НАВЧАЛЬНО-МЕТОДИЧНА ЛІТЕРАТУРА

Міністерство освіти і науки України
Тернопільський національний технічний університет
імені Івана Пулюя
Факультет економіки та менеджменту

Кафедра Менеджменту інноваційної
діяльності та підприємництва

КУРС ЛЕКЦІЙ

з дисципліни

«ЕКОЛОГІЧНЕН УПРАВЛІННЯ ТА БЕЗПЕКА БІЗНЕСУ»

для студентів всіх форм навчання

напрям підготовки 07 «УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ»,
спеціальність 073 «МЕНЕДЖМЕНТ»
спеціалізація «УПРАВЛІННЯ ІННОВАЦІЙНОЮ ДІЯЛЬНІСТЮ»

Тернопіль
2017

Курс лекцій розроблено відповідно до навчальних планів підготовки фахівців освітньо-кваліфікаційного рівня “магістр” за спеціальністю 073 «МЕНЕДЖМЕНТ», спеціалізація «УПРАВЛІННЯ ІННОВАЦІЙНОЮ ДІЯЛЬНІСТЮ».

Укладачі: к.е.н., асист. Шерстюк Р.П.
к.е.н., доц. Малюта Л.Я.
к.е.н., ст. викл. Мельник Л.М.

Рецензенти: д.е.н., проф. Андрушків Б.М.
к.т.н., доц. Стойко І.І.

Методичні вказівки розглянуто та схвалено на засіданні кафедри менеджменту інноваційної діяльності та підприємництва.
Протокол № 9 від 26.01.2017 р.

Методичні вказівки рекомендовано до друку методичною комісією ФЕМ.
Протокол № 6 від 14.02.2017 р.

ЗМІСТ

ВСТУП

Метою даного курсу є формування у майбутніх управлінців системи знань і практичних навичок для управління усією сукупністю впливів підприємства на навколишнє середовище з поступовим зниженням ступеня таких впливів шляхом економії сировини та енергії, мінімізації відходів і забруднень, забезпечення безпечних умов праці персоналу, оцінки ступеня екологічних ризиків і формування свідомого екологічного світогляду як необхідного атрибуту якісно нової ідеології управління підприємством та оволодіння студентами теоретичних відомостей, основних понять, загальних принципів, категорій та методологічних положень економічної безпеки підприємства і підприємництва.

Основним завданням курсу є освоєння методів оцінки зовнішнього середовища підприємства з екологічних позицій, аналізу функціонуючих систем менеджменту, оцінювання екологічної діяльності підприємств, формулювання екологічної політики, підготовки планів і розробки екологічних програм на підприємствах, впровадження систем екологічного менеджменту, оцінки їх результативності та ефективності, ознайомити із поняттям економічної безпеки бізнесу, основними її видами, принципами та методологічними положеннями в контексті виникнення необхідності формування заходів та ефективної системи безпеки вітчизняного підприємства розглянути основні види рейдерства, які базуються на злитті, поглинанні та корпоративному захопленні компаній (підприємств) та організаційно-економічні заходи щодо його попередження, навчитися практично аналізувати конкретні ситуації і вирішувати поставленні завдання, що випливають із запропонованих тем лекційних занять та захист фінансово-майнової, інноваційної безпеки та економічної безпеки держави загалом.

МОДУЛЬ 1

Тема 1:«ЕКОЛОГІЧНЕ УПРАВЛІННЯ У КОНЦЕПЦІЇ СТАЛОГО РОЗВИТКУ»

1. КОНЦЕПЦІЯ СТАЛОГО РОЗВИТКУ

Концепція сталого розвитку має довгу історію становлення. Починаючи від наукових праць В.І. Вернадського про ноосферу (початок минулого сторіччя), декларації першої конференції ООН з навколишнього середовища (Стокгольм, 1972 р.), де було зазначено зв'язок економічного і соціального розвитку з проблемами навколишнього середовища, наукових доповідей Римського клубу (1972 р.), у яких формулювалися ідеї переходу цивілізації до стану «глобальної динамічної рівноваги», до звіту Всесвітньої комісії ООН з навколишнього середовища і розвитку в 1987 р., конференції ООН з проблем навколишнього середовища і розвитку в Ріо-де-Жанейро (1992 р.), Всесвітнього саміту з питань сталого розвитку в Йоганнесбурзі (2002 р.) і сьогодення.

Появу терміну «сталий розвиток» (sustainable development) пов'язують з ім'ям прем'єр-міністра Норвегії Гру Харлем Брундланд, яка сформулювала його в звіті «Наше спільне майбутнє», що було підготовлено для ООН і опубліковано у 1987 р. Міжнародною комісією з навколишнього середовища і розвитку. Вона визначала його як розвиток, який задовольняє потреби теперішнього часу, проте не ставить під загрозу здатність майбутніх поколінь задовольняти свої власні потреби.

В червні 1992 р. у Ріо-де-Жанейро відбулася Конференція ООН з навколишнього середовища і розвитку, на якій було прийнято історичне рішення про зміну курсу розвитку усього світового співтовариства. Це безпрецедентне рішення глав урядів і лідерів 179 країн було обумовлено катастрофічною глобальною екологічною ситуацією і прогнозованою глобальною катастрофою, що може вибухнути вже в XXI ст. і призвести до загибелі всього живого на планеті. На цій конференції була прийнята Світова програма дій «Порядок денний на XXI століття», яка є програмою дій з впровадження засад сталого розвитку в країнах світу. В Програмі дій наголошується, що досягнення сталого розвитку вимагає ув'язки та інтеграції трьох основних цілей:

1) *економічних* – ця концепція передбачає оптимальне використання обмежених ресурсів і використання екологічних – природо-, енерго- і матеріалозберігаючих технологій, включаючи видобуток і переробку сировини, створення екологічно прийнятної продукції, мінімізацію, переробку і знищення відходів;

2) *соціальних* – орієнтована на людину і спрямована на збереження стабільності соціальних і культурних систем, в тому числі, на скорочення числа

руйнівних конфліктів між людьми. Важливим аспектом цього підходу є справедливий розподіл благ;

3) *екологічних* – сталий розвиток має забезпечувати цілісність біологічних і фізичних природних систем. Основна увага приділяється збереженню здібностей до самовідновлення і динамічної адаптації таких систем до змін, а не збереження їх у деякому «ідеальному» статичному стані.

Концепція сталого розвитку охоплює, як мінімум, дві найважливіші **ідеї**:

- такий розвиток передбачає вирішення економічних, соціальних та екологічних проблем. Розвиток буде сталим тільки тоді, коли буде досягнута рівновага між різними факторами, що зумовлюють загальний рівень життя;
- нинішнє покоління має обов'язок перед прийдешніми поколіннями залишити достатні запаси соціальних, природних та економічних ресурсів для того, щоб вони могли забезпечити для себе рівень добробуту не нижчий, ніж той, що ми маємо зараз.

Узгодження цих ідей та їх переклад на мову конкретних заходів, які є засобами досягнення сталого розвитку – завдання величезної складності, оскільки всі три елементи сталого розвитку повинні розглядатися збалансовано. Важливі також і механізми взаємодії цих трьох концепцій. Економічний і соціальний елементи, взаємодіючи один з одним, породжують такі нові завдання, як досягнення справедливості всередині одного покоління (наприклад, щодо розподілу доходів) та надання цілеспрямованої допомоги бідним верствам населення. Механізм взаємодії економічного та екологічного елементів породив нові ідеї щодо вартісної оцінки та інтерналізації (обліку в економічній звітності підприємств) зовнішніх впливів на навколишнє середовище. Нарешті, зв'язок соціального та екологічного елементів викликала інтерес до таких питань як внутрішньопоколінна і міжпоколінна рівність, включаючи дотримання прав майбутніх поколінь, та участі населення в процесі прийняття рішень.

Невід'ємною частиною концепції стійкого розвитку є система індикаторів, розроблена Комісією ООН зі сталого розвитку.

Індикатори сталого розвитку – з одного боку, відображають соціальні, економічні і екологічні параметри у єдиному комплексі; з іншого – їх розвиток розглядається через зміну станів, кожен з який характеризується визначеною сталістю і здатністю до змін.

Комісія пропонує 134 індикатори сталого розвитку, які розділені на наступні основні групи:

1. *Група соціальних індикаторів*: боротьба з бідністю; демографічна динаміка і стан; поліпшення освіти, поінформованості і виховання суспільства; захист і поліпшення здоров'я людей; поліпшення розвитку поселень.

2. *Група економічних індикаторів*: міжнародна кооперація для прискорення сталого розвитку і пов'язана з цим місцева політика; зміна характеристик споживання; фінансові ресурси і механізми; передача екологічно чистих технологій, співробітництво і створення потенціалу.

3. *Група екологічних індикаторів*: збереження якості водних ресурсів і

забезпеченість ними; захист морів і прибережних територій; комплексний підхід до планування і раціонального використання земельних ресурсів; раціональне управління вразливими екосистемами, боротьба з опустелюванням і посухами; сприяння веденню сталого сільського господарства і розвитку сільських районів; боротьба за збереження лісів; збереження біологічної розмаїтості; екологічно безпечне використання біотехнологій; захист атмосфери; екологічно безпечне управління твердими відходами і стічними водами; екологічно безпечне управління токсичними хімікатами; екологічно безпечне управління небезпечними відходами; екологічно безпечне управління радіоактивними відходами.

4. *Група інституціональних індикаторів*: облік питань екології і розвитку в плануванні і управлінні для сталого розвитку; національні механізми і міжнародне співробітництво для створення потенціалу в країнах, що розвиваються; міжнародний інституціональний порядок; міжнародні правові механізми; інформація для прийняття рішень; посилення ролі основних груп населення.

Складність практичного застосування концепції сталого розвитку полягає в тому, що короткострокові економічні вигоди окремих країн найчастіше суперечать довгостроковим інтересам сталого розвитку та потенційним економічним вигодам світової спільноти.

Варто відзначити, що досягнення оптимального варіанту розвитку декларують ряд країн, у кожної країни свій шлях розвитку. В одних цей шлях тільки починається, в інших вже розпочався, треті вже стали на шлях сталого економічного розвитку (США, Японія, країни Європейського Союзу). Існує багато і таких країн, яким не до сталого розвитку і вони його не сприймають. На перше місце вони ставлять одну стратегічну мету – вижити. Саме такі країни провокують загрози, що поширюються до інших держав та їхніх регіонів. Досягти сталого розвитку регіонів надзвичайно важко, адже близьке сусідство з іншими державами формує загрозу екологічної небезпеки, а глобалізація, що стрімко набрала обертів, сприяє утворенню та загостренню економічних та соціальних небезпек, що зрештою торкаються регіонального розвитку.

2. ОРГАНІЗАЦІЙНІ ПІДХОДИ І МЕТОДИ ЗНИЖЕННЯ РІВНЯ ВПЛИВУ ВИРОБНИЦТВА НА ДОВКІЛЛЯ

Підприємства виробничої та невиробничої сфери є основними суб’єктами, від результатів діяльності яких залежить рівень екологічної безпеки, і тим самим, добробут нинішніх і майбутніх поколінь. Ступінь впливу на навколишнє середовище при цьому залежить від вибору технології виробництва (ресурсномісткої або, навпаки, екологічно чистої, маловідходної), видів своєї продукції і наданих послуг. Таким чином, екологічна проблематика впливає на всі сторони діяльності підприємства, діючи на внутрішні механізми прийняття

управлінських рішень та на взаємини з партнерами по бізнесу, органами екологічного контролю, фінансовими організаціями, місцевим населенням. Очевидно, що успішне ведення бізнесу залежить від ступеня врахування екологічних аспектів діяльності та пов'язаних з ними можливостей і ризиків.

Зниження впливу промислового виробництва на навколишнє середовище може бути досягнуто:

- мінімізацією викидів, скидів, відходів;
- раціональним використанням сировини і енергетичних ресурсів;
- створенням маловідходних ресурсозберігаючих технологічних процесів.

Все розмаїття методів мінімізації впливу промислового виробництва на навколишнє середовище можна розділити на:

- технологічні та технічні методи очищення викидів і скидів, утилізації відходів;
- технологічні та технічні методи, спрямовані на зниження кількості забруднюючих речовин, що утворюються;
- організаційні методи.

За оцінками фахівців, основною причиною економічних та екологічних проблем в Україні є неефективне управління. Існуюча на багатьох підприємствах система управління, сформована в умовах планової економіки, не відповідає сучасним вимогам. До типових проблем вітчизняних підприємств можна віднести:

- відсутність чітких орієнтирів і принципів діяльності;
- дисбаланс повноважень і відповідальності;
- невміння мотивувати персонал;
- наявність організаційних структур, орієнтованих на внутрішні потреби, а не на запити клієнтів, відсутність ефективного зворотного зв'язку з зацікавленими сторонами.

До даного моменту світовою спільнотою накопичено позитивний досвід ефективного менеджменту, який може бути успішно адаптований в українських умовах. Розроблено теоретичні основи менеджменту, як області знань і професійної діяльності, спрямованої на формування і досягнення цілей організації шляхом раціонального використання наявних ресурсів. Відпрацьовано та стандартизовані ефективні моделі управління, зокрема концепція загального управління якістю (Total Quality Management – TQM), яка послужила основою для розробки систем екологічного менеджменту.

3. СУТНІСТЬ І ЗАВДАННЯ ЕКОЛОГІЧНОГО МЕНЕДЖМЕНТУ

Система екологічного управління – відносно нове явище в світовому господарстві, яке можна визначити як спеціальну систему управління, спрямовану на збереження якості навколишнього середовища, забезпечення нормативно-правових екологічних параметрів і засновану на концепції сталого розвитку

суспільства.

Практична реалізація принципів сталого розвитку багато в чому визначається організацією і розвитком систем виробничо-екологічного управління та екологічного менеджменту.

Розрізняють природоохоронний менеджмент і екологічний менеджмент.

Природоохоронний менеджмент (Environmental Management) не вимагає істотної зміни ситуації техніко-економічної системи. Це як би консервативний екологічний менеджмент або перша ступінь готовності підприємства до вирішення проблем екологічної безпеки. Природоохоронний менеджмент – це система економічного управління об'єктом шляхом пристосування вже наявної інфраструктури до вимог національних і міжнародних нормативів, актів, правил у сфері ресурсозбереження та раціонального природокористування.

Основними завданнями природоохоронного менеджменту є:

- економія сировинних ресурсів;
- мінімізація відходів і забруднень навколишнього середовища;
- організація безпечної праці персоналу;
- оцінка екологічного ризику;
- виділення коштів на створення «зеленого» іміджу підприємства;
- інформування населення про характер виробничої діяльності підприємства і про стан навколишнього середовища в зоні дії підприємства.

Екологічний менеджмент (Ecological Management) – більш досконала система управління. Стосовно підприємства він передбачає формування екологічно безпечного виробничо-територіального комплексу, забезпечує оптимальне співвідношення між екологічними та економічними показниками протягом усього життєвого циклу як самого комплексу, так і виробленої ним продукції.

Основними завданнями екологічного менеджменту є:

- організація екологічно безпечних виробничих процесів;
- забезпечення екологічної сумісності всіх виробництв;
- попередження негативного антропогенного впливу на природу в процесі виробництва, споживання та утилізації продукції, що випускається;
- отримання максимального результату при мінімальній шкоді для навколишнього середовища;
- перетворення екологічних обмежень у нові можливості зростання виробничої діяльності;
- оновлення продукції виходячи з попиту та створення «зеленого» іміджу підприємства в очах громадськості;
- створення і впровадження маловідходних технологій;
- стимулювання природоохоронних ініціатив, що знижують витрати або сприяють зростанню доходів.

Разом з тим, говорячи про переваги еко-менеджменту, не можна не сказати і про ризики, пов'язані з його впровадженням. Загалом розрізняють:

1. *Ефекти, що позначаються на витратах*, наприклад:

- високі інвестиційні та виробничі витрати на обладнання для охорони навколишнього середовища;
- високі витрати, пов'язані з реалізацією екологічного менеджменту в інших сферах (таких як організація роботи з громадськістю в екологічних питаннях; введення на ринок екологічно чистих продуктів; організація екологічної інформаційної системи; проведення науково-дослідної роботи з екологічної тематики);
- витрати, пов'язані з проведенням зовнішньої експертизи та отриманням офіційного дозволу.

2. *Ринкові та інноваційні ризики*:

- збільшення класичних інноваційних ризиків (наприклад, через незавершених природозберігаючих технологій);
- особливі ринкові ризики еко-продуктів (у зв'язку з перебільшеною оцінкою розміру ринку і т.д.);
- пильна увага громадськості та порушення підприємницької солідарності (наприклад, у зв'язку із занадто швидким проривом в області екологічних стандартів, що набагато випереджає середні темпи пристосування галузі);

3. *Відсутність систематики і слабка координація діяльності з охорони навколишнього середовища*.

Однак, всі зазначені ризики не можуть звільнити сучасні підприємства, що працюють на тривалу перспективу, від необхідності впровадження систем активного екологічного менеджменту.

4. КОРОТКІ ІСТОРИЧНІ ВІДОМОСТІ ТА ЕТАПИ РОЗВИТКУ СИСТЕМИ ЕКОЛОГІЧНОГО УПРАВЛІННЯ

Аналіз взаємодії людини з природою дозволяє виділити чотири періоди, різних за часом і силою впливу людей на природу. В даний час спостерігається перехід до п'ятого періоду.

Перший період – ера примітивної культури кам'яного століття і первіснообщинного укладу життя. Це найтриваліший період взаємодії людини з природою, що призвів до мало відчутних змін у ній.

Другий період – з початку землекористування, тобто від VIII-VII ст. до н.е. до становлення промислового виробництва в XV ст. н.е. Це період рабовласницького і феодального суспільства, період активного розвитку скотарства і землеробства. Іригація земель. Використання підземних вод. Використання деревини як основного енергетичного джерела і будівельного матеріалу призводить до скорочення площі лісових масивів. Розвиток мореплавства, китовий промисел призвели до скорочення стада китів.

Використання природних ресурсів викликає необхідність пізнання законів природи, що призводить до прискорення розвитку науки, в тому числі

природознавства. Формуються перші природоохоронні положення, законодавства і традиції.

Так, феодали встановлюють найжорстокіші порядки щодо вирубування лісів, відстрілу тварин, випасання худоби тощо у своїх володіннях. У той же час в нескінченних міжусобних війнах вони нерідко знищують все живе на землях своїх сусідів, руйнують природні ландшафти, іригаційні системи і т.д., що призводить до міграції та вимирання народів, втрати родючості землі.

Третій період охоплює з XVI по XIX ст. Це час становлення і розвитку капіталізму, приватного підприємництва, концентрації продуктивних сил. Але це і період загарбницьких воєн, що призводили до поділу світу. Активне освоєння мінерально-сировинних ресурсів, розвиток гірничої справи, металургії, видобутку вугілля призвело до порушення геохімічного балансу біосфери.

Розширення і вдосконалення виробництва, його концентрація в промислових районах. Інтенсивний процес урбанізації. Використання вугілля як палива, відсутність систем очищення призвело до швидкого забруднення повітряного басейну, річкових систем й іноді – до деградації ґрунтового покриву (гірничо-промислові райони Великобританії, Центральної Європи, Південного Уралу та Сполучених Штатів Америки).

Четвертий період – період соціальних революцій, період імперіалізму. Організація великих промислових виробництв, посилення їх шкідливого впливу на навколишнє середовище. Реальна небезпека виснаження не тільки невідновлюваних, а й відновлюваних природних ресурсів.

Вплив людини визначається трьома обставинами:

1. Синтез понад 1 млн. хімічних речовин, відсутніх у природних умовах і які володіють якостями, не характерними для природних сполук.

2. Будівництво широкої мережі газо-, нафтопроводів, ліній електропередач, магістральних доріг, масове транспортування різноманітної сировини – все це призвело до забруднення атмосфери, літосфери та гідросфери.

3. Масове виробництво і застосування добрив, пестицидів, гербіцидів, негативна побічна дія яких виявилася через тривалий час з початку їх застосування.

Погіршення стану довкілля та небезпека виснаження невідновлюваних і відновлюваних ресурсів привернули увагу багатьох вчених, політиків і громадськості до проблеми забруднення навколишнього середовища. Англійський дослідник Л.Дж. Боттон писав: «Можливі два варіанти: або люди зроблять так, що в повітрі стане менше диму, або дим зробить так, що на Землі стане менше людей».

У 1972 р. відбулася Міжнародна Стокгольмська конференція щодо навколишнього середовища людини, в роботі якої взяли участь представники 113 країн. У 1983 р. ООН створила Всесвітню комісію з навколишнього середовища і розвитку, у звіті якої за 1987 р. відмічено, що якщо людство не змінить багато чого в своїй виробничій діяльності і способі життя, то його чекають надзвичайно важкі випробування і різке погіршення навколишнього середовища.

У червні 1992 р. у м. Ріо-де-Жанейро відбулася конференція ООН з навколишнього середовища і розвитку. Представниками 179 держав був прийнятий історичний документ «Порядок денний на XXI століття».

П'ятий етап – епоха інформаційного суспільства. З кінця XX ст. масовий наступ інформації на всі сторони життя людини і суспільства. Інформаційні ресурси, технології, інформація – товар в сучасній економіці. У цій епосі можна виділити такі фази розширеного відтворення інформації: інформатизація ринку, менеджменту; віртуальний капітал, віртуальні фінанси; екологічний менеджмент – як екологічно безпечне управління сучасним виробництвом в умовах різних форм власності і різних галузей економіки.

Сучасне виробниче екологічне управління в першу чергу направлене на дотримання обов'язкових державних вимог у галузі навколишнього середовища і використання природних ресурсів. Очевидна необхідність розробки і прийняття міжнародних стандартів з управління навколишнім середовищем.

5. *ОСНОВНІ НАПРЯМКИ ЕКОЛОГІЧНОЇ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА ТА СТРУКТУРА ЙОГО ЕКОЛОГІЧНОГО МЕНЕДЖМЕНТУ*

Якщо раніше підприємства традиційно розглядали реалізацію екологічних заходів як додаткове економічне навантаження (особливо в частині інвестицій в технології, що дозволяють дотримуватися встановлених нормативних вимог), то в останні 20 років ситуація змінилася. Посилення законодавства, зростання можливостей для просування екологічно чистої продукції, підвищення тиску зі сторони громадськості, питання етики і зобов'язання країн у рамках міжнародних/регіональних конвенцій зумовили підвищення значимості екологічних питань.

У загальному вигляді еволюція підходів до вирішення питань екологічної безпеки господарської діяльності на рівні підприємства в країнах ЄС (рис. 1.1.) полягає в переході від *екологічно пасивної* до *екологічно реактивної стратегії* (очищення викидів і скидів «на кінці труби»), далі до *активної* (використання найкращих економічно і технічно доступних маловідходних, ресурсо- та енергозберігаючих технологій без надмірних витрат), *превентивної* або *попереджувальної* (зменшення або виключення утворення емісій і відходів у місцях їх можливої появи, зменшення споживання вихідної сировини, матеріалів та енергії в технологічних процесах) і *превентивно-проактивної* стратегії, що ототожнюється з поняттям «чисте виробництво».

Екологічна діяльність на рівні підприємства стратегічно націлена на реалізацію сталого розвитку, який в сучасних умовах можливий тільки шляхом застосування нової практики ведення бізнесу, зокрема, інтеграції всіх економічних суб'єктів – виробника (товарів і послуг), постачальників сировини і комплектуючих виробів, торговельних і логістичних фірм, споживачів,

суспільства та інших зацікавлених сторін, а також тісної співпраці з організаціями, що займаються просуванням продукції на ринку, що забезпечують успіхи в конкурентній боротьбі та формують імідж підприємства.

Традиційно виділяють два основних напрямки екологічної діяльності підприємства – **раціональне природокористування** і **природоохоронна діяльність**. Крім цього на даний час розвиваються нові напрями екологічної діяльності, які мають безпосередній вплив на підвищення результатів фінансового і соціально-економічного стану, здійснення господарської діяльності. Ці нові напрямки пов'язані з забезпеченням конкурентоспроможності, якості і екологічної безпеки продукції і соціального розвитку підприємства, а також з включенням екологічної діяльності в автоматизовану систему управління.

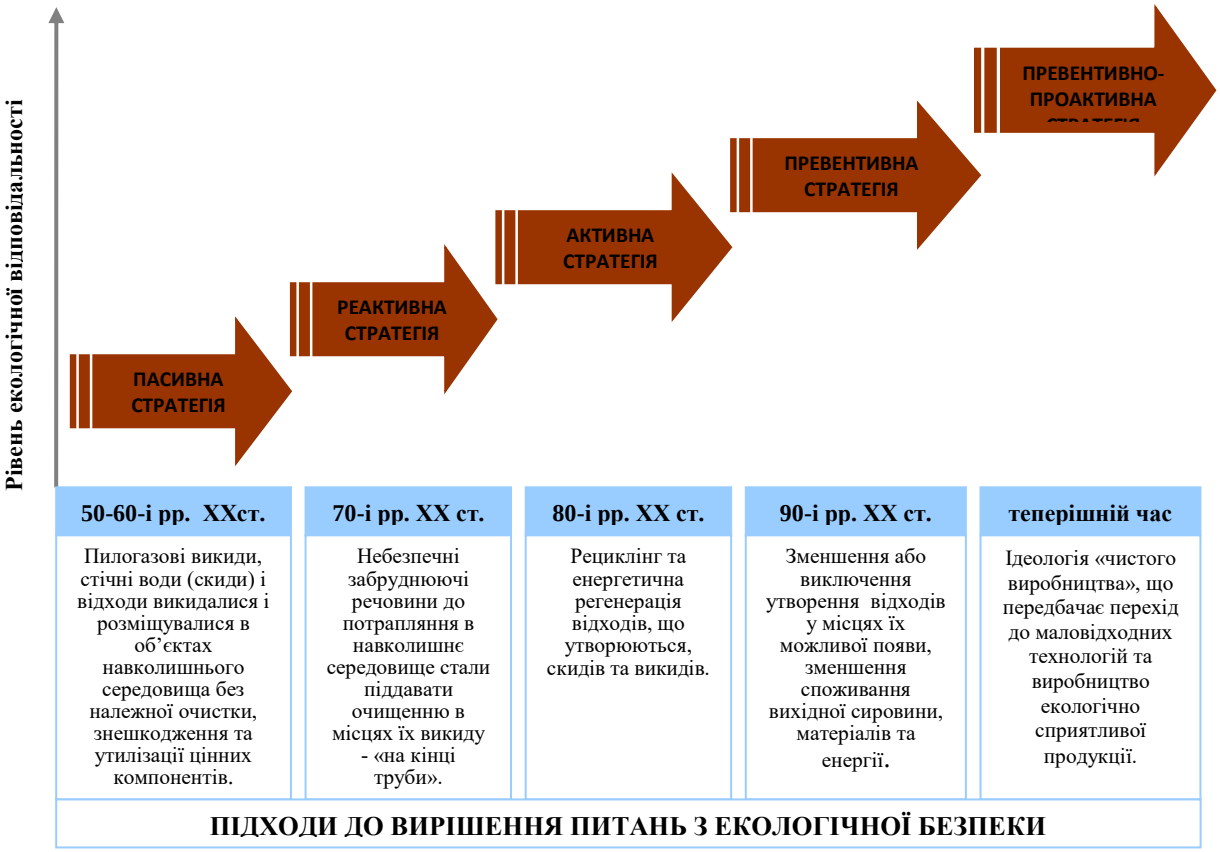


Рис. 1.1. Еволюція підходів до вирішення питань екологічної безпеки господарської діяльності на рівні підприємства

Таким чином напрямки екологічної діяльності підприємства на сучасному етапі є такі:

- раціональне природокористування;
- природоохоронна діяльність;
- екологізація технології виробництва продукції;
- інформаційне забезпечення екологічної діяльності.

Слід звернути увагу, що екологізація технології виробництва безпосередньо

пов’язана з інноваційними і виробничими питаннями розробки, виробництва і реалізації конкурентоспроможної продукції.

Система визначених напрямків екологічної діяльності підприємства формує особливу структуру управління – екологічний менеджмент підприємства, який характеризується такими якісними особливостями:

1) безпосереднє відношення до вирішення проблем конкурентоспроможності, якості і екологічної безпеки продукції, що виробляється та реалізується;

2) безпосереднє відношення до підтвердження відповідності продукції стандартам якості на основі екологічного підходу у вирішенні проблем сертифікації;

3) в бюджеті екологічного менеджменту підприємства частину фінансових витрат на екологічну діяльність підприємства можна віднести на собівартість продукції і отримати додаткові інвестиції у виробництво безпечної, екологічно чистої продукції;

4) необхідність впровадження екологічного менеджменту в загальну систему менеджменту підприємства може вимагати необхідність підготовки спеціалістів у сфері екологічної діяльності підприємства з необхідними технологічними навиками організації і виконання екологічних робіт на підприємстві;

5) стимулювання розширення інформаційної бази підприємства і застосування сучасних інформаційних комп’ютерних технологій;

6) стимулювання розвитку підприємницької діяльності в умовах вільної конкуренції товаровиробництва і забезпечення екологічно чистого виробництва;

7) комплексна реалізація екологічної політики підприємства з врахуванням інноваційних проектів.

Це свідчить про те, що екологічний менеджмент підприємства має чітко визначені функціональні типи діяльності й обґрунтовує потребу в конкретних спеціалістах і цілком самостійний статус в структурі управління господарською діяльністю підприємства.

6. ЕКОЛОГІЧНА СЛУЖБА ПІДПРИЄМСТВА

Ключовою ланкою у системі екологічного управління та менеджменту є екологічна служба підприємства, або у випадку невеликих виробництв окремий кваліфікований спеціаліст (менеджер), уповноважений вирішувати відповідні завдання.

На практиці зустрічаються чотири основних типи структур систем екологічного управління та менеджменту, що розрізняються за положенням у них екологічної служби підприємства або уповноваженого спеціаліста:

1. Структура з відсутньою екологічною службою або фахівцем у галузі екологічного менеджменту.

2. Структура, в якій екологічна служба (посадові обов'язки менеджера) поєднана з яким-небудь іншим підрозділом (іншими посадовими обов'язками) підприємства.

3. Структура, в якій екологічна служба (менеджер) виділена в окремий підрозділ (посада).

4. Структура, в якій екологічна служба виділена в окремий підрозділ з керівником, рівним за рангом заступнику директора підприємства.

Найменш ефективною є структура екологічного управління першого типу. Рішення виробничих екологічних завдань у даному випадку покладено на ту чи іншу посадову особу в якості додаткового навантаження. Це можуть бути головний інженер, головний технолог, головний енергетик та інші. Оскільки ці посадові особи в першу чергу виконують свої безпосередні обов'язки, то вся природоохоронна діяльність зводиться ними переважно до виконання формальних вимог чинного природоохоронного законодавства, наприклад до заповнення необхідної звітності.

Для структури другого типу характерне існування підрозділу або окремого фахівця, який займається питаннями екологічного управління. При цьому їхні функції (посадові обов'язки) суміщені з іншими функціями (посадовими обов'язками). Наприклад, досить часто відбувається поєднання в одному підрозділі екологічної служби та служби охорони праці або суміщення екологічної служби та служби експлуатації «дружнього» до навколишнього середовища обладнання. Для систем екологічного управління та менеджменту даного типу характерні такі недоліки:

- недостатня увага до екологічних аспектів діяльності підприємства;
- обмеженість часу і ресурсів для практичної реалізації природоохоронної діяльності;
- великий обсяг обов'язків, що обмежує можливості ініціативної діяльності;
- недолік авторитету екологічної служби (спеціаліста-менеджера).

У третьому типі системи екологічного управління екологічна служба (фахівець у галузі екологічного менеджменту) виділена в окремий підрозділ підприємства (посаду), має свого керівника, але при цьому не володіє достатньою вагою в ієрархічній структурі підприємства. Тут можна виділити один характерний недолік – ефективність функціонування екологічної служби (спеціаліста-менеджера) залежить від підпорядкованості та місця у загальній системі менеджменту. Разом з тим даний тип структури екологічного управління набуває суттєвих переваг:

- можливість комплексно і повноцінно здійснювати екологічну діяльність;
- більш високий авторитет екологічної служби (спеціаліста-менеджера);
- детальне вивчення екологічних проблем.

Найбільш ефективною і яка має найбільше потенційних можливостей у використанні переваг екологічного менеджменту є система четвертого типу, в якій екологічна служба виділена в окремий підрозділ, а її керівник (фахівець-

менеджер) за посадою залежно від розміру підприємства прирівнюється до заступника директора або заступника головного інженера. Для таких структур характерні такі переваги:

- можливість найбільш комплексно, раціонально і повноцінно здійснювати екологічну діяльність;
- ефективне поєднання основних виробничих і екологічних цілей і завдань на підприємстві;
- здійснення різноманітної і економічно ефективної екологічної діяльності.

За способом організації діяльності можливий наступний розподіл екологічних служб підприємств:

1. Екологічні служби *диференційованого типу*, в яких обов'язки співробітників розділені за видами впливу на навколишнє середовище. Поділ обов'язків співробітників за видами технологічних операцій виправдано для великих підприємств (виробничих об'єднань), на яких екологічна служба включає більше 10 чоловік. Перевага екологічної служби такого типу полягає у тому, що можна досконало вивчити вимоги і можливості в певній галузі діяльності чи на окремій технологічній операції, здійснювати більш ефективне управління, наприклад, у галузі поводження з відходами виробництва і споживання, і приймати правильні рішення. До недоліків структури екологічних служб цього типу відноситься ізольованість сфер діяльності фахівців.

2. Екологічні служби *інтегрованого типу*. Співробітники екологічної служби такого типу в складі підрозділу відповідають за природоохоронну діяльність на підприємстві, разом виконують роботи, пов'язані з охороною навколишнього середовища та раціональним використанням природних ресурсів. Такий тип структури екологічної служби підприємства досить поширений для середніх і дрібних підприємств. Переваги екологічних служб подібного типу:

- взаємозамінність співробітників (у разі відсутності когось із співробітників інші фахівці можуть успішно виконувати його обов'язки);
- комплексний характер робіт (при розгляді питань, пов'язаних з одним видом впливу на навколишнє середовище, враховуються й інші аспекти такого впливу. Так, наприклад, при розробці обґрунтування лімітів розміщення відходів важливими являються не тільки знання і навички в даній області, а й в області дії на атмосферне повітря, раціонального використання водних і земельних ресурсів);
- розробка правильної екологічної політики, визначення комплексних цілей і завдань підприємства в галузі охорони навколишнього середовища та раціонального використання природних ресурсів.

3. Екологічні служби *змішаного типу*. Співробітники подібних екологічних служб можуть виконувати обов'язки, пов'язані з різними видами впливу на навколишнє середовище, а також займатися екологічними проблемами певної технологічної операції. Екологічним службам такого типу притаманні переваги і недоліки служб вищеописаних типів.

Оптимальним типом організації виробничої екологічної служби для дрібних і середніх підприємств є служба інтегрованого типу з відсутністю поділу

обов’язків за видами впливу на навколишнє середовище.

Для великих підприємств і виробничих об’єднань з кількістю співробітників в екологічній службі понад 10 осіб ефективніша служба диференційованого типу з поділом обов’язків між співробітниками.

При будь-якій організації виробничої екологічної служби важливий комплексний підхід у здійсненні ефективного екологічного управління.

Тема 2: «НОРМАТИВНО-МЕТОДИЧНА СИСТЕМА ЕКОЛОГІЧНОГО УПРАВЛІННЯ»

1. ДЖЕРЕЛА ЕКОЛОГІЧНОГО ПРАВА В УКРАЇНІ

Під джерелами екологічного права розуміють нормативно-правові акти, якими регулюються відносини у сфері взаємодії навколишнього природного середовища і суспільства.

Загалом виділяють такі групи джерел екологічного права:

➢ *за юридичною силою* – закони і підзаконні акти:

1) закони: «Про охорону навколишнього природного середовища»;
2) підзаконні акти:

- укази Президента України: «Про збереження і розвиток природно-заповідного фонду України», «Про біосферні заповідники України», «Про приватизацію та оренду земельних ділянок несільськогосподарського призначення для здійснення підприємницької діяльності», «Про день довкілля» (3-я субота квітня) та ін.;

- постанови Кабінету Міністрів України – значна частина постанов стосується затвердження правил природокористування, порядку здійснення контрольних функцій, затвердження різноманітних екологічних нормативів, ін. Зокрема, постановами КМУ були затверджені: Положення про порядок встановлення лімітів використання ресурсів загальнодержавного значення, Положення про порядок розроблення екологічних програм, Положення про порядок видачі дозволів на спеціальне використання природних ресурсів, Положення про державну систему моніторингу довкілля тощо;

- накази, інструкції, інші нормативно-правові акти міністерств та інших центральних органів виконавчої влади – найбільш широкими повноваженнями в екологічній сфері щодо видання таких актів наділені Міністерство екології та природних ресурсів України, Міністерство охорони здоров'я України, Державне агентство земельних ресурсів України, Державне агентство водних ресурсів України, Державне агентство лісових ресурсів України та ін.;

- акти місцевих державних адміністрацій та органів місцевого самоврядування: ними вирішуються питання місцевого життя, в т.ч. екологічного характеру, зокрема затверджуються програми охорони навколишнього природного середовища, передбачаються заходи екологічного характеру в процесі забудови і благоустрою, забезпечення санітарного благополуччя, утилізації та переробки відходів тощо;

➢ *за характером правового регулювання* – загальні (Конституція України, ЗУ «Про основи національної безпеки України») та спеціальні (стосуються виключно екологічних питань – ЗУ «Про охорону навколишнього природного середовища»);

➢ *за предметом правового регулювання* – комплексні (ЗУ «Про охорону навколишнього природного середовища») і природоресурсні (Земельний, Водний та Лісовий кодекси, ЗУ «Про тваринний світ» тощо) або ті, якими регулюються окремі питання екологічної діяльності (ЗУ «Про екологічну експертизу», «Про екологічний аудит», ін.);

➢ *за способом правового регулювання* – матеріальні (визначаються права й обов'язки, а також юридична відповідальність учасників еколого-правових відносин) та процесуальні (регулюють процедуру реалізації норм права);

➢ *за ступенем систематизації* – кодифіковані (ЗУ «Про охорону навколишнього природного середовища» (він є стрижнем комплексної галузі екологічного права і законодавства), Земельний, Водний і Лісовий кодекси, Кодекс України про надра, ЗУ «Про Тваринний світ» та «Про охорону атмосферного повітря») й усі інші.

2. *ЕКОЛОГІЧНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ПРИРОДООХОРОННОГО ЗАКОНОДАВСТВА*

Екологічна відповідальність – компенсаційна матеріально-фінансова відповідальність за завдану екологічну шкоду; обов'язок суб'єкта економічної діяльності відшкодувати завдану екологічну шкоду.

Екологічна відповідальність існує в двох формах: *еколого-правовій* (юридична відповідальність) і *еколого-економічній* (економічна відповідальність).

У системі різновидів **юридичної відповідальності** за екологічні правопорушення розрізняють такі види відповідальності:

- кримінальну;
- адміністративну;
- майнову (цивільно-правову);
- дисциплінарну.

➢ **Кримінальна відповідальність** у галузі екології регулюється Кримінальним кодексом України і застосовується у випадку вчинення екологічних злочинів, які відокремлені в самостійний розділ «Злочини проти довкілля» та охоплює 19 складів злочинів. Усі вони передбачають екологічно-небезпечні наслідки.

Покарання за екологічні злочини:

- виправні роботи;
- кримінальний штраф;
- позбавлення волі;
- конфіскація незаконно добутих знарядь злочину;
- позбавлення права займати відповідні посади.

➢ **Адміністративна відповідальність** – це вид юридичної відповідальності, що найчастіше має місце в сфері природокористування та охорони навколишнього середовища. Перелік екологічних адміністративних

правопорушень міститься в главі 7 Кодексу України про адміністративні правопорушення «Адміністративні правопорушення в галузі охорони природи, використання природних ресурсів, охорони пам'яток історії та культури».

За своїми об'єктивними ознаками адміністративне правопорушення зовні схоже зі злочином, однак основним критерієм їх розмежування є ступінь небезпеки діяння, тяжкість заподіяних наслідків. Основні ознаки, що дають можливість розмежувати екологічний злочин і адміністративний проступок – це повторність здійснення екологічного правопорушення, наявність умислу, систематичність, тяжкість наслідків, які свідчать про підвищену небезпеку та інші.

Види адміністративно-правових стягнень:

- штраф;
- вилучення об'єктів правопорушення;
- позбавлення права заняття спеціальною діяльністю;
- конфіскація знарядь правопорушення;
- обмеження, зупинення, припинення діяльності чи експлуатації об'єктів.

➢ **Майнова відповідальність** за екологічні правопорушення (делікти) – це різновид юридичної відповідальності, яка передбачає виконання обов'язків фізичних і юридичних осіб щодо компенсації шкоди, заподіяної власником чи користувачем природних ресурсів, порушення екологічних та інших прав громадян.

Підставою майнової відповідальності є наявність реальної шкоди (майнової, моральної).

Способи (методи) обчислення шкоди, заподіяної екологічним правопорушенням:

- нормативний;
- витратний;
- таксовий;
- розрахунковий.

➢ **Дисциплінарна відповідальність** за екологічне правопорушення регламентується ст. 68 Закону України «Про охорону навколишнього природного середовища» і Кодексом законів про працю України. Вона виражається у накладенні власником підприємства, установи, організації чи уповноваженим ним органом на винного працівника дисциплінарного стягнення за невиконання чи неналежне виконання ним його трудових обов'язків, пов'язаних з використанням природних ресурсів, охороною навколишнього середовища, за порушення вимог екологічного законодавства, дотримання якого є його посадовим обов'язком. Законодавство не встановлює конкретного переліку дисциплінарних проступків у галузі охорони довкілля, за які настає відповідальність, як це має місце стосовно адміністративної чи кримінальної відповідальності.

Згідно з Кодексом законів про працю України до порушників можуть бути застосовані наступні дисциплінарні стягнення:

- догана;

- звільнення;
- депреміювання (повне чи часткове позбавлення премії за підсумками року, наприклад, за невиконання планів і заходів щодо охорони навколишнього середовища або за порушення природоохоронного законодавства).

Економічна відповідальність – це платежі за використання природних ресурсів, забруднення довкілля, які відповідний суб'єкт вносить до бюджету у безспірному порядку в наперед визначених розмірах.

3. СТАНДАРТИ І МІЖНАРОДНІ РЕКОМЕНДАЦІЇ В СИСТЕМІ ЕКОЛОГІЧНОГО МЕНЕДЖМЕНТУ (УПРАВЛІННЯ)

Міжнародний стандарт – стандарт розроблений міжнародною організацією стандартизації. Найвідомішою з них є International Organization for Standardization (ISO).

Міжнародні стандарти допомагають долати технічні бар'єри в міжнародній торгівлі, що спричинюються відмінностями стандартів розроблених окремо кожною нацією.

Протягом 90-х років XX століття у галузі екологічного управління було розроблено:

- **BS 7750** – британський стандарт (перша версія – березень 1992 року);
- **EMAS** – стандарт Євросоюзу (перша версія – 1993 року);
- **IS 310** – ірландський стандарт (1994 рік);
- **CSA Z750 94A** – канадський стандарт (1994 рік);
- **ISO 14000** – серія стандартів Міжнародної організації з стандартизації (1996 рік), ін.

3.1. БРИТАНСЬКИЙ СТАНДАРТ BS 7750 В СИСТЕМІ ЕКОЛОГІЧНОГО МЕНЕДЖМЕНТУ

У 1992 році у Великобританії був прийнятий перший у світі стандарт в області систем екологічного менеджменту BS 7750, підготовлений і випущений Британським Інститутом Стандартизації.

Характерною особливістю цього стандарту є те, що він не пропонує і не визначає конкретних вимог до природоохоронної діяльності підприємства, але містить рекомендації, корисні для створення ефективної системи екологічного менеджменту і для розвитку екологічного аудиту. Це, у свою чергу, призводить до поліпшення екологічних характеристик діяльності організації в цілому і до поліпшення стану навколишнього середовища. Таким чином, цей стандарт робить непрямий позитивний вплив на стан навколишнього середовища.

Стандарт BS 7750 передбачає такі стадії розробки та впровадження системи

екологічного менеджменту на підприємствах:

1. Попередній огляд ситуації. На цій стадії необхідно визначити всі екологічні нормативні вимоги, що пред'являються до діяльності підприємства, і встановити, які елементи екологічного менеджменту вже існують на даному об'єкті.

2. Розробка заяви про екологічну політику, яка б охоплювала всі аспекти діяльності підприємства і його продукцію.

3. Визначення структури розподілу обов'язків і відповідальності в системі екологічного менеджменту.

4. Оцінка ступеня впливу підприємства на навколишнє середовище. Ця оцінка включає складання переліку діючих нормативів, переліку характеристик викидів в атмосферу і викидів у водні екосистеми, переліку характеристик відходів, що розміщуються, а також опис аспектів впливу на навколишнє середовище підприємств-постачальників.

5. Розробка екологічних цілей і завдань підприємства.

6. Визначення тих стадій виробництва та видів діяльності, реалізованих на підприємстві, які можуть завдати суттєвого негативного впливу на навколишнє середовище, і розробка системи контролю цих стадій та видів діяльності.

7. Розробка програми екологічного менеджменту, призначення старшого менеджера, відповідального за її виконання. Програма повинна бути складена таким чином, щоб враховувалися не тільки теперішні, а й усі минулі види діяльності підприємства, а також можливий вплив на навколишнє середовище життєвого циклу нових видів продукції.

8. Розробка і випуск детального керівництва, яке дозволяло б аудитору системи екологічного менеджменту визначити, що система екологічного менеджменту функціонує нормально.

9. Встановлення системи реєстрації всіх екологічно вагомих подій, видів діяльності тощо, наприклад, записи випадків порушення вимог екологічної політики, описи вжитих заходів для поліпшення ситуації, звітів з підсумками інспекції та поточного контролю.

10. Аудити. BS 7750 включає опис процедури аудиту і деталізує вимоги до аудиторського плану. У стандартах BS 7750 під аудитом розуміється систематична оцінка, націлена для визначення, узгодження чи функціонування системи екологічного менеджменту із запланованими цілями, завданнями, структурою тощо, чи впроваджена система екологічного менеджменту є ефективною і відповідає вимогам екологічної політики підприємства.

3.2. СХЕМА ЕКОЛОГІЧНОГО МЕНЕДЖМЕНТУ І АУДИТУ EMAS

У 1993 р. Радою Європейського співтовариства було прийнято «Положення, яке дозволяє добровільну участь компаній промислового сектора в Схемі еко-менеджменту та аудиту Співтовариства». Документом була визначена «Схема

еко-менеджменту та аудиту» (Eco-management and audit scheme або EMAS), до якої входили вимоги щодо системи менеджменту підприємств, що брали участь (по великому рахунку, схожі з вимогами BS 7550, але доповнені положенням щодо публікації екологічного звіту), вимоги щодо реєстрації підприємств і організацій та їх акредитації в країнах ЄС.

Мета розробки EMAS полягала в оцінюванні та поліпшенні екологічних характеристик діяльності промислових підприємств і в створенні умов для надання населенню екологічної інформації. Передбачалося, що впровадження систем екологічного менеджменту буде сприяти постійному поліпшенню екологічних характеристик діяльності підприємств шляхом:

- розробки та реалізації екологічної політики та екологічних програм;
- періодичної об'єктивної та систематизованої оцінки параметрів діяльності всіх підрозділів підприємства;
- надання населенню екологічної інформації про підприємство;
- реєстрація (сертифікація) організацій відповідно до вимог є добровільною; система створена виключно для промислових підприємств.

Цикл системи екологічного менеджменту відповідно до вимог EMAS включає п'ять основних компонентів:

1. Розробку екологічної політики та випуск документа (заяви), що описує прихильність організації досягненню конкретних екологічно значущих цілей шляхом вирішення певних завдань.

2. Оцінку існуючої ситуації, тобто встановлення початкових характеристик діяльності, по відношенню до яких буде оцінюватися ефективність функціонування системи екологічного менеджменту.

3. Формулювання конкретних завдань (тобто встановлення тих характеристик діяльності, які підлягають поліпшенню), що відповідають цілям екологічної політики підприємства.

4. Розробка екологічної програми, що деталізує шляхи і стадії вирішення поставлених завдань.

5. Проведення екологічного аудиту для того, щоб періодично перевіряти чи вирішуються поставлені організацією завдання і чи веде система екологічного менеджменту до поліпшення екологічних показників діяльності підприємства.

Як видно, багато вимог стандартів BS 7750 і EMAS близькі. Вважається, що британський стандарт BS 7750 послужив моделлю для розробки європейського рекомендаційного документа EMAS. Схема еко-менеджменту та аудиту Європейського Союзу EMAS не є стандартом у повному розумінні цього слова.

3.3. СЕРІЯ МІЖНАРОДНИХ СТАНДАРТІВ СИСТЕМИ ЕКОЛОГІЧНОГО МЕНЕДЖМЕНТУ ISO 14000

Рішення про розробку серії **стандартів ISO 14000** було результатом

Уругвайського раунду переговорів зі Всесвітньої торгової угоди та зустрічі на вищому рівні з проблем навколишнього середовища й розвитку в Ріо-де-Жанейро в 1992 р. Стандарти ISO 14000 розроблено Технічним комітетом 207 (ТС 207) Міжнародної Організації Стандартизації (ISO) з урахуванням вже зарекомендованих міжнародних стандартів із систем менеджменту якості продукції (ISO 9000).

Система стандартів ISO 14000 орієнтована не на кількісні параметри (обсяг викидів, концентрації речовин тощо) і не на технології (вимога використовувати або не використовувати певні технології, вимога використовувати «найкращу доступну технологію»). Основним предметом ISO 14000 є система екологічного менеджменту (EMS). Типові положення цих стандартів полягають у тому, що в організації повинні виконуватися визначені процедури, повинні бути підготовлені певні документи, призначені відповідальні за визначені сфери екологічно значимої діяльності.

Стандарти серії ISO 14000 не містять ніяких «абсолютних» вимог до впливу організації на навколишнє середовище, за винятком того, що організація в спеціальному документі (екологічній політиці) повинна оголосити про своє прагнення відповідати національному природоохоронному законодавству і національним стандартам.

Такий характер стандартів обумовлений, з одного боку, тим, що ISO 14000 як міжнародні стандарти не повинні втручатися у сферу дій національних нормативів. З іншого боку, попередником ISO є «організаційні» підходи до якості продукції (наприклад, концепція «загального управління якістю»), згідно з якими, ключем до досягнення якості є побудова належної організаційної структури і розподіл відповідальності за якість продукції і послуг.

Таким чином основною метою серії стандартів ISO 14000 і встановлених ними вимог є просування найбільш ефективних і результативних практик екологічного менеджменту в організаціях, а також надання: корисних, придатних до використання, економічно-вигідних, систематизованих, гнучких і здатних до пристосування під діяльність різних організацій інструментів.

Документи, що входять до серії ISO 14000, можна умовно поділити на три групи:

- принципи створення й використання систем екологічного менеджменту;
- інструменти екологічного контролю і оцінки;
- стандарти, зорієнтовані на продукцію.

За названими групами розроблені та впроваджуються відповідні документи (табл. 1.1.).

Система стандартів має забезпечувати зменшення несприятливих дій на навколишнє середовище на трьох рівнях:

- *організаційному* – через поліпшення екологічної «поведінки» корпорацій;
- *національному* – через створення суттєвого доповнення до національної нормативної бази й компоненти державної екологічної політики;
- *міжнародному* – через поліпшення умов міжнародної торгівлі. У

міжнародних стандартах серії ISO 14000 екологічний аспект визначено як елемент діяльності підприємства, його продукції та послуг, який взаємодіє чи може взаємодіяти з навколишнім середовищем.

Таблиця 1.1.

Перелік міжнародних стандартів серії ISO 14000

Принципи створення й використання систем екологічного менеджменту	
ISO 14001	Система екологічного менеджменту (EMS) – Специфікації та посібник з використання
ISO 14004	EMS – Загальний посібник з принципів, систем і методів
ISO 14014	Посібник з визначення «початкового рівня» екологічної ефективності підприємства
Інструменти екологічного контролю і оцінки	
ISO 14010	Посібник з екологічного аудиту – Загальні принципи
ISO 14011/1	Посібник з екологічного аудиту – Процедури аудиту. Аудит систем екологічного менеджменту
ISO 14012	Посібник з екологічного аудиту – Критерії кваліфікації екологічних аудиторів
ISO 14031	Посібник з оцінки екологічних показників діяльності організації
Стандарти, зорієнтовані на продукцію	
ISO 14020 (серія)	Принципи екологічного етикетування продукції
ISO 14040 (серія)	Методологія «оцінки життєвого циклу» – оцінки екологічного впливу, пов'язаного з продукцією на всіх стадіях її життєвого циклу
ISO 14050	Екологічний менеджмент. Глосарій (словник)
ISO 14060	Посібник з обліку екологічних аспектів у стандартах на продукцію

Окрім стандартів, у економічно розвинених країнах використовують також ринкові інструменти екологічного менеджменту, серед яких:

- податкові інструменти (пільгові чи дискримінативні): податки на продукцію, види діяльності, джерела забруднення, вміст шкідливого компонента;
- інструменти системи кредитування (пільгові чи податкові);
- субсидії (прямі й непрямі) на державні екологічні проекти, на екологічні цілі населенню, дотації на екологічно досконалу продукцію;
- екологічні платежі за викиди шкідливих речовин в атмосферу, водні джерела, ґрунт;
- цінові інструменти;
- сплата за досягнення певних екологічних результатів тощо.

Якщо врахувати важкий фінансовий стан більшості промислових

підприємств, різке скорочення бюджетного фінансування, яке виділяється на охорону природи й відтворення природних ресурсів, недоліки законодавства, то очевидно, що західна модель екологічного управління вітчизняну економіку не цілком влаштовує. Адже сьогодні Україна не в змозі застосовувати настільки сильний стимуляційний механізм ринкових інструментів, щоб підприємства самостійно переходили до екологічного виробництва, але деякі із західних моделей все-таки можна застосувати.

Переваги міжнародно визнаних стандартів достатньо очевидні. Наприклад, успішна участь у міжнародних тендерах сильно залежить від того, чи відповідає компанія технічним вимогам і стандартам, що включені в умови тендеру. Якщо це міжнародні стандарти, то рівні умови для учасників тендера гарантуються в принципі. Решта переваг, які фірма отримує у разі успішного впровадження системи екологічного менеджменту, що відповідає вимогам стандартів серії ISO 14000, можна звести в наступний список:

1. Можливість отримання міжнародного сертифікату екологічної відповідності. Сертифікація по ISO 14000 є однією з неодмінних умов маркетингу продукції на міжнародних ринках. Стандартний процес сертифікації займає від 12 до 18 місяців. Стільки ж займає впровадження на підприємстві системи екологічного менеджменту.

2. Поліпшення іміджу фірми у сфері виконання природоохоронних вимог (у т.ч. природоохоронного законодавства). Зі зростанням обізнаності громадськості про екологічні проблеми, стає все більш очевидно, що довіра до екологічної діяльності організації починає відігравати значну роль у залученні покупців.

Наприклад, тепер екологічні аспекти організації зазвичай відображаються на етикетках та упаковці багатьох основних видів продукції. Хоча використання стандарту ISO 14001 не має на увазі, що дана продукція буде обов'язково екологічно чистою, але сам факт, що виробник або постачальник послуг намагається зменшити вплив своєї продукції або послуг на навколишнє середовище, може схилити споживача до купівлі саме у цього постачальника, а не у того, хто в цій області докладає мінімум зусиль і не проводить ніякої екологічної політики.

3. Економія енергії і ресурсів, у тому числі спрямовуються на природоохоронні заходи, за рахунок більш ефективного управління ними.

4. Збільшення оцінювальної вартості основних фондів підприємства.

5. Можливість виходу на ринки «зелених» продуктів.

6. Покращення системи управління підприємством.

7. Можливість залучення висококваліфікованої робочої сили.

8. Стандарти ISO 14000 важливі для розвитку торгівлі, оскільки якщо всі грають за одними і тими же правилами, то урядам важче знаходити приводи для виправдання протекціонізму.

9. Серед компаній існує стійка позитивна кореляція між високою екологічною ефективністю компанії та її прибутковістю і загальним благополуччям.

10. Наявність системи екологічного менеджменту допомагає компанії захистити себе від правової відповідальності, пов'язаної з порушенням навколишнього середовища.

У зв'язку з нанесенням шкоди довкіллю можливе настання адміністративної, цивільної та кримінальної відповідальності. Екологічні організації і профспілки можуть «вхопитися» за будь-яке порушення та використовувати судовий процес і публічну критику для того, щоб утруднити, обмежити або затримати роботу компанії. Крім того, репутація порушника закону може призвести до затримування у видачі органами влади дозволів і ліцензій, а також до більш ретельної перевірки діяльності організації контролюючими органами. Екологічні аварії та інші випадки, що завдають шкоди навколишньому середовищу в цивілізованому суспільстві коштують дорого. Загалом, вважається, що приблизно 91 % усіх втрат можуть бути віднесені до недоліків системи управління, в тому числі і екологічного.

11. Поліпшуються умови фінансової захищеності компаній.

Наприклад, страхові компанії стали вимагати більш детальну інформацію про забруднення навколишнього середовища. Для банків-кредиторів існує прямий ризик потенційних збитків і зростає кредитний ризик у кредитуванні тих компаній, які завдають шкоди навколишньому середовищу. За наявності на об'єкті хорошої системи екологічного менеджменту можна уникнути значної кількості екологічних подій або аварій. Негаразди компанії у сфері охорони навколишнього середовища як правило призводить до збільшення страхових внесків.

12. Зниження витрат, збільшення прибутку. Правильно розроблена система екологічного менеджменту дозволяє ефективно знаходити можливості зниження витрат – вона стимулює управлінські та технологічні інноваційні рішення, знижує загальну собівартість продукції або підвищує її цінність. Ці поліпшення дозволяють компаніям продуктивніше використовувати ресурси на вході: від сировини і енергії, до трудових ресурсів. Таким чином, компенсуються витрати на зменшення впливу на навколишнє середовище.

13. Збільшення конкурентоспроможності.

Забруднення навколишнього середовища часто представляє собою форму економічного марнотратства. Коли відходи і шкідливі речовини, що утворюються у процесі виробництва, вироблення електроенергії, надання послуг, викидаються у навколишнє середовище у вигляді забруднення, це ознака того, що ресурси використовуються не повністю або неефективно. У цьому випадку організаціям доводиться прикладати додаткові зусилля, які збільшують витрати, але не створюють додаткової вартості для споживачів, наприклад зусилля з видалення забруднюючих речовин. Неефективність використання ресурсів в організації найбільш очевидна у разі неповної утилізації матеріалів і поганого управління технологічними процесами, що веде до зайвих відходів, дефектів та складування матеріалів.

Основними перевагами в конкурентній боротьбі, які одержує підприємство

при впровадженні системи екологічного менеджменту, є:

- економія матеріалів внаслідок більш повної обробки, заміщення, повторного використання компонентів продукції;
- збільшення виходу продукції;
- зменшення простоїв внаслідок більш ретельного моніторингу та технічного обслуговування;
- переробка відходів у комерційно значиму форму;
- зменшення енергоспоживання;
- зменшення витрат, пов'язаних з утилізацією відходів;
- поліпшення продукції в результаті змін у технологічному процесі;
- більш висока якість продукції;
- нижча вартість продукції (наприклад, внаслідок заміщення матеріалів);
- зниження вартості упаковки.

13. Мотивація співробітників. Впровадження системи екологічного менеджменту в організації часто призводить до поліпшення морального клімату в колективі і підвищенню мотивації співробітників.

Очевидно, що ISO 14000 висуває вимоги швидше до самої системи екологічного менеджменту. Обов'язковим є поступове, поетапне, але не постійне покращення функціонування цієї системи. Це є безсумнівною перевагою ISO 14000 перед традиційними стандартами, але приховує у собі також ряд небезпек:

- підприємство може бути сертифіковане за ISO 14000, навіть якщо його технологічні системи та організаційні заходи не забезпечують власне зменшення впливу на навколишнє середовище;
- стандарти створюють сприятливі умови для «експорту забруднень» – перенесення шкідливих виробництв у країни, що розвиваються. Компанія може бути сертифікована у країні, що розвивається, відповідаючи набагато м'якшим національним нормативам. Сертифікацію у цих країнах може полегшити позитивне ставлення до великих іноземних інвесторів, а також розвинена корупція;
- надмірна гнучкість стандартів – підприємство-забруднювач може, знижуючи свої викиди на мізерну величину, тим не менш, формально відповідати вимогам стандарту. Іноді висловлюється думка, що ISO 14000 з його повною відсутністю кількісних вимог взагалі не може вважатися стандартом;
- екологічна політика, будучи єдиним документом, що доступний громадськості, носить занадто загальний характер.

З метою підвищення конкурентоспроможності вітчизняних підприємств на світовому ринку Держстандарт України розробив національні стандарти на основі стандартів серії ISO 14000. Вони набрали чинності в Україні з 1998р., як добровільні стандарти у сфері управління навколишнім середовищем.

Таблиця 2.1.

Стандарти сфері екологічного управління, що діють в Україні

Група	Міжнародний стандарт	Національний стандарт
Системи екологічного менеджменту	ISO 14001:1996. Системи екологічного менеджменту. Специфікація і настанови із застосування	ДСТУ ISO 14001-97 Система управління навколишнім середовищем. Склад та опис елементів і настанови щодо їх застосування (не чинний з 01.01.2007 р.)
	ISO 14001:2004. Системи екологічного менеджменту. Вимоги і настанови із застосування	ДСТУ ISO 14001:2006 Системи екологічного управління. Вимоги та настанови щодо застосування (чинний з 15.05.2006 р.)
	ISO 14004:1996. Системи екологічного менеджменту. Загальне керівництво щодо принципів, систем і методів (скасований ISO)	ДСТУ ISO 14004-97 Системи екологічного управління. Загальні настанови щодо принципів, систем та засобів забезпечення (не чинний з 01.01.2007 р.)
	ISO 14004:2004. Системи екологічного менеджменту. Загальне керівництво щодо принципів, систем і методів	ДСТУ ISO 14004:2006 Системи екологічного управління. Загальні настанови щодо принципів, систем та засобів забезпечення (чинний з 01.07.2006 р.)
Екологічний аудит і екологічна оцінка	ISO 14015:2001. Екологічний менеджмент. Екологічна оцінка площадок і організацій	ДСТУ ISO 14015:2005 Екологічне керування. Екологічне оцінювання виробничих об'єктів та організацій
	ISO 19011:2002. Керівництво з аудиту якості і екологічного аудиту	ДСТУ ISO 19011-2003 Настанови щодо здійснення аудитів систем управління якістю та (чи) навколишнім середовищем
Екологічне маркування та декларування	ISO 14020:2000. Екологічні маркування і декларування. Загальні принцип	ДСТУ ISO 14020-2003. Екологічні маркування та декларації. Загальні принципи
	ISO 14021:1999. Екологічні маркування і декларації – Само-декларуючі екологічні заяви (екологічне маркування типу II)	ДСТУ ISO 14021-2002. Екологічні маркування та декларації. Екологічні самодекларації (екологічне етикетування типу II)
	ISO 14024:1999. Екологічні маркування і декларації – Екологічне маркування типу I – Принципи та процедури	ДСТУ ISO 14024-2002. Екологічні маркування та декларації. Екологічне етикетування типу I. Принципи та методи
	ISO/TR 14025:2000. Екологічні маркування і декларації – Екологічні декларації типу III (скасований ISO)	ДСТУ ISO/TR 14025-2002. Екологічні маркування і декларації. Екологічні декларації типу III
	ISO 14025:2006. Екологічні маркування і декларації – Екологічні декларації типу III – Принципи і процедури	ДСТУ ISO/TR 14025:2002 Екологічне маркування та декларації. Екологічні декларації типу III
Оцінка екологічної результативності	ISO 14031:1999. Екологічний менеджмент. Оцінка екологічної результативності. Керівництво	ДСТУ ISO 14031:2004 Екологічне керування. Настанови щодо оцінювання екологічної характеристики
	ISO 14031:1999. Екологічний менеджмент. Оцінка екологічної результативності. Керівництво	ДСТУ ISO 14031:2004 Екологічне керування. Настанови щодо оцінювання екологічної характеристики
	ISO/TR 14032:1999. Екологічний менеджмент. Приклади оцінки екологічної результативності	ДСТУ ISO/TR 14032:2004 Екологічне керування. Приклади оцінювання екологічної характеристики

Продовження табл. 2.1.

Оцінка життєвого циклу продукції та послуг	ISO 14040:1997. Екологічний менеджмент – Оцінка життєвого циклу – Принципи і структура (скасований ISO)	ДСТУ ISO 14040:2004 Екологічне керування. Оцінювання життєвого циклу. Принципи та структура
	ISO 14040:2006. Екологічний менеджмент – Оцінка життєвого циклу – Принципи і структура	Немає
	ISO 14041:1998. Екологічний менеджмент – Оцінка життєвого циклу – Визначення мети і області дослідження, інвентаризаційний аналіз	ДСТУ ISO 14041:2004 Екологічне керування. Оцінювання життєвого циклу. Визначення цілі і сфери застосування інвентаризації
	ISO 14042:2000. Екологічний менеджмент – Оцінка життєвого циклу – Оцінка впливу життєвого циклу	Немає
	ISO 14043:2000. Екологічний менеджмент – Оцінка життєвого циклу – Інтерпретація життєвого циклу	Немає
	ISO 14044:2006. Екологічний менеджмент – Оцінка життєвого циклу – Принципи і настанови	Немає
	ISO/TR 14047:2003. Екологічний менеджмент – Оцінка життєвого циклу – Приклади застосування стандарту ISO 14042	Немає
	ISO/TS 14048:2002. Екологічний менеджмент – Оцінка життєвого циклу – Формат документування даних з оцінки життєвого циклу	Немає
	ISO/TR 14049:2000. Екологічний менеджмент – Оцінка життєвого циклу – Приклади застосування стандарту ISO 14041 для визначення мети і області дослідження, а також інвентаризаційного аналізу	ДСТУ ISO/TR 14049:2004 Екологічне керування. Оцінювання життєвого циклу. Приклади використання ISO 14041 для визначення цілі і сфери застосування та аналізування інвентаризації
Словник	ISO 14050:1998. Екологічний менеджмент – Словник (скасований ISO)	ДСТУ ISO 14050:2004 Екологічне керування. Словник термінів
	ISO 14050:2002. Екологічний менеджмент – Словник	Немає

Тема 3: «ІНСТРУМЕНТИ ЕКОЛОГІЧНО ЗОРІЄНТОВАНОГО УПРАВЛІННЯ ПІДПРИЄМСТВОМ»

1. ЕКОЛОГІЧНА СЕРТИФІКАЦІЯ ЯК ІНСТРУМЕНТ ЕКОЛОГІЧНОГО УПРАВЛІННЯ

У світовій практиці екологічну сертифікацію почали запроваджувати з 1992 р. на основі Директиви 92/880/ЕС «Про екологічні знаки», британського стандарту BS 7750 «Система екологічного управління», міжнародних стандартів ISO/TC207 «Управління навколишнім середовищем» тощо. Поступ України до єдиного ринку стає додатковим чинником у формуванні тенденцій щодо вимог стосовно якості, конкурентоспроможності та безпеки пропонованих продукції, послуг та діяльності об'єктів управління ДСЕУ (державна система екологічного управління).

Нині недостатньо декларувати «якість» і «безпеку»: треба мати їх об'єктивні докази. Отримання таких доказів здійснюється через незалежну сертифікацію.

Сертифікація – це процедура підтвердження відповідності, за допомогою якої незалежна від виробника (продавця, виконавця) і споживача (покупця) організація засвідчує у письмовій формі, що продукція, процес або послуга відповідає встановленим вимогам.

Впровадження екологічної сертифікації ставить за мету розв'язання нагальних завдань у трьох сферах діяльності держави.

1. У сфері функціонування господарського комплексу:

- реалізація обов'язкових екологічних вимог природоохоронного законодавства під час ведення господарської діяльності;
- впровадження систем екологічного менеджменту;
- створення екологічно безпечних виробництв, технологічних процесів і обладнання;
- додержання вимог екологічної безпеки і запобігання забрудненню довкілля під час розміщення, переробки, транспортування, ліквідації й захоронення відходів виробництва і споживання;
- додержання вимог екологічної безпеки впродовж усього життєвого циклу будь-якої продукції;
- запобігання ввезенню в Україну екологічно небезпечних продукції, відходів, технологій і послуг.

2. У сфері інтеграції України до Європейського союзу:

- сприяння інтеграції економіки країни в Європейський ринок;
- гармонізація системи екологічної сертифікації з міжнародними й національними системами акредитації та сертифікації;
- підвищення конкурентоспроможності вітчизняної продукції;

- усунення технічних бар'єрів у міжнародній торгівлі;
- надання екологічному сертифікату й екологічному знаку відповідності статусу документів, які в особі уповноваженого органу державної влади з екологічної сертифікації гарантують додержання вимог природоохоронного законодавства України.

3. У сфері міжнародного співробітництва в галузі охорони навколишнього природного середовища:

- сприяння участі України у формуванні світового механізму охорони навколишнього природного середовища;
- забезпечення виконання Україною міжнародних угод, конвенцій та договорів у природоохоронній галузі;
- виконання міжнародних зобов'язань України у сфері управління якістю навколишнього природного середовища;
- забезпечення контролю за транскордонним переміщенням забруднювальних речовин та перевезенням небезпечних відходів.

Особливість системи екологічної сертифікації полягає у тому, що ця система ставить за мету забезпечити захист не тільки споживачів від недоброякісної й небезпечної продукції, а й самого навколишнього середовища від шкідливого впливу як цієї продукції, так і деструктивної діяльності людини. Тому саме для екологічної сертифікації набуває особливого значення розподіл сфер «обов'язковості» і «добровільності», інтересів національної безпеки і ринкових інтересів у визначенні структури цієї системи та правил її функціонування.

За своїм характером будь-яка сертифікація може бути обов'язковою або добровільною.

1. Згідно із стандартом ДСТУ 3410-96 «Система сертифікації УкрСЕПРО», **обов'язкова сертифікація** проводиться на відповідність об'єкта сертифікації вимогам чинних законодавчих актів України та обов'язковим вимогам нормативних документів міжнародних і національних стандартів інших держав, що діють в Україні. Обов'язкова сертифікація є формою державного контролю за безпекою продукції в ДСЕУ і повинна проводитись у законодавчо регульованій сфері.

2. Добровільна сертифікація проводиться на відповідність усім необхідним споживацьким вимогам, що не віднесені до обов'язкових, на договірних засадах між заявником та органом із сертифікації. Добровільна сертифікація проводиться в законодавчо нерегульованій сфері і може здійснюватися як у державній, так і в недержавній системах сертифікації.

Сертифікацію у недержавній сфері, на відміну від державної, може проводити як вітчизняний орган із сертифікації, так і представництво закордонного органу із сертифікації.

Зазначимо, що в Європейському союзі переважає добровільна сертифікація. Для України, з огляду її загального екологічного стану, існує потреба в посиленому державному управлінні в галузі екологічної безпеки й контролю за

додержанням екологічних вимог. Саме цей чинник наголошує на першочерговому значенні для нашої держави обов'язкової екологічної сертифікації.

Для державної системи сертифікації можна визначити такі *об'єкти обов'язкової екологічної сертифікації*:

- системи управління охороною навколишнього середовища, регламентовані міжнародними стандартами, що розробляються в технічному комітеті ISO/TC207 «Управління охороною навколишнього середовища», у якому Україна бере участь;
- продукція, шкідлива для навколишнього середовища, включаючи озоноруйнівні речовини й продукція, що їх містить, передбачувані до ввозу в Україну і вивозу з України, а також товари, увезені на митну територію України;
- екологічно шкідливі технології, включаючи ті, що ввезені на митну територію України і використовуються на промислових і дослідно-експериментальних об'єктах підприємств і організацій оборонних галузей промисловості;
- відходи виробництва і споживання, включаючи небезпечні й інші відходи, які є об'єктом транскордонного перевезення, і діяльність у сфері поводження з відходами;
- види тварин і рослин, їхні частини або деривати, що підпадають під дію Конвенції про міжнародну торгівлю видами дикої фауни і флори, які знаходяться під загрозою зникнення, здобуті у відкритому морі суднами під прапорами України.

При позитивних результатах перевірки органи із сертифікації видають заявникам екологічні сертифікати встановленого зразка і дозвіл на право маркування об'єктів сертифікації екологічним знаком відповідності.

Процедура сертифікації:

1. Подання заявки. Для проходження сертифікації системи екологічного управління (СЕУ) заявник повинен заповнити заявку встановленого зразку та надати її разом з підтверджуючою документацією, переліченою у формі заявки, на розгляд до органу сертифікації (далі – ОС).

Заявка та кожен документ до неї повинен бути підписаний керівником, завірений надписом «копія вірна» та печаткою підприємства.

Номер та дата реєстрації заявки заповнюється органом сертифікації (ОС).

2. Попереднє оцінювання (передсертифікаційний аудит). Передсертифікаційний аудит не є обов'язковою стадією сертифікаційного аудиту і проводиться виключно на прохання замовника. Його мета – проведення загального обстеження СЕУ замовника та визначення областей, де є або потенційно можуть бути невідповідності до стандарту.

Передсертифікаційний аудит включає аналіз документації СЕУ та аудит підрозділів організації замовника.

3. Первинний сертифікаційний аудит. Відповідно до вимог ДСТУ ISO 14001:2006, ISO/IEC 17021:2011 первинний сертифікаційний аудит СЕУ

замовника здійснюється у два етапи:

Етап 1 (початковий аудит). Мета цього аудиту – пересвідчитися у тому, що організація має документально оформлену СЕУ, що відповідає вимогам ДСТУ ISO 14001:2006 і провести планування головного аудиту на підставі даних про СЕУ та визначення ступеня готовності організації до головного аудиту. На цьому етапі здійснюється аналізування документів. ОС може виконувати роботи за цим етапом на місці розташування Замовника з тим, щоб краще оцінити адекватність СЕУ сфері діяльності організації. Виконання робіт на цьому етапі необхідне для:

- планування та виділення ресурсів, що необхідні для проведення етапу 2;
- забезпечення можливості зручного оперативного обміну інформацією з організацією Замовника;
- збирання необхідної інформації щодо процесів та місць(я) розташування організації;
- погодження з організацією деталей головного аудиту (етап 2).

Зокрема, під час першого етапу аудиту:

- оцінюється документація СЕУ;
- перевіряється розуміння Замовником вимог стандарту ДСТУ ISO 14001:2006;
- перевіряється планування цілей в області СЕУ;
- перевіряється відповідність області сертифікації, вказаній у заявці;
- оцінюється система внутрішніх аудитів;
- перевіряється звіт вищого керівництва з аналізу функціонування СЕУ.

Етап 2 (головний аудит). Роботи на цьому етапі проводяться на місці розташування організації. Ці роботи полягають у проведенні головного аудиту з метою оцінювання впровадження СЕУ організації.

Упродовж 2-го етапу аудиту перевіряються:

- відповідність СЕУ вимогам стандарту ДСТУ ISO 14001:2006, законодавчим та іншим нормативним документам;
- впровадження моніторингу процесів, цілей та задач в області екологічного управління;
- наявність операційного контролю за процесами відповідно до діючих процедур та інструкцій;
- обов’язки вищого керівництва щодо впровадження політики в області СЕУ;
- компетентність персоналу;
- дієвість внутрішніх аудитів та аналізу СЕУ з боку вищого керівництва;
- управління процесами аутсорсингу.

Група аудиторів складає та надає замовникові звіт з аудиту, в якому містяться результати аудиту та галузь сертифікації, а також, у разі необхідності, погоджений характер коригуючих дій.

Аудитори виписують лише ті невідповідності, усунення яких покращує СЕУ замовника.

4. Видача сертифіката. Тільки після усунення невідповідностей та

виконання усіх коригуючих дій, погоджених із замовником, підписується акт здавання-приймання робіт та видається сертифікат.

2. ЕКОЛОГІЧНЕ МАРКУВАННЯ

2.1. СУТНІСТЬ ТА КРИТЕРІЇ ЕКОЛОГІЧНОГО МАРКУВАННЯ

Виробники та продавці використовують певний набір «комунікативних інструментів» для того, щоб вплинути на поведінку споживачів. Найбільш очевидним комунікативним інструментом є ціна. При наявності вибору споживачі намагаються купувати товари за нижчою ціною. Крім ціни, торговельні знаки можуть виконувати комунікативну функцію.

Однією з причин використання екологічного маркування є привернення уваги екологічно свідомих покупців і «захоплення» за рахунок цього додаткової частки ринку. Якщо продукція компанії відповідає певним екологічним вимогам і, на думку компанії, екологічне маркування певного виду продукції дозволить їй підвищити рівень продажів, то, цілком ймовірно, компанія зважиться на екологічне маркування даної продукції. Таким чином, екологічні етикетки можуть забезпечити успіх одним компаніям, але негативно позначитися на інших.

З точки зору покупців екологічне маркування продукції задовольняє запити екологічно свідомих споживачів в екологічно чистих товарах. У деяких країнах число покупців, які вибирають товари з екологічними етикетками, становить значну частину від загальної кількості покупців.

У ряді країн екологічні етикетки виявилися, без сумніву, ефективним інструментом для стимулювання споживчого попиту і для руху ринку споживчих товарів в бік більшої екологічної стійкості.

Еко-маркування – один з видів екологічної декларації, що характеризує вплив продукції або послуги на навколишнє середовище на всіх стадіях життєвого циклу.

Існує два основних поняття еко-маркування: загальне змістове та маркетингове.

- **Загальне змістове поняття** включає в себе маркування, яке відображатиме весь комплекс відомостей у вигляді тексту, окремих графічних, колірних символів (умовних позначень) та їх комбінацій, який використовується з метою охорони навколишнього середовища.
- **Маркетингове поняття** включає в себе ту частину загального, яка становить сукупність інформації про суб'єктів господарської діяльності, які процеси ними використовуються, їх продукцію та послуги, спрямовані на забезпечення споживачів (користувачів) достовірною інформацією про екологічність даного об'єкту, і застосовується добровільно для формування таким чином сталого споживчого попиту на екологічні товари і на основі цього сприяє розробці, виробництву та використанню виробів, які меншою мірою негативно

впливають на навколишнє середовище протягом всього свого життєвого циклу.

Поява і застосування еко-маркування (еко-заяв) було обумовлено:

- зростанням чутливості людей до проблем збереження середовища проживання і готовності у міру можливості особисто сприяти цьому процесу;
- прагненням суспільства до формування стійкого споживчого попиту на екологічні товари;
- можливістю використання, в тій чи іншій мірі, екологічних характеристик виробничих процесів, продукції та послуг підприємцями в якості основного або додаткового фактора конкурентної боротьби на ринку товарів і послуг.

Щоб отримати еко-маркування, дана продукція повинна пройти сертифікацію, тобто експертну перевірку на відповідність нормативно встановленим еко-критеріям для цієї продукції.

Екологічні критерії, еко-критерії – вимоги екологічності, яким повинна відповідати продукція , щоб їй було присвоєне екологічне маркування.

Екологічне маркування є функцією екологічного менеджменту і поділяється на:

а) *обов'язкове* (нанесення якого передбачене законодавством України);

б) *добровільне* (регулюється державними стандартами України).

Обов'язкове екологічне маркування наноситься згідно з чинним законодавством для інформування про відповідність продукції екологічним вимогам (національний знак відповідності) чи про екологічну небезпеку певної продукції (вантажу).

Наприклад, відповідно до постанови Кабінету Міністрів України «Питання обігу харчових продуктів, що містять генетично модифіковані організми та/або мікроорганізми» від 1 серпня 2007 року № 985, з 1 листопада 2007 року в Україні впроваджується обов'язкове спеціальне маркування харчових продуктів, що містять ГМО у кількості більш як 0,9 %. Законодавство про перевезення небезпечних вантажів регулює порядок екологічного маркування таких вантажів.

2.2. ТИПИ ЕКОЛОГІЧНОГО МАРКУВАННЯ

Існуюче еко-маркування умовно можна розділити на кілька основних груп.

За предметною ознакою:

➢ *інформація про екологічність* (нешкідливість для навколишнього середовища) предметів (товару, процесу або виробничої системи) в цілому або їх окремих властивостей:

- знаки на аерозольних препаратах, що відображають відсутність речовин, що призводять до руйнування озонового шару навколо Землі;
- знаки на предметах вжитку (в основному, на предметах із пластиків і частіше – поліетилену), що відображають можливість їх утилізації з

найменшою шкодою для навколишнього середовища, та ін.;

- спеціальне маркування матеріалів, зокрема, пакувальних, у рамках заходів щодо поводження з відходами, яка, в принципі, спрямована на заощадження ресурсів і охорону природи;
- знаки для матеріалів (наприклад, упаковки), які можуть бути піддані вторинній переробці (іноді в рамках спеціальних програм);

➢ *маркування, яке вказує на мінімізацію впливу виробничих процесів підприємства на навколишнє середовище* або на успішне проходження сертифікації (реєстрації) системи управління навколишнім середовищем на підприємстві на відповідність міжнародними стандартами ISO серії 14000. Це вказує на турботу виробника про охорону навколишнього середовища, але не має прямого відношення до екологічності виробленої продукції і відповідно до вимог ISO повинно застосовуватися у формах, що не вводять споживачів в оману щодо екологічності товару;

➢ *інформація про натуральність* або органічне походження продукції (використовуваних сировини і процесів виготовлення;

➢ *інформація щодо підтримки і пропаганди природоохоронних дій*, куди відносяться заклики берегти природу, допомагати природоохоронним організаціям тощо;

➢ *інформація про можливу шкоду для навколишнього середовища* і шляхи його запобігання. До складу маркування небезпечних речовин, матеріалів та пов'язаних з ними виробів, яка використовується на міжнародному та європейському рівнях, входять окремі знаки, що відображають небезпеку предмета для навколишнього середовища.

Прикладами таких знаків можуть служити:

- спеціальний знак для позначення речовин, які становлять небезпеку для морської флори і фауни, при їх перевезенні по водних шляхах;
- знак «Небезпечно для навколишнього середовища», що використовується у рамках законодавства ЄС про класифікацію, пакування та маркування небезпечних речовин і препаратів;
- знак, який вказує на необхідність окремого збору використаних джерел живлення (батарейок та акумуляторів), що містять деякі небезпечні речовини, наприклад, ртуть, кадмій, свинець. На додаток (де необхідно) наводиться вид речовини і вказівка на вторинну переробку.

За видом декларування:

➢ *екологічне маркування типу I* (повинен відповідати вимогам міжнародного стандарту ISO 14024 (ДСТУ ISO 14024)): надання за результатами перевірки третьою стороною (органом екологічного маркування) права на нанесення знаку екологічного маркування, що підтверджує загальну екологічну перевагу продукції (видається сертифікат і ліцензія на використання знаку екологічного маркування);

➢ *екологічне маркування типу II* (повинен відповідати вимогам міжнародного стандарту ISO 14021 (ДСТУ ISO 14021)): самомаркування, тобто

підприємство саме маркує свою продукцію за результатами власних досліджень.

Прикладом екологічного маркування ІІ типу можуть бути таки декларації, як: «вміст повторно переробленого матеріалу», «придатний для повторного перероблення», «придатний для компостування», «розбірна конструкція» тощо або спеціальні знаки, які визначені міжнародним стандартом ISO 7000;

➢ *екологічне маркування типу ІІІ* (повинен відповідати вимогам міжнародного стандарту ISO 14025 (ДСТУ ISO 14025)): нанесення кількісної інформації про екологічний вплив продукції протягом її життєвого циклу за результатами незалежної перевірки органом сертифікації чи незалежним експертом.

Екологічне маркування типу ІІІ, як і екологічне маркування типу І здійснюється на підставі висновку третьої сторони, але екологічне маркування типу ІІІ передбачає не просто нанесення знаку екологічного маркування, що свідчить про загальну екологічну перевагу продукції, а надання кількісної інформації про екологічний вплив продукції протягом усього її життєвого циклу. Відтак, екологічне маркування типу ІІІ вважається найбільш інформативним, хоча адресоване більше технічним спеціалістам, ніж споживачам.

2.3. ЕКОЛОГІЧНИЙ ЗНАК В УКРАЇНІ

Знак екологічного маркування визначає екологічну перевагу та безпеку маркованої ним продукції відносно іншої, аналогічного призначення, представленої на ринку.

Український знак екологічного маркування зображує стилізованого під зелений паросток журавлика на фоні Землі, і символізує життя на нашій планеті. За більше, ніж 10 років свого існування, в народі він отримав назву «Зелений журавлик».

Надпис по колу знаку «екологічний сертифікат» вказує на те, що позначена ним продукція сертифікована. Код екологічного стандарту «СОУ ОЕМ 001» вказує на порядковий номер екологічних критеріїв на певну категорію продукції.

Знак екологічного маркування належить екологічній сертифікаційній системі, його логотип зареєстрований Міністерством юстиції України, свідоцтво № 444 від 18.02.2002 року, права охороняються Законом.

В Україні екологічне маркування добровільне. Його застосування регламентується технічним регламентом з екологічного маркування і національним стандартом ДСТУ ISO 14024.

Технічний регламент з екологічного маркування обмежує використання екологічних тверджень, які є нечіткими чи неконкретними, які вважаються такими, що вводять в оману або лише натякають на те, що продукція є екологічно сприятливою чи екологічно безпечною. Забороняється використовувати подібні декларації або твердження ні на упаковці, етикетці, ні в рекламі товарів та

послуг.

За вимогами цього Технічного регламенту товаровиробники не повинні використовувати такі неперевірені екологічні твердження, як «екологічно чистий» «екологічно безпечний», «екологічно сприятливий», «сприятливий до ґрунту», «не забруднюючий», «зелений», «сприятливий до природи» та «сприятливий до озону» тощо.

Екологічне твердження «вільний від...» дозволяється робити лише у випадку, коли рівень зазначеної речовини не перевищує фонового рівня.

З січня 2014 року згідно пункту 42 Технічного регламенту з екологічного маркування суб'єкт господарювання має право розміщувати екологічне маркування на продукції тільки з обов'язковим зазначенням реєстраційного номера екологічного сертифікату.

3. *ЕКОЛОГІЧНИЙ АУДИТ У СИСТЕМІ ЕКОЛОГІЧНОГО УПРАВЛІННЯ*

Екологічний аудит – це документально оформлений системний незалежний процес оцінювання об'єкта екологічного аудиту, що включає збирання і об'єктивне оцінювання доказів для встановлення відповідності визначених видів діяльності, заходів, умов, системи екологічного управління та інформації з цих питань вимогам законодавства України про охорону навколишнього природного середовища та іншим критеріям екологічного аудиту.

Об'єктами екологічного аудиту є:

- підприємства, установи та організації, їх філії та представництва чи об'єднання, окремі виробництва, інші господарські об'єкти;
- системи екологічного управління;
- інші об'єкти.

Суб'єктами екологічного аудиту є:

- замовники;
- виконавці екологічного аудиту.

Докази екологічного аудиту – це документально зафіксована інформація щодо діяльності об'єкта екологічного аудиту, яка може бути перевірена.

Висновок екологічного аудиту – професійна оцінка об'єкта екологічного аудиту, виконана екологічним аудитором, яка ґрунтується на доказах екологічного аудиту та є головною складовою звіту про екологічний аудит.

Висновок екологічного аудиту є офіційним документом, який засвідчується підписом та печаткою екологічного аудитора.

Основними завданнями екологічного аудиту є:

- збір достовірної інформації про екологічні аспекти виробничої діяльності об'єкта екологічного аудиту та формування на її основі висновку екологічного аудиту;
- встановлення відповідності об'єктів екологічного аудиту вимогам

законодавства про охорону навколишнього природного середовища та іншим критеріям екологічного аудиту;

- оцінка впливу діяльності об'єкта екологічного аудиту на стан навколишнього природного середовища;
- оцінка ефективності, повноти і обґрунтованості заходів, що вживаються для охорони навколишнього природного середовища на об'єкті екологічного аудиту.

Екологічний аудит проводиться у процесі приватизації об'єктів державної власності, іншої зміни форми власності, зміни конкретних власників об'єктів, а також для потреб екологічного страхування, в разі передачі об'єктів державної та комунальної власності в довгострокову оренду, в концесію, створення на основі таких об'єктів спільних підприємств, створення, функціонування і сертифікації систем екологічного управління, а також здійснення господарської та іншої діяльності.

Екологічний аудит в Україні може бути добровільним чи обов'язковим.

Добровільний екологічний аудит здійснюється стосовно будь-яких об'єктів екологічного аудиту на замовлення заінтересованого суб'єкта за згодою керівника чи власника об'єкта екологічного аудиту.

Обов'язковий екологічний аудит здійснюється на замовлення заінтересованих органів виконавчої влади або органів місцевого самоврядування щодо об'єктів або видів діяльності, які становлять підвищену екологічну небезпеку, відповідно до переліку, що затверджується Кабінетом Міністрів України, у таких випадках:

- банкрутство;
- приватизація, передача в концесію об'єктів державної та комунальної власності, крім визначених законом випадків;
- передача або придбання в державну чи комунальну власність;
- передача у довгострокову оренду об'єктів державної або комунальної власності;
- створення на основі об'єктів державної та комунальної власності спільних підприємств;
- екологічне страхування об'єктів;
- завершення дії угоди про розподіл продукції відповідно до закону;
- в інших випадках, передбачених законом.

Екологічний аудит поділяється на внутрішній та зовнішній.

- *Внутрішній екологічний аудит* об'єкта проводиться на замовлення його власника чи органу, уповноваженого на управління ним, для власних потреб.
- *Зовнішній екологічний аудит* проводиться на замовлення інших заінтересованих суб'єктів.

Результати екологічного аудиту подаються у формі звіту про екологічний аудит.

Здійснення процедури еко-аудиту дозволяє:

1) оптимізувати фінансові витрати підприємства з врахуванням

екологічних факторів;

2) попередити випадки заподіяння шкоди, пов'язаної із забрудненням навколишнього середовища і нераціональним природокористуванням;

3) покращити взаємовідносини з природоохоронними органами і населенням;

4) добитися відповідних фінансових пільг, субсидій, корегування платежів за природокористування з врахуванням реального внеску підприємств-природокористувачів в оздоровлення навколишнього середовища;

5) перейти на всесвітньо визнані стандарти і процедури екологічного управління, що пов'язане з інтеграцією українських підприємств в систему світової економіки і міжнародної екологічної безпеки.

На даний час виділяють декілька типів еко-аудиту, що відрізняються колом цілей і проблем, що розглядаються:

- ***Аудит дотримання стандартів***: здійснюється за допомогою співставлення показників якості навколишнього середовища з однієї сторони і положень національних і міжнародних стандартів. ціль такого співставлення – визначення необхідних заходів, націлених на приведення екологічних характеристик даного підприємства до відповідності зі стандартом якості навколишнього середовища.
- ***Аудит відповідальності***: за результатами такого аудиту визначається ризик відповідальності за спричинену шкоду навколишньому середовищу.
- ***Аудит при екологічному страхуванню***: він здійснюється за умови підписання договору страхування, розроблення плану превентивних заходів зі зниження екологічних ризиків, в процесі оцінювання завданої шкоди, за умови настання страхового випадку чи розгляду позову до підприємств з приводу забруднення довкілля.
- ***Аудит в системі екологічної сертифікації***: здійснюється з метою оцінювання відповідності об'єктів сертифікації встановленим екологічним вимогам (стандартам, нормативам).
- ***Аудит території***: здійснюється з метою оцінювання екологічного стану території.
- ***Аудит при підготовці рішення про розділ продукції***: здійснюється з метою більш повного і детального вивчення з екологічної точки зору ймовірних об'єктів інвестування, включаючи дослідження надр, ресурсів рослинного і тваринного світу. До завдань аудиту входить також оцінка раніше завданої екологічної шкоди, вартість відновлення пошкоджених об'єктів навколишнього середовища, витрат на ліквідацію понаднормативних негативних дій на навколишнє середовище.

4. ЕКОЛОГІЧНА ЕКСПЕРТИЗА ЯК ІНСТРУМЕНТ ОЦІНЮВАННЯ АНТРОПОГЕННОГО ВПЛИВУ НА ДОВКІЛЛЯ

Всебічний екологічний аналіз та правильна, достовірна експертна оцінка проектів споруджуваних господарських об'єктів, комплексів та систем набувають принципово важливого значення, оскільки «людські проекти», що не враховують закони природи, приносять чимало лиха.

Важлива роль серед ефективних заходів протидії цьому належить екологічній експертизі.

Екологічна експертиза – це комплексний аналіз технологій, матеріалів, устаткування, техніки, проектів, планів, прогнозів та іншої документації, аналіз та оцінка результатів запланованої або існуючої господарської діяльності, що чинить чи може чинити негативний вплив на навколишнє природне середовище, який проводять висококваліфіковані спеціалісти-експерти для визначення відповідності поданих матеріалів чинному законодавству і розробки конструктивних пропозицій щодо охорони навколишнього середовища.

Екологічна експертиза спрямована на запобігання новим, обмеження або ліквідацію існуючим негативним джерелам впливу на оточуюче природне середовище та здоров'я населення.

Необхідність та процедура проведення екологічної експертизи визначені природоохоронним законодавством України. Здійснюється вона на підставі закону України «Про екологічну експертизу».

Екологічній експертизі підлягають:

- державні інвестиційні програми, програми розвитку окремих галузей народного господарства;
- проекти схем розвитку і розміщення продуктивних сил, розвитку галузей економіки, генеральних планів населених пунктів, схем районного планування, схем генеральних планів промислових вузлів, схем розміщення підприємств у промислових вузлах і районах, схем упорядкування промислової забудови, інша передпланова і передпроектна документація;
- інвестиційні проекти, техніко-економічні обґрунтування і розрахунки, проекти й робочі проекти на будівництво і реконструкцію (розширення, технічне переозброєння) підприємств та інших об'єктів, документація з перепрофілювання, консервації та ліквідації діючих підприємств, окремих цехів, виробництв та інших промислових і господарських об'єктів, що можуть негативно впливати на стан навколишнього середовища, незалежно від форм власності та підпорядкування, в тому числі військового призначення;
- проекти інструктивно-методичних і нормативно-технічних актів та документів, які регламентують господарську діяльність, що негативно впливає на навколишнє середовище;
- проекти законодавчих та інших нормативно-правових актів, що регулюють відносини в царині гарантування екологічної (в тому числі радіаційної) безпеки, охорони навколишнього природного середовища і використання природних ресурсів, діяльності, що може негативно впливати на стан навколишнього природного середовища та здоров'я людей;
- документація на створення нової техніки, технологій, матеріалів і речовин,

у тому числі та, що закуповується за кордоном, які можуть створювати потенційну загрозу навколишньому природному середовищу та здоров'ю людей;

- матеріали, речовини, продукція, господарські рішення, системи й об'єкти, впровадження чи реалізація яких може призвести до порушення норм екологічної безпеки та негативного впливу на навколишнє середовище чи створення небезпеки для здоров'я людей;
- екологічно небезпечні діючі об'єкти та комплекси, в тому числі військового та оборонного призначення.

Еколого-експертні оцінки реалізуються в еколого-експертних висновках та рекомендаціях, які підготовлюються еколого-експертними органами за результатами проведення експертизи. По проектах, які рекомендуються до затвердження, дається загальна екологічна оцінка проектних проробок, їх якості у відповідності до екологічних вимог, а також пропозиції, спрямовані на покращання природоохоронних розділів проектів, що проходять експертизу.

Наприклад, еколого-експертні органи, проводячи екологічну експертизу генерального плану та проекту планування приміської зони курорту Хмільник дійшли до висновку, що проектні рішення в цілому відповідають екологічним вимогам та враховують динаміку взаємозв'язків даної екологічної системи. В той же час проектувальникові рекомендується проробити, виходячи із місцевих умов екосистеми, питання комплексного використання ставків та водосховищ для задоволення потреб водозабезпечення, організації місць рекреації, ведення рибного господарства, організації спортивного та аматорського риболовства, а також передбачати можливість винесення із зони меблевої фабрики, що є основним джерелом забруднення курорту.

Було виявлено факти будівництва промислових об'єктів без позитивних висновків державної екологічної експертизи. Фінансування цих об'єктів припинено. Це – будівництво фабрики килимових виробів на ВАТ «Оріана», асфальто-бетонного заводу в м. Долині, молокозаводу в с. Казанів Коломийського району, лісопильного і меблевого виробництва в с. Черганівка Косівського району та ін.

Передбачено державну і громадську екологічну експертизу. За ініціативою заінтересованих осіб та організацій, а також за рішенням центральних або місцевих органів влади може проводитися додаткова незалежна екологічна експертиза.

➢ *Державна екологічна експертиза* являє собою урегульовану законом та іншими правовими нормами цілеспрямовану діяльність державних органів з розгляду, перевірки, аналізу, оцінки на основі екологічних знань представлених проектів на предмет їх відповідності нормам і правилам охорони навколишнього середовища, раціонального природокористування та вимогам екологічної безпеки, корегування екологічних параметрів та формулювання найоптимальніших варіантів природоохоронного та соціального захисту проектних рішень для запобігання негативного впливу проектованих об'єктів в процесі їх реалізації в конкретній екологічній системі.

➢ *Громадська екологічна експертиза* проводиться для врахування громадської думки щодо реалізації наміченої проектом господарської діяльності, її соціально-екологічних наслідків.

5. *ЕКОЛОГІЧНІ ІННОВАЦІЇ ЯК ЗАСІБ ЕФЕКТИВНОГО РОЗВИТКУ ПІДПРИЄМНИЦТВА*

У світі, побудованому на основі наших уявлень,
ще існують проблеми, які неможливо вирішити,
якщо мислити по-старому.
Альберт Енштейн

Наука і практика нововведень мають великі можливості поступової гармонізації виробничої діяльності людини до природного середовища в рамках сталого розвитку.

Екологічні інновації – це результат творчої діяльності, спрямованої на розробку, створення та впровадження нововведень у вигляді нової продукції, технологічного методу, форми організації виробництва й ін., які б прямо чи побічно сприяли зниженню екодеструктивного впливу виробництва і споживання на навколишнє середовище і вирішували б екологічні проблеми.

Більш повніше можна охарактеризувати екологічні інновації як результат творчої діяльності, спрямованої на:

- розробку, створення і впровадження нових технологічних процесів і технологічних циклів розробки і погодженого розвитку всіх функціональних ланцюжків по видобутку ресурсів, їхній переробці, використанню відходів і відтворенню цих ресурсів;
- розробку і застосування ресурсозберігаючої техніки і технологій;
- розробку і впровадження маловідхідних і безвідхідних технологій, у т.ч. енергозберігаючих;
- розробку технологій, що забезпечують комплексне використання сировини і природних ресурсів;
- розробку біотехнологій, наприклад, біотехнології очищення води від забруднюючих речовин і очищення стоків промислових і агропромислових підприємств, біотехнології очищення грунту, біотехнологічні методи еко-моніторингу (біосенсори, біотести) та ін.;
- освоєння нових територій, а також розширення діючих з врахуванням екологічної безпеки населення і виробництва;
- розробку і випуск нових екологічно чистих продуктів і створення потужностей для їх виробництва;
- розробку варіантів застосування нових і поновлюваних джерел енергії;
- розробку матеріалів з новими властивостями, що знижують навантаження на навколишнє середовище в результаті їхнього використання, переробки

й утилізації;

- впровадження нових організаційних форм, включаючи удосконалення організаційно-територіальної структури потенційно небезпечних виробництв із метою зниження їхньої небезпеки;
- формування нового мислення в розроблювачів нових технологій і продуктів з погляду екологізації виробничого устаткування шляхом впровадження екологічної освіти.

Інновації, як відомо, найчастіше виступають у формі інноваційних проектів, який охоплює весь цикл від виникнення нововведення до її практичної реалізації на ринку.

Під **еколого-інноваційними проектами** слід розуміти великі інноваційні проекти (програми), які прямо чи побічно вирішують загальнодержавні, галузеві, регіональні та підприємницькі екологічні проблеми.

Особливістю еколого-інноваційних проектів у порівнянні зі звичайними інноваційними проектами є в більшості випадків їх невисока економічна ефективність, поряд з високою екологічною ефективністю.

Екологічні інновації можна класифікувати за рядом ознак.

Залежно від сфер реалізації екологічні інновації поділяють на:

➢ *технічні* – нові екологічно безпечні й екологічно чисті продукти, мало- і безвідхідні технології, енергозберігаючі технології й екологічно чисті джерела енергії, нові конструкційні матеріали, що характеризуються високою екологічною безпекою їхньої переробки й утилізації, екологічно безпечне устаткування та ін.;

➢ *організаційні* – нові методи і форми організації усіх видів діяльності підприємств (їхніх об'єднань), спрямовані на зниження екологічної небезпеки виробництва;

➢ *соціальні* – різні форми активізації творчої активності в напрямку екологізації виробництва і споживання, включаючи: професійну підготовку і постійне підвищення кваліфікації персоналу на основі екологічної освіти, стимулювання його творчої діяльності в напрямку розробки екологічно безпечного устаткування і продукції, створення комфортних і екологічно безпечних умов життя і праці.

Класифікація інновацій за ступенем новизни:

1) з погляду їхньої значимості в економічному розвитку:

➢ *базисні інновації* (абсолютна новизна) – спрямовані на освоєння нових поколінь машин і матеріалів та засновані на принципово нових технологіях або на сполученні існуючих технологій у новому їхньому застосуванні. Такі інновації в історії виникали рідко, хоча на етапі прискорення НТП вони стали з'являтися частіше (прикладом може бути заміна двигуна внутрішнього згорання електричним двигуном на сонячних батареях; біоенергетика, що використовує енергію біомаси органічних відходів та ін.);

➢ *інновації, що поліпшують* (відносна новизна) – зазвичай, мають відношення до вже існуючого продукту, якісні чи вартісні характеристики якого були поліпшенні за рахунок використання більш ефективних компонентів і

матеріалів, частково зміни однієї чи ряду технічних підсистем (у випадку складного продукту). Ці інновації служать поширенню й удосконалюванню освоєних поколінь техніки, створенню нових моделей машин і матеріалів, поліпшенню характеристик вироблених товарів і технологій;

➢ *псевдоінновації* (умовна новизна, модернізація) – спрямовані на часткове поліпшення застарілих поколінь техніки і технології, вони не сприяють раціональному використанню природних ресурсів, розвитку НТП і лише частково запобігають забрудненню, що наноситься екологічно небезпечними технологіями виробництва і продуктами споживання (прикладом може бути застосування удосконалених очисних споруджень, фільтрів на вже діючому устаткуванні й у діючому виробництві);

2) за рангами новизни:

➢ *світові* (принципово нові з погляду світових зразків);

➢ *національні* (державні – з погляду національної економіки);

➢ *регіональні*;

➢ *галузеві*;

➢ *виробничо-господарські*.

Класифікація еко-інновацій за ступенем адаптованості до змін: *адаптовані* і *неадаптовані*.

Ефективними вважають еко-інновації, які приносять відповідний ефект. Це може бути:

- економічний (економія чи запобігання втрат природних ресурсів, живої й упредметненої праці в усіх сферах – виробничої, невиробничої, особистого споживання);
- екологічний (зниження чи запобігання негативного впливу на навколишнє середовище і поліпшення його стану виявляється в зниженні обсягів забруднень, збільшенні кількості придатних до використання природних ресурсів і виміряється в залежності від виду антропогенних порушень навколишнього середовища);
- соціальний (поліпшення умов життя, праці і відпочинку населення; зменшення захворюваності, збільшення тривалості життя, підвищення працездатності та ін.);
- науково-технічний (рівень і масштаб новизни, перспективність закладених в інновації принципів технології і технічного оснащення, відповідність сучасним технологічним вимогам в індустріально розвинених країнах);
- бюджетний (вплив еколого-інноваційного проекту на доходи (витрати) бюджету);
- інтегральний (сукупний ефект).

Тема 4: «СИСТЕМА ЕКОЛОГІЧНОГО МЕНЕДЖМЕНТУ ПІДПРИЄМСТВА»

1. *ПОНЯТТЯ СИСТЕМИ ЕКОЛОГІЧНОГО МЕНЕДЖМЕНТУ (СЕМ) ТА ЇЇ РОЛЬ У РОЗВИТКУ ПІДПРИЄМСТВА*

Екологічний менеджмент може здійснюватися на різних рівнях. До них відносяться державний, регіональний і локальний рівні. Під локальними звичайно розуміють рівень підприємств.

На державному та регіональному рівні екологічний менеджмент являє собою систему управління, в яку входять не тільки суб'єкти господарської діяльності (підприємства), але також і об'єкти, на які спрямована вплив господарюючих суб'єктів – атмосферне повітря, водні об'єкти, ґрунти та інші природні ресурси.

На сучасному етапі все більша роль у вирішенні екологічних проблем відводиться безпосередньо об'єктам економічного ринку – підприємствам, які відповідальні за свою виробничу діяльність. Тому система екологічного менеджменту має застосування насамперед на рівні підприємств і дозволяє їм вирішувати екологічні проблеми. Створення та впровадження на підприємстві такої системи дозволяє зберегти баланс між інтересами самого підприємства та вимогами природоохоронного законодавства.

Екологічний менеджмент підприємства є частиною загальної системи управління підприємством, що включає в себе організаційну структуру, планування, розподіл відповідальності, практичні методи, процедури, процеси і ресурси, необхідні для розробки, впровадження, реалізації, аналізу та розвитку природоохоронної діяльності підприємства.

Діюча система екологічного менеджменту дозволяє підприємству досягти, систематично контролювати і мінімізувати рівень екологічних впливів своєї господарської діяльності на навколишнє середовище. При цьому, як правило, спостерігаються зниження екологічних витрат і платежів за забруднення навколишнього середовища, економія сировини, енергії та інших матеріальних ресурсів, а також досягаються важливі нематеріальні вигоди для підприємства. Таким чином, системи екологічного менеджменту орієнтовані на задоволення потреб усього суспільства і навіть майбутніх поколінь.

Позитивні ефекти впровадження системи екологічного менеджменту на підприємстві:

- *структурні* – розвиток системи стратегічного управління, розвиток взаємодії між підрозділами, збільшення мотивації персоналу й розвиток системи його навчання;
- *ринкові* – пріоритет при взаємодії з міжнародними установами, компаніями та розвиток зовнішньої діяльності; формування ринку екологічних

товарів та послуг;

- *ризикові* – зниження вірогідності аварійних та позаштатних ситуацій, наслідків порушення законодавства;
- *ресурсні* – збільшення прибутку й стабільності виробництва за рахунок раціонального використання сировини та ресурсів;
- *природоохоронні* – зниження захворювання населення, підвищення ефективності праці, зниження виплат за негативний вплив на навколишнє природне середовище.

Базовим міжнародним стандартом в області екологічного менеджменту є стандарт ISO 14001:2004 «Environmental management system. Specification with guidance for use». В Україні цей стандарт відомий як ДСТУ ISO 14001:2006 «Системи екологічного управління. Вимоги та настанови щодо застосування». Він є єдиним офіційним міжнародним документом, що містить вимоги, виконання яких може бути перевірено за допомогою аудиту зовнішньою організацією для сертифікації. Відповідність стандартам ISO 14001:2004 та ДСТУ ISO 14001:2006 дозволяють створити систему управління охороною навколишнім середовищем, придатну для незалежної оцінки відповідності певним критеріям, підтвердженим сертифікатом, який засвідчує наявність належної системи управління охороною навколишнього середовища на підприємстві.

В основі функціонування СЕМ лежить спіраль (модель Демінга) повторюваних циклів, спрямованих на послідовне вдосконалення системи в цілому (рис. 4.1). Модель символізує вимоги до поліпшення стану навколишнього середовища і постійний підйом на більш високу ступінь.

З малюнка видно, що створення і вдосконалення СЕМ послідовно проходить кілька важливих етапів, кожен з яких вирішує певні завдання, вимагає різних ресурсів (матеріальних, фінансових, інформації, часу, фахівців, документів і т.д.), характеризується результативністю.

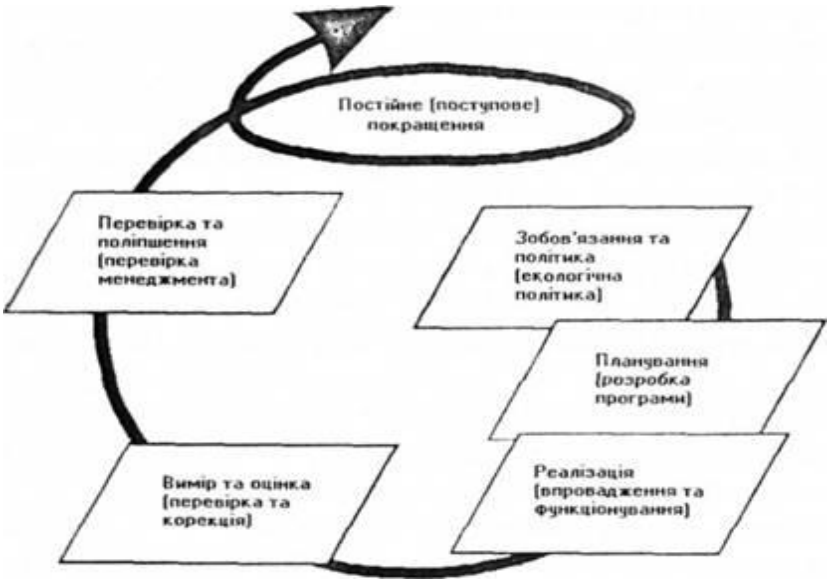


Рис. 4.1. Модель Демінга

Цілком очевидно, що ядром процесу є *впровадження*. Однак не менш значимі і попередні етапи. *Планування*, у результаті реалізації якого, ідентифікуються основні екологічні аспекти діяльності підприємства і з'являється детальна програма СЕМ. *Проведення перевірок та здійснення коригуючих дій* – етап, що дозволяє вчасно визначити і виправити помилки. *Оцінка ефективності СЕМ* полягає в останньому етапі спіралі – аналіз з боку керівництва, висновки якої використовуються для вдосконалення системи і окремих її елементів.

2. ПРОЦЕС ВПРОВАДЖЕННЯ СЕМ

Процес впровадження СЕМ на підприємстві відбувається послідовно у 5 етапів:

Назва етапу	**Опис дій**
I. Підготовчий	1. Прийняття попереднього рішення вищим керівництвом про впровадження СЕМ, визначення сфери охоплення планованої СЕМ і доцільності залучення консультанта. 2. Навчання фахівців впровадженню СЕМ, тим більше, якщо оцінка вихідної ситуації проводиться самим підприємством. 3. Оцінка вихідної ситуації: встановлення відповідності діючої системи екологічного управління вимогам ДСТУ ISO 14001:2006 (ISO 14001:2004), а також оцінка впливу на навколишнє середовище та виконання вимог природоохоронного законодавства, виявлення пріоритетних екологічних аспектів. 4. Створення робочої групи екологічного менеджменту. 5. Розробка програми (плану) впровадження СЕМ. 6. Розробка системи стандартів, що регламентують застосування процедур, пов'язаних з СЕМ.
II. Планування	7. Розробка екологічної політики, доведення її до персоналу підприємства та зацікавлених сторін. 8. Ідентифікація та виявлення пріоритетних екологічних аспектів діяльності. 9. Формування та ведення реєстру законодавчих актів та інших вимог, що пред'являються до природоохоронної діяльності. 10. Розробка цільових і планових екологічних показників, а також внутрішніх критеріїв ефективності. 11. Розробка програм природоохоронних заходів.
III. Впровадження та функціонування	12. Формування організаційної структури СЕМ. 13. Організація системи освіти. 14. Перегляд документації у зв'язку з впровадженням СЕМ і організація управління. 15. Організація системи обміну інформацією. 16. Підготовка до аварійних ситуацій.
IV. Контрольні та коригуючі дії	17. Організація моніторингу та вимірювань. 18. Проведення перевірок та розробка коригуючих дій. 19. Управління зареєстрованими даними. 20. Організація і проведення внутрішнього аудиту СЕМ.
V. Аналіз системи з боку керівництва	21. Аналіз системи з боку керівництва

І. Підготовчий етап:

➢ *Прийняття рішення з боку керівництва*. Приймаючи рішення на користь розробки та впровадження системи екологічного менеджменту, керівники виходять як з її переваг з фінансової точки зору (економія ресурсів і засобів, підвищення ефективності виробництва, розвиток потенційних можливостей на ринках), так і з точки зору зниження виникнення ризиків, пов'язаних з неадекватним ставленням до екологічних аспектів роботи підприємства, які система дозволить докорінно змінити (аварії; санкції регулюючих органів, труднощі в залученні нових, в першу чергу закордонних, інвесторів і клієнтів, в отриманні банківського кредиту, втрата ринків тощо).

Таким чином, основною умовою прийняття рішення про впровадження СЕМ вищим керівництвом компанії є розуміння того, що для збереження свого становища в бізнесі підприємству слід враховувати екологічні вимоги при формуванні стратегії і довгостроковому плануванні.

Рішення вищого керівництва може стосуватися як усього підприємства, так і його окремих підрозділів. При цьому впровадження СЕМ на окремих підрозділах здійснюється або для прискорення отримання сертифіката на виробництво певного виду продукції, або з метою реалізації пілотного проекту.

Після того, як керівництвом підприємства прийнято рішення про створення СЕМ відповідно до вимог міжнародних стандартів, необхідно зрозуміти, зможе підприємство впровадити самостійно дану систему або необхідно залучити консультантів.

➢ *Навчання фахівців впровадженню СЕМ*. Необхідність наявності в організації підготовленого персоналу з питань екологічного управління та організаційної структури визначається по-перше тим, що систему екологічного менеджменту необхідно підтримувати в робочому стані, постійно вдосконалювати, періодично пред'являти різним контролюючим органам, а також тим, що актуальність екологічних питань постійно зростає в роботі кожного – від вищого керівника до окремого робітника. Таким чином, обізнаність та компетентність усього персоналу – одне з ключових вимог стандарту ISO 14001.

Програмами навчання в області охорони навколишнього середовища та ресурсозбереження, повинні бути охоплені працівники всіх рівнів – вище керівництво, фахівці середньої ланки і робітники всіх спеціальностей. Така необхідність викликана тим, що на етапі створення і впровадження СЕМ весь персонал повинен усвідомити свою відповідальність за вплив його діяльності на навколишнє середовище.

Основні етапи навчання та компетенції персоналу – це визначення потреби в освіті, розробка програм, безпосередньо навчання (внутрішнє та зовнішнє) і оцінка ефективності навчання. Програма навчання складається за рівнями персоналу. Для цього за характером діяльності та рівнем відповідальності весь персонал поділяється на групи, для кожної з яких становлять конкретний план навчання.

Типові програми навчання повинні включати в себе наступні питання:

- загальна інформація про СЕМ, загальне уявлення про вимоги ДСТУ ISO 14001:2006;
- існуючий стан охорони навколишнього середовища на підприємстві;
- екологічні аспекти діяльності і впливу на навколишнє середовище;
- передбачувані переваги від впровадження СЕМ;
- характеристика основних елементів СЕМ;
- існуючі структури та підходи управління;
- плани впровадження СЕМ;
- ресурси, необхідні від підприємства для впровадження СЕМ;
- шляхи безперервного вдосконалення та підвищення ефективності СЕМ.

Такий підхід до підготовки та підвищення кваліфікації персоналу дозволить підвищити загальну культуру виробництва, усвідомити і відчути відповідальність всіх співробітників компанії за успіх функціонування системи екологічного менеджменту.

➢ *Оцінка вихідної ситуації*. У процесі оцінювання передбачається вирішення наступних завдань:

- оцінка вихідного стану природоохоронної діяльності підприємства;
- виявлення пріоритетних екологічних аспектів та розробка попередніх рекомендацій щодо запобігання негативних екологічних впливів;
- аналіз ресурсів, необхідних для впровадження СЕМ і орієнтовної економічної ефективності заходів у рамках СЕМ.

У цілому основні напрямки вивчення вихідної ситуації зводяться до таких:

- вимоги законодавчих та нормативних актів;
- екологічні аспекти діяльності підприємства, її продукції, послуг;
- дотримання вимог стандартів, регламентів, правил, норм;
- існуюча практика і процедури екологічного управління;
- існуюча політика та ділові процедури з виконання контрактів, поставок;
- реалізація зворотного зв’язку за результатами аудиту;
- можливості забезпечення переваг у конкурентоспроможності;
- оцінка зацікавлених сторін;
- функції та діяльність інших організаційно-технічних систем, які можуть сприяти або перешкоджати поліпшенню характеристик навколишнього середовища.

➢ *Створення робочої групи*. Практика показує, що для середнього чи великого підприємства потрібно укомплектування робочої групи 3-5 фахівцями на повний термін роботи до року. На малих підприємствах цією роботою може займатися одна або дві особи (при 50% часу протягом робочого дня). Вважається, що в середньому для ведення роботи зі впровадження СЕМ необхідна одна людина на 200 працюючих.

На початковому етапі група екологічного менеджменту звичайно є складовою частиною відповідного природоохоронного підрозділу підприємства. Поступово в міру реалізації положень СЕМ група екологічного управління трансформується в службу ЕМ.

➢ *Розробка плану впровадження СЕМ*. Група екологічного менеджменту (у співпраці з консультантом) розробляє план впровадження СЕМ, який повинен бути затверджений вищим керівництвом, визначає послідовність дій, передбачає залучення до цієї роботи фахівців, керівників середньої та нижчої ланки підрозділів, враховує існуючі програми розвитку підприємства.

➢ *Розробка системи внутрішніх стандартів*. Особлива роль у позитивному вирішенні проблеми впровадження СЕМ на підприємстві належить внутрішнім стандартам, які розробляються і затверджуються підприємствами самостійно. Кількість стандартів не повинно бути занадто великою, щоб залишалася можливість прийняття самостійних рішень екологічного характеру. З іншого боку, їх, не повинно бути й занадто мало, щоб не знизити значущість і можливість контролю. Найбільш доцільна кількість документів і стандартів становить 20-25.

Перелік рекомендованих стандартів екологічного менеджменту на підприємстві:

- «Керівництво з СЕМ»;
- «Ідентифікація екологічних аспектів»;
- «Ідентифікація законодавчих та інших екологічних вимог»;
- «Цільові і планові показники. Програма екологічного менеджменту»;
- «Відповідальність і повноваження. Організаційні структури, положення про структурні підрозділи, посадові інструкції. Порядок розробки та оформлення»;
- «Людські ресурси. Підготовка та підвищення кваліфікації персоналу»;
- «Внутрішні і зовнішні комунікації»;
- «Управління документацією. Основні положення»;
- «Управління документацією. Порядок розгляду проектів стандартів, технічних умов та інших нормативних документів з стандартизації»;
- «Управління операціями»;
- «Організація виробничого екологічного контролю»;
- «Інфраструктура. Технічне обслуговування та ремонт обладнання»;
- «Закупівлі»;
- «Підготовленість до аварійних ситуацій та реагування на них»;
- «Організація екологічного моніторингу»;
- «Управління засобами моніторингу та вимірювань. Засоби вимірювання. Перевірка, калібрування, ремонт, експлуатація, облік і зберігання»;
- «Управління засобами моніторингу та вимірювань»;
- «Невідповідності. Коригувальні та запобіжні дії»;
- «Управління екологічними записами»;
- «Внутрішній аудит»;
- «Аналіз функціонування СЕМ з боку керівництва».

При цьому початковою розробці підлягає половина необхідних стандартів, решта припускають коригування існуючих.

Обов’язково узагальнюючим документом, що регулює впровадження СЕМ, є «Керівництво з СЕМ», обсяг якого не повинен виходити за межі 35-40 сторінок,

інакше документ стає нечитабельним.

Як правило, в «Керівництво з СЕМ» включається опис області поширення системи екологічного менеджменту, наводиться коротка екологічна характеристика об'єктів, що входять в область сертифікації, описуються відповідальність і повноваження керівного складу підприємства в рамках СЕМ і дається короткий опис всіх елементів системи та їх взаємодії. Як додаток в Керівництві можуть бути наведені: адміністративна структура управління на підприємстві, матриця розподілу відповідальності в СЕМ, екологічна політика, перелік основних документів СЕМ із зазначенням їх місця зберігання.

II. Етап планування:

➢ У загальному циклі створення СЕМ першим кроком, що передує роботі з планування, є *формулювання екологічної політики підприємства*.

Відповідно до стандарту ІСО 14001, **екологічна політика** – заява організації про свої наміри і принципи, що пов'язані з її загальною екологічною ефективністю.

Екологічна політика являє собою документ (не більш сторінки), прочитавши який можна зрозуміти, на випуск якої продукції спрямована основна діяльність підприємства, які екологічні вершини задає собі колектив підприємства і за допомогою яких принципів він передбачає їх досягти.

Розробку екологічної політики здійснює робоча група СЕМ, в уточненні та коригуванні документа бере участь весь колектив підприємства.

Текст сформульованої та затвердженої екологічної політики повинен бути розміщений на видному місці кожного підрозділу підприємства.

➢ *Екологічні аспекти діяльності підприємства*. Визначення екологічних аспектів – один з найскладніших етапів. **Екологічний аспект** – це елемент діяльності підприємства, його продукції та послуг, який може взаємодіяти з навколишнім середовищем, тобто змінювати параметри її якості.

Ідентифікація екологічних аспектів і оцінка пов'язаних з ними впливів виконується в кілька етапів. На першому етапі здійснюється вибір виду діяльності, продукції або послуги, які здійснюють вплив на навколишнє середовище. Потім для обраного виду діяльності визначається як можна більшу кількість екологічних аспектів, пов'язаних з ним, наприклад: забруднення атмосферного повітря викидами, споживання електроенергії; вилучення водних ресурсів та утворення стічних вод; утворення відходів; можливі аварійні ситуації. Після чого проводиться визначення максимальної кількості впливів (негативних і позитивних) на навколишнє середовище, які пов'язані з кожним ідентифікованим екологічним аспектом.

Виявлені екологічні аспекти необхідно сформувати в загальний перелік – реєстр екологічних аспектів, на основі яких фахівці групи СЕМ повинні формувати опитувальні листи для роботи комісії з виділення пріоритетних екологічних аспектів. Виконання оцінки пріоритетності рекомендується встановлювати за допомогою методу експертних оцінок. Вибрані найбільш важливі екологічні аспекти необхідно винести в окремий перелік. Саме на їх

основі будуть визначені екологічні цілі і завдання підприємства.

Реєстр законодавчих актів. Функціонування СЕМ на підприємстві передбачає дотримання всіх законодавчих та нормативних вимог у галузі охорони навколишнього середовища, у зв'язку з чим, в обов'язковому порядку, повинен формуватися реєстр законодавчих вимог та екологічних аспектів діяльності підприємства, його продукції та послуг, а також реєстр нормативних документів.

До складу *законодавчих актів* входять: міжнародні правові акти, закони України, укази і розпорядження Президента, постанови КМУ, правові акти галузевого, відомчого та корпоративного характеру, правові акти місцевих органів влади.

До складу *нормативних документів* входять: міждержавні та державні стандарти, гігієнічні нормативи, санітарні правила і норми, будівельні норми і правила.

Таблиця 4.1.

Приклад оформлення реєстру законодавчих вимог і нормативних документів

Вид документа	Назва документа	Номер, дата затвердження документа, дата останньої редакції документа
1	*2*	*3*

➢ *Розробка цільових і планових екологічних показників*. **Цільові показники** – це кількісна характеристика цілей СЕМ на певний період часу. Всі цільові показники повинні спиратися на екологічну політику. **Планові показники** – це кількісна характеристика завдань.

Документ з остаточно розробленими цільовими і плановими показниками носить назву «відомість цільових і планових показників» і затверджується керівником підприємства.

Встановлені цільові та планові показники, оформлені документально, служать основою складання програм природоохоронних заходів.

➢ *Розробка програм природоохоронних заходів*. **Програма природоохоронних заходів** – це комплекс технічних і технологічних заходів, спрямованих безпосередньо на зниження шкідливого впливу екологічних аспектів діяльності підприємства на якість навколишнього середовища, а також організаційні заходи щодо вдосконалення системи екологічного моніторингу, організації системи екологічної освіти, розробку необхідної природоохоронної документації.

Програма природоохоронних заходів – це керівництво до дії, в якому вказано хто, в які терміни, за рахунок яких ресурсів і що повинен робити.

До розробки програм повинні залучатися всі структурні підрозділи

компанії, плани заходів цих підрозділів є основою розробки програми для підприємства в цілому.

Таблиця 4.2.

Форма плану заходів структурного підрозділу

Найменування природоохоронного заходу	Плановані витрати на поточний рік	Джерело фінансування	Терміни виконання		Відповідальний виконавець	Очікувані результати
			початок	завершення		

Програма, оформлена відповідно до діючих вимог, затверджується керівництвом підприємства.

III. Впровадження і функціонування системи екологічного менеджменту:

➢ *Формування організаційної структури*. Найкращою структурою є спеціалізована служба менеджменту, керівник якої прирівнюється за рангом заступнику генерального директора або заступнику головного інженера. В обов'язки групи (бюро) СЕМ входить вирішення наступних питань:

- навчання, обізнаність персоналу (підвищення кваліфікації персоналу з спеціально розробленими програмами);
- внутрішні і зовнішні зв'язки (створення внутрішніх зв'язків між структурними підрозділами, а також координація зовнішніх зв'язків з зацікавленими сторонами з питань охорони навколишнього середовища підприємства);
- розробка і управління документацією в СЕМ (у тому числі розробка стандартів підприємства за системою екологічного менеджменту);
- аудит СЕМ (встановлюється порядок проведення внутрішніх аудитів з метою підтвердження ефективності функціонування СЕМ).

Важливим елементом цього етапу є формування матриці розподілу відповідальності в СЕМ.

➢ *Організація системи освіти* повинна бути направлена на зміну ставлення робітників до проблем навколишнього середовища, на виховання в них екологічної свідомості, а також на отримання інформації про можливі шляхи і методи зниження впливу на довкілля.

У процесі навчання приймає участь весь технічний персонал підприємства, залучені консультанти, спеціалісти суміжних організацій, вищестоящі підприємства. Програми навчання при цьому відрізняються. Навчання середньої управлінської ланки і спеціалісті доцільно організувати в активній формі (семінари і практичні заняття більш доречні, аніж лекції); для працівників найбільш доцільно проводити інструктаж і навчання на робочому місці.

Таблиця 4.3

Види навчання при впровадженні СЕМ

Контингент, що навчається	Вид начиння	Ціль
Вище керівництво	Оглядовий курс про стратегічну важливість екологічного менеджменту	Отримання знань і вмінь формування екологічної політики підприємства, інформації про нові закони і підзаконні акти
Усі працівники	Базовий курс про охорону навколишнього середовища, основи екологічного менеджменту	Отримання знань з питань політики, цілей і завдань охорони навколишнього середовища, виховання почуття відповідальності
Працівники, відповідальні за заходи з охорони навколишнього середовища	Підвищення кваліфікації, участь у семінарах по обміну досвідом	Підвищення рівня знань з окремих питань, отримання оперативної інформації про зміни в стандартах
Робітники, чиї функції мають відношення до проблем охорони навколишнього середовища	Короткі програми додаткового навчання, поточна інформації про впровадження СЕМ	Ознайомлення з нормативними актами і внутрішніми вимогами

➢ *Документування*. Документація з СЕМ повинна бути інформативної, зручною для перегляду та вміщувати опис всіх процедур, що стосуються її розробки, погодження, використання, перегляду і зберігання.

Розроблені документи погоджуються з відповідними посадовими особами служби екологічного менеджменту. Права на затвердження документів СЕМ має директор, головний інженер, керівник СЕМ, директора за напрямами діяльності в межах визначених повноважень.

Рис. 4.2. Структура і рівні документації СЕМ

➢ *Організація системи зовнішніх і внутрішніх комунікацій*. Комунікаційні процеси у сфері екологічного менеджменту поділяються на внутрішні (між

співробітниками підприємства) і зовнішні (між підприємством та зовнішнім середовищем). Під **комунікаціями** в даному випадку розуміють взаємозв'язки, що виникають між людьми в процесі обміну інформацією, пов'язаною з діяльністю підприємства в галузі екологічного менеджменту.

Однією з форм зовнішніх комунікацій є поширення екологічної звітності, що відбиває планування, організацію та оцінку фактичної ефективності СЕМ, включаючи негативні результати. Способи подання ініціативної екологічної звітності можуть бути різні: видання інформаційних листів, матеріалів у ЗМІ, ведення сторінки в INTERNET і т.д. Найбільш поширеною формою екологічної звітності є річний ініціативний звіт, форма, зміст, способи і області поширення якого визначаються самим підприємством.

Управління внутрішніми операціями і процесами, що надають найбільший вплив на навколишнє середовище, відбувається через наступні документи: стандарти підприємства; технологічні інструкції; положення щодо екологічної безпеки підприємства; посадові інструкції та ін. На підприємстві також повинні бути встановлені правила щодо екологічно безпечного зберігання, переміщення, транспортування та використання хімікатів, сировини, матеріалів і відходів, що містять шкідливі речовини.

➢ *Підготовка до аварійних ситуацій*. На підприємстві передбачається розробка спеціального порядку щодо попередження аварійних ситуацій, які можуть виникати при здійсненні виробничих процесів, результатом яких може бути значний вплив на навколишнє середовище. Цей порядок має бути документований і затверджений керівництвом підприємства в Положенні про систему управління екологічною безпекою, в стандартах підприємства «Підготовленість до аварійних ситуацій та реагування на них», у переліку типових аварій, що мають негативні впливи на навколишнє середовище та їх екологічні аспекти.

На підприємстві повинен вестися облік усіх аварій та катастроф, які виникали для аналізу причин і наслідків цих ситуацій і розробки плану дій їх ліквідації та попереджувальних заходів. Плани дій з ліквідації аварії повинні постійно переглядатися, коригуватися і оновлюватися.

Особливо слід відзначити, що ліквідація наслідків аварійних ситуацій або зменшення їх масштабу, а також відшкодування втрат, зумовлених цими наслідками, пов'язані зі значними фінансовими витратами на здійснення компенсаційних заходів, що вимагає формування механізму вишукування джерел вільних фінансових коштів.

Одним з таких механізмів в ринковій економіці є *система страхування* (у тому числі екологічного), яка виконує ряд важливих функцій: захист підприємців від економічних втрат, захист економічних інтересів громадян, а також соціальний захист (ініційовані державою програми соціальної реабілітації, ліквідації наслідків екологічних лих та ін.). Дуже розповсюдженими є позови про відшкодування шкоди навколишньому середовищу, що пред'являються органами державної влади.

VI. Контрольні і коригуючі дії:

➢ *Організація моніторингу*. Екологічний моніторинг проводиться для оцінки якості та виявлення зміни в навколишньому середовищі, які є наслідком негативного впливу підприємства, а також вжиття заходів щодо усунення відхилень від діючих нормативно-методичних та інших законодавчих екологічних вимог.

Завданнями екологічного моніторингу є:

- реальна оцінка поточної екологічної ситуації;
- аналіз тенденцій зміни якості навколишнього середовища;
- спостереження за параметрами основних джерел забруднення навколишнього середовища;
- оцінка ефективності природоохоронних заходів за критеріями якості навколишнього середовища;
- реєстрація інформації для того, щоб простежити за відповідністю цільовим та плановим показникам;
- прогноз зміни ситуації на перспективу.

Основні об'єкти виробничого екологічного моніторингу на підприємстві – це сировина, матеріали, реагенти, що використовуються у виробництві, джерела утворення відходів, джерела викидів забруднюючих речовин в атмосферне повітря, джерела скидів забруднюючих речовин у поверхневі води, системи очищення газів, що відходять, майданчики тимчасового зберігання відходів. Крім того до об'єктів виробничого екологічного моніторингу відноситься готова продукція, а також компоненти природного середовища в зоні впливу підприємства.

Система виробничого екологічного моніторингу охоплює всі структурні підрозділи, здійснюється персоналом підприємства та централізовано – екологічною службою.

Група екологічного моніторингу повинна вирішувати такі завдання:

- контролювати дотримання вимог нормативної та технологічної документації (технологічних інструкцій, виробничо-технічних інструкцій) у виробничих процесах підрозділів підприємства, пов'язаних зі значними впливами на навколишнє середовище;
- враховувати номенклатуру і кількість забруднюючих речовин, що надходять у навколишнє середовище від підрозділів підприємства;
- контролювати стабільність і ефективність роботи природоохоронного устаткування;
- контролювати екологічну безпеку продукції;
- здійснювати контроль викидів в атмосферу, скидів стічних вод, водоспоживання та водовідведення безпосередньо на кордонах технологічного процесу для оцінки дотримання нормативів;
- стежити за дотриманням підрозділами підприємства встановлених нормативів впливу на навколишнє середовище і лімітів розміщення відходів.

Відповідальність за організацію та проведення екологічного контролю на підприємстві несе головний інженер, і керівники структурних підрозділів.

➢ *Проведення перевірок та коригуючих дій*. Відповідно до ISO 14001:2004 організація повинна здійснювати перевірку діяльності персоналу в кожному конкретному підрозділі (що входить в область поширення СЕМ), оцінку обізнаності персоналу, його дисциплінованості (у плані технологічної та виконавської дисципліни) і осмисленої готовності сприяти (у межах своєї компетенції) реалізації спільних цілей компанії, а також здійснювати постійну перевірку відповідності системи екологічного менеджменту запланованим заходам, у тому числі вимогам стандарту ISO 14001:2004.

У загальному вигляді коригуючі та запобіжні дії у сфері охорони навколишнього середовища служать реагуванням, на які виявляються невідповідності діяльності організації законодавчим та іншим нормативним вимогам природоохоронного, санітарного та іншого характеру, а також вимогам самої системи управління охороною навколишнього середовища на підприємстві, і передбачають прийняття відповідальних рішень (в тому числі вищим керівництвом підприємства) щодо своєчасної розробки та реалізації необхідних і достатніх заходів для усунення виявлених невідповідностей.

Особливе значення мають процедури виконання коригуючих дій при виникненні екологічних інцидентів та аварійних ситуацій. Тому елемент системи «Коригуючі та запобіжні дії» тісно пов'язаний з елементом «Підготовленість до аварійних ситуацій та реагування на них», який є лише в стандартах ISO серії 14000 і відсутній в стандартах ISO серії 9000 по системах якості.

У залежності від значимості і причин ситуацій, що виникли коригуючі дії можуть включати:

- зупинку виробничого процесу;
- технічні дії з усунення невідповідності (ремонт, переналагодження і т.д.);
- отримання особливих дозволів (наприклад, на використання резервних потужностей, запасів і т.д.);
- оповіщення місцевої влади (при аварійній ситуації);
- введення в дію аварійного плану.

Коригуючі та запобіжні дії спрямовані на реалізацію головного принципу функціонування СЕМ – постійне поліпшення.

➢ *Управління зареєстрованими даними*. Документально зареєстровані дані (протоколи вимірювань основних характеристик впливу підприємства на навколишнє середовище, плани-графіки виконання замірів та перевірок, форми державної статистичної звітності природоохоронної діяльності підприємства, акти перевірок структурних підрозділів, копії реєстрів екологічних аспектів, реєстри законодавчих та інших екологічних вимог) повинні зберігатися у відділі управління охорони навколишнього середовища; журнали первинної звітної документації – у структурних підрозділах підприємства у відповідальних за природоохоронну діяльність.

➢ *Організація та проведення внутрішніх аудитів*. На відміну від

«Моніторингу та вимірювань», які проводяться в основному з метою забезпечення інструментального контролю якості навколишнього середовища та впливу підприємства на компоненти навколишнього середовища і «Оцінки відповідності вимогам природоохоронного законодавства та інших нормативних документів», яка передбачає перевірку зовнішніх вимог до підприємства в цілому, внутрішній аудит спрямований на перевірку діяльності співробітників у кожному конкретному підрозділі (що входить в область поширення СЕМ), оцінку обізнаності персоналу, його дисциплінованості (у плані технологічної та виконавської дисципліни) і розумінню процесів необхідних для здійснення спільних цілей природоохоронної діяльності підприємства.

По суті **внутрішній аудит** – це виробничий самоконтроль (на всіх рівнях), який забезпечується силами персоналу самого підприємства і може бути більш глибоким і конкретним, ніж зовнішній, оскільки зсередини краще видно стан і проблеми підприємства.

Підставою для проведення внутрішнього аудиту є річний графік і рішення керівництва служби екологічного менеджменту.

Здійснення екологічного аудиту вигідно керівництву компанії, тому що результат аудиту інформує його, чи працює впроваджена система екологічного менеджменту так, як вона повинна працювати відповідно до заявленої екологічної політики.

Звіт з аудиту повинен бути представленим керівнику структурного підрозділу, де проводився аудит, і головному інженеру підприємства для прийняття відповідних рішень.

V. Аналіз з боку керівництва:

Наявність процедури регулярної звітності для керівництва про результати та можливості подальшого розвитку діяльності з екологічного менеджменту, а також документованого висновку керівництва підприємства за цим звітом є одним з ключових умов відповідності СЕМ стандарту ISO 14001.

Аналіз з боку керівництва дозволяє, з одного боку реалізувати принципи послідовного поліпшення, розвиваючи СЕМ, з іншого боку, він дає можливість підтримувати ефективність та адекватність СЕМ.

3. ВИТРАТИ НА ВПРОВАДЖЕННЯ СЕМ

Ніяка нова діяльність, ніяка зміна не обходиться без витрат. Це, безперечно, відноситься і до впровадження СЕМ. Очевидно також, що для різних за типом і розміром організацій витрати будуть відрізнятися. Але наскільки і якими будуть ці витрати – однозначних відповідей на ці питання не дає ніхто, і на практиці виявляється, що витрати організації рідко відповідають запланованим.

Основні етапи і елементи процесу впровадження СЕМ:

І. Підготовчий етап:

Можлива тривалість етапу: від 1 міс.

1.1. Отримання загальної інформації, придбання нормативної та методичної літератури.

Витрати можуть істотно відрізнятися залежно від того, доступні чи ні некомерційні інформаційні семінари, чи достатньо доступної методичної літератури. У будь-якому випадку, витрати на цьому етапі не будуть дуже великі.

1.2. Навчання спеціалістів – майбутніх менеджерів СЕМ.

Звичайно фахівці направляються на навчання з впровадження СЕМ та/або підготовку внутрішніх аудиторів СЕМ тривалістю від трьох днів до двох тижнів. Великі організації навчають кількох людей, середні – зазвичай одного-двох. Таким чином, трудовитрати фахівців становлять від 5 до 30 люд.-днів.

Альтернативними варіантами можна вважати використання можливостей навчання у процесі некомерційних проектів тощо (потрібні тільки витрати часу фахівців); прийняття на роботу фахівця, який вже має досвід впровадження СЕМ. У великих компаніях, що включають до свого складу кілька підприємств, навчені фахівці одного з них можуть передавати досвід іншим підрозділам.

1.3. Оцінка вихідної ситуації для впровадження СЕМ.

Оцінка вихідної ситуації – один з найважливіших етапів впровадження СЕМ. Зазвичай її проведення доручається консультантам, причому включається як один з етапів у комплексний договір на впровадження СЕМ.

Як альтернативу можна розглядати здійснення оцінювання вихідної ситуації силами компанії або із запрошенням фахівців (у т.ч. фахівців інших підприємств) на індивідуальній основі. У цьому випадку буде потрібно більше часу і більшим буде внесок фахівців компанії, але сумарні витрати будуть менше. Трудовитрати становлять від 3 до 20 люд.-днів.

1.4. Ухвалення рішення про впровадження СЕМ, планування і виділення ресурсів.

Цей етап рідко розглядається як витратний, до нього далеко не завжди підходять методично, і рішення про впровадження СЕМ звичайно приймається вищим керівником в «наказовому» порядку.

II. Розробка СЕМ (етап планування):

Можлива тривалість стадії: від 3 до 6 міс.

2.1. Навчання керівництва.

Навчання керівників при роботі з консультантом зазвичай проводиться у вигляді наради, займаючи близько половини робочого дня вищих керівників основних напрямків (якість, виробництво, фінанси, маркетинг, постачання, інформація). Альтернативний варіант – навчання керівників силами фахівців, що вже пройшли підготовку. У будь-якому випадку, витрати часу приблизно однакові.

2.2. Навчання спеціалістів підприємства.

Для малого підприємства часто достатнім є навчання одного або декількох фахівців (див. етап 1.2), які потім проводять курс навчання для фахівців і керівників середньої ланки, які, в свою чергу, навчають підлеглих. Для середніх і, особливо, великих підприємств доцільним може виявитися навчання основної

групи фахівців на спеціально організованому семінарі силами консультантів або запрошених викладачів. У цьому випадку трудовитрати викладачів складуть 8-12 люд.-днів (включаючи підготовку адаптованих матеріалів для навчання), залучені до навчання фахівці будуть зайняті протягом 2-3 днів кожний. Для великих підприємств, у зв'язку з чисельністю фахівців, може знадобитися навчання в кілька етапів.

На цій стадії будуть потрібні також витрати на навчальні та інформаційні матеріали, можливо, на оренду презентаційного устаткування або приміщення, проїзд та проживання консультантів або фахівців підприємства.

2.3. Створення робочої групи з розробки СЕМ.

При уявній формальній простоті створення робочої групи займає досить багато часу. Необхідно підібрати групу спеціалістів, які отримали відповідну підготовку і здатні працювати над новими завданнями, забезпечити можливість роботи групи. Якщо для малої організації може бути достатньо 2-3 спеціалісти, зайнятих на 50% часу; розробка СЕМ для середнього або великого підприємства потребують залучення фахівців, еквівалентного повної зайнятості 3-5 чоловік на термін до року. Групі необхідно забезпечити робочі місця, звільнити обраних спеціалістів від інших видів діяльності і, відповідно, забезпечити їх заміщення на час впровадження СЕМ. Нерідко на початок роботи групи йде кілька тижнів, хоча для передачі справ фахівцям достатньо 1-2 днів.

2.4. Розробка елементів СЕМ.

2.4.1. Розробка системних елементів СЕМ (описи загальної структури СЕМ, опису процесів організації, політики, загальних процедур, цілей, регістрів і т.п.)

Існують два основні варіанти виконання цього етапу: всі основні документи розробляються консультантом на основі наявних шаблонів або документи розробляються робочою групою СЕМ за підтримки консультанта і широкому залученні фахівців підприємства.

У тому випадку, коли робота виконується фахівцями підприємства, трудовитрати консультантів відносно невеликі – зазвичай в діапазоні 5-15 люд.-днів. Залучення вищих керівників потрібно в основному при розробці структури СЕМ, екологічної політики, постановці екологічних цілей, і при розробці процедур аналізу та оцінки керівництвом. Значне залучення спеціалістів різних підрозділів і керівників середньої ланки буде потрібно при розробці структури СЕМ, описі процесів організації, екологічних цілей. Найбільші трудовитрати робочої групи з впровадження СЕМ будуть потрібні для виявлення та визначення пріоритетних екологічних аспектів, а також розробки відповідних процедур.

2.4.1. Розробка «практичних» елементів СЕМ (завдання і програми, відповідальність, робочі процедури, система моніторингу і т.п.).

У тому випадку, коли робота виконується спеціалістами підприємства, внесок консультантів зазвичай невеликий, але залежить від розмірів організації. У той же час для виконання етапу необхідні значні трудовитрати спеціалістів підприємства, і особливо лінійних керівників. Участь вищих керівників потрібно зазвичай лише для затвердження повноважень, пов'язаних з СЕМ.

III. Впровадження і функціонування СЕМ:

Можлива тривалість етапу: від 3 до 6 міс.

3.1. Мотиваційна діяльність.

Залежно від традицій, структури і принципів управління підприємства мотивація може мати різні форми; витрати на неї можуть докорінно відрізнятися. У будь-якому випадку певні витрати на мотивацію спеціалістів і персоналу будуть необхідні.

3.2. Навчання працівників і впровадження процедур.

Для впровадження у практику змінених процедур необхідний певний час, протягом якого помітне навантаження будуть нести керівники середнього та нижчого рівня. Зазвичай повне впровадження процедур займає від одного до двох тижнів.

Природно, впровадження змінених процедур супроводжується навчанням: спочатку керівників нижчої ланки, а потім – персоналу. Трудовитрати на етап складають 5-15 люд.-днів спеціалістів групи з впровадження СЕМ, по 1-2 дні для майстрів змін і начальників дільниць, від половини до одного дня на кожного працівника штату, до діяльності якого належать змінені процедури. Варто відзначити, що в більшості випадків навіть грамотно розроблені процедури потребуватимуть коригування за результатами пілотного застосування.

Крім трудовитрат, необхідні також витрати на навчальні та інформаційні матеріали. Мінімально потрібне тиражування змінених типових інструкцій і процедур для персоналу.

IV. Функціонування СЕМ (етап контрольних і коригуючих дій):

Мінімальна тривалість стадії до сертифікації: 3 міс.

4.1. Контроль виконання процедур і коректування.

Контроль виконання процедур повинен здійснюватися керівниками нижчої ланки протягом досить тривалого часу для того, щоб переконатися у чіткому і регулярному виконанні процедур персоналом та ідентифікувати принаймні основні проблеми невідповідності. Зазвичай при впровадженні СЕМ на цей етап потрібно 2-3 місяці.

4.2. Моніторинг.

Основна увага в СЕМ приділяється моніторингу процесів і результатів діяльності. Хоча розвиток моніторингу і може вимагати певних капітальних витрат (наприклад, на установку витратомірів тощо), такі витрати визначаються обов’язково з урахуванням доцільності та наявних коштів. Зазвичай помітного збільшення витрат на інструментальний моніторинг не відбувається.

4.3. Внутрішні аудити.

Проведення внутрішніх аудитів СЕМ вимагає участі декількох спеціалістів; найчастіше внутрішній аудит різних підрозділів проводиться за заздалегідь розробленою програмою, що охоплює значний період часу. Звичайні трудовитрати аудиторів – 5-25 люд.-днів.

V. Аналіз з боку керівництва:

5.1. Аналіз системи, оцінка керівництвом і перегляд системи.

Матеріали для аналