

34. Коваль М. Промислове шпигунство: профілактика, оперативне правове реагування http://attorneys.ua/uk/publications/industrial-epionage-prevention-rapid-legal-response/

35. Конкурентная разведка и корпоративная стратегия компании. – К.: ООО «Консалтинговая компания «СИДКОН», 2013. – 52с.

36. Конституція України від 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

37. Кормич Б.А. Інформаційна безпека: організаційно-правові основи [Текст] : навч. посібник для студ. вищих навч. закл. / Б.А. Кормич. – К. : Кондор, 2004. – 384 с. – (Юридична книга).

38. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: монографія / Б.А. Кормич. – Одеса: Юридична література, 2003. – 472 с.

39. Крегул Ю.І., Зубок М.І. Правове регулювання безпеки підприємницької діяльності: навч. посібник. – К.: КНТЕУ, 2013. – 216с .

40. Крегул Ю.І., Зубок М.І., Банк Р.О. Комерційна розвідка та внутрішня безпека на підприємництві. – К.: КНТЕУ, 2014. – 176с.

41. Крюков О. І. Інформаційна безпека держави в умовах глобалізації / О. І. Крюков. // Державне будівництво. - 2007. - № 2. - Режим доступу: http://nbuv.gov.ua

42. Кулініч О.О. Інформація з обмеженим доступом як об’єкт цивільних прав / О.О. Кулініч: : дис…к. юрид. наук. – Одеса, 2006. – 200 с.

43. Литвиненко О.В. Інформаційні впливи та операції. Теоретико-аналітичні нариси: монографія / О.В. Литвиненко. – К.: НІСД, 2003. – 240 с.

44. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський. – К.: КНТ, 2006. – 280 с. (Серія: Національна і міжнародна безпека.)

45. Ліпкан В.А. Національна безпека України: Навч.посіб. – 2-ге вид. – К., 2009 . – С.220 – 221.

46. Ліпкан В.А. Національна і міжнародна безпека у визначеннях та поняттях [Текст] / В. А. Ліпкан, О. С. Ліпкан. – Вид. 2-ге, доп. і переробл. – К. : Текст, 2008. – 400 с.

47. Логінова Н.І.,Дробожур Р.Р. Правовий захист інформації: Навчальний посібник. - О.: Фенікс, 2015. - 264 с.

48. Максименко Ю.С. Теоретико-правові засади забезпечення інформаційної безпеки України: Дис. … канд..юрид.наук. – К., -2007. –с.118

49. Марущак А. І. Інформація як об’єкт цивільних прав // Бюл. Мін’юсту України. – 2005. - №3(41). – с. 44-50

50. Марущак А. Протидія злочинним та конкурентним механізмам. Доступу до інформації про суб’єкта господарювання / А. Марущак. – Сайт юридичного журналу «ЮСТІНІАН» http://www.justinian.com.ua.

51. Марущак А.І. Юридична природа права на інформацію // Бюл. Мін’юсту України. – 2005. - №9. – с.47-52.

52. Марченко О.С. Інформаційна безпека фінансової системи: головні складові та загрози / О.С. Марченко // Збірник наукових праць Міжнародної науково-практичної Інтернет-конференції «Актуальні питання фінансової системи держави», м. Харків, 21 лютого 2014 р. – С. 34-37.

53. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспективи розвитку державності / О. Морозов // Віче. – 2007. – № 12.– Спецвипуск. – С. 23-25.

54. Муковський І.Г., Міщенко А.Г., Шевченко М.М. Інформаційно-аналітична діяльність в міжнародних відносинах: навч. посібник. – К.: Кондор, 2012. - 224с.

55. Мунтіян В. І. Економічна безпека України. – К.: КВІЦ, 1999. – 463 с.

56. Муравська(Якубівська)Ю. Є. Тенденції розвитку промислового шпигунства у світі//Ефективна економіка № 1, 2017/[Електронне наукове фахове видання] Режим доступу: http://www.economy.nayka.com.ua/?op=1&z

57. Нашинець-Наумова А.Ю. Адміністративно-правові методи забезпечення інформаційної безпеки корпорацій / А.Ю. Нашинець-Наумова // Підприємництво, господарство і право. – 2015. – № 10. – С.16-20.

58. Нашинець-Наумова А.Ю. Організаційно-правові методи забезпечення інформаційної безпеки корпорацій / А.Ю. Нашинець-Наумова // Підприємництво, господарство і право. – 2015. – № 11. – С.21-24.

59. Нашинець-Наумова А.Ю. Особливості застосування адміністративних методів забезпечення інформаційної безпеки корпорацій / А.Ю. Нашинець-Наумова // Информационные технологии и безопасность: материалы XV международной научно-практической конференции ИТБ-2015 (г. Киев, 21 октября 2015 г.). – К.: ИПРИ НАН Украины, 2015. – С. 163-166.

60. Нашинець-Наумова А.Ю. Поняття та ознаки інсайдерської інформації як особливого виду інформації з обмеженим доступом / А.Ю. Нашинець-Наумова // Підприємництво, господарство і право. – 2016. – № 4. – С. 73-76.

61. Нашинець-Наумова А.Ю. Правове регулювання інформаційної безпеки корпорацій / А.Ю. Нашинець-Наумова // Правова інформатика. – 2014. – №4/44. – С. 95-99.

62. Нашинець-Наумова А.Ю. Проблеми правового регулювання доступу до конфіденційної інформації на підприємстві / А.Ю. Нашинець-Наумова // Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»: зб. наук. праць. – 2012. – №4 (25). – С. 119-124.

63. Нашинець-Наумова А.Ю. Реалізація адміністративно-правових форм у сфері забезпечення інформаційної безпеки корпорацій / А.Ю. Нашинець-Наумова // Підприємництво, господарство і право. – 2015. – № 8. – С. 46-48.

64. Новицька Н.Б. Правове забезпечення інформаційної безпеки // Інформаційна безпека людини, суспільства, держави. – 2009. – №1 - С.44 -47 - с.46

65. Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки України / О.В. Олійник // Право і суспільство. – 2012. – № 3. – С. 132-137.

66. Основи інформаційного права України [Текст] : навч. посіб. / В.С. Цимбалюк [та ін.] ; ред. М. Я. Швець [та ін.]. – К. : Знання, 2004. – 274 с.

67. Пастернак-Таранущенко С. Економічна безпека держави. – К., 1994.

68. Петрик В. М. Визначення інформаційної безпеки та її різновид // Форми та методи забезпечення інформаційної безпеки держави: зб. матер. міжнар. наук.-прак. конф. (м. Київ, 13 березня 2008 р.). – К.: Видавець Захаренко В.О., 2008. – 216 с.]

69. Петрик В.М. Інформаційна безпека України: поняття, сутність та загрози / В.М. Петрик, М.В. Галамба // Юридичний журнал. – 2006. – №11. – С. 49-52.

70. Питання концепції реформування інформаційного законодавства України / Р. А. Калюжний, В. Гавловський, В. Цимбалюк, М. Гуцалюк // Збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». К.: НТУУ «КПІ», Міносвіти і нацуки України, СБУ. - К. – 2000. – с. 17-21.

71. Потреба часу – створення Інформаційного кодексу України [Електронний ресурс] / Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=70301&cat_id=6465.

72. Почепцов Г.Г. Інформаційний та віртуальний простори України: кроки в майбутнє. [Електронний ресурс]. – Режим доступу: http://osvita.mediasapiens.ua

73. Правове забезпечення інформаційної діяльності в Україні / за заг. ред. Ю. С. Шемшученка, І. С. Чижа. – К.: ТОВ «Юридична думка», 2006. – 384 с.

74. Прибутько П.С., Лук'янець І.Б. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. –К.: Видавець ПАЛИВОДА А.В., 2007. – 252с.

75. Про боротьбу з тероризмом: Закон України // Відомості Верховної Ради України. – 2003. – № 25. – Ст. 180.

76. Про доступ до публічної інформації : Закон України від 13 січ.2011 р. № 2939. / [Електронний ресурс]. – Режим доступу : http://zakon1. rada. gov. ua/cgi-bin/laws/main. cgi? nreg=2939-17.

77. Про електронний цифровий підпис, Закон України. ВВР, 2003, №36, ст.276

78. Про електронні документи та електронний документообіг, Закон України. ВВР, 2003, №36, ст.275

79. Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу : Закон України від 18 вересня 2004 р. // ВВРУ. – 2004. – №29. – Ст. 367.

80. Про затвердження Положення «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці»: наказ Адміністрації Держспецзв'язку від 29.03.2013 – №05.

81. Про затвердження Положення про формування інформаційної бази даних про ринок цінних паперів : Рішення Національної комісії з цінних паперів та фондового ринку від 03.06.2014. – № 733.

82. Про захист від недобросовісної конкуренції, Закон України, ВВР, 1996, №36, ст. 164

83. Про захист інформації в інформаційно-телекомунікаційних системах, Закон України. ВВР, 1994, №31, ст. 281

84. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Указ № 449/2014 про рішення РНБО від 28 квітня 2014 року.

85. Про інформацію: Закон України від 2 жовтня 1992 року №2658- XII.

86. Про Концепцію Національної програми інформатизації, Закон України. ВВР, 1998, №27-28, ст.182

87. Про національну безпеку України: Закону України 21 червня 2018 року 2469-VIII [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2469-19

88. Про перелік відомостей, що не становлять комерційної таємниці Постанова Кабінету Міністрів України від 09.08.93 р. № 611.

89. Про порядок здійснення криптографічного захисту інформації в Україні, Положення, затверджене Указом Президента України від 22.05.1998р. №505. [Електронний ресурс]. – Режим доступу: www.rada.kiev.ua

90. Про технічний захист інформації в Україні. Положення, затверджене Указом Президента України від 27.09.1999р., №1229/ (99). [Електронний ресурс]. – Режим доступу: www.rada.kiev.ua

91. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розповсюдження відомостей, що становлять комерційну або банківську таємницю: Монографія. – Х.: Ксілон, 2008. – 202 с.

92. Северин Л. І., Северин С. Л., Дудатьєв А. В. Правове забезпечення захисту інформації. Навчальний посібник. – Вінниця: ВНТУ, 2004. – 145 с.

93. Сороківська О. А., Гевко Л. Інформаційна безпека підприємства: нові загрози та перспективи.// Вісник Хмельницького національного університету 2010, № 2, Т. 2

94. Степко О. М. Аналіз головних складових інформаційної безпеки держави / О. М. Степко // Інститут міжнародних відносин Національного авіаційного університету. – 2011. [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/Soc_Gum/Nvimvnau/2011_1/83-92.pdf

95. Стратегія розвитку інформаційного суспільства в Україні, затверджена Розпорядженням КМУ від 15.05.2013р. №386 – Р. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua

96. Типове положення про службу захисту інформації в автоматизованій системі: Наказ Департаменту спеціальних телекомунікаційних

систем та захисту інформації Служби безпеки України від 04 грудня 2000 р. - № 53.

97. Тихомиров О. Забезпечення інформаційної безпеки: теоретико-правовий аспект / О. Тихомиров // Право України. – 2011. – № 4. – С. 252-259.

98. Ткачук Т.Ю. Конкурентна розвідка:навч. Посібник. – К.: 2009. 295

99. Управління захистом комерційної таємниці: курс лекцій / Укладач: Суярова О.О. – Суми: Вид-во СумДУ, 2009. –73 с.

100. Фомін В.О. Сутність і співвідношення понять «інформаційна безпека», «інформаційна війна» та «інформаційна боротьба» / В.О. Фомін, А.О. Рось [Електронний ресурс] / Режим доступу: http://www.security.ukrnet.net/search.php.

101. Ханін Г. Формування міжнародної системи інформаційної безпеки: економічні орієнтири для україни, Ефективна економіка № 4, 2015

102. Харенко О.В. Поняття «інформація» в юридичній науці та законодавстві України //Часопис Київського університету права. – 2014. – №3.

103. Цивільний кодекс України від 16.01.2013р. [Електронний ресурс]. – Режим доступу: www.rada.kiev.ua

104. Цимбалюк В.С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Зб. наук. праць. – 2004.– Вип. 8. – С. 32.

105. Цимбалюк В.С., Бабійська А.В. «Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики» // Адміністративне право і процес. - № 2(8). – 2014 - с.22 – 28 – С.28

106. Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. Комплексні системи захисту інформації : навчальний посібник / ВНТУ. – Вінниця : ВНТУ, 2018. – 118 с.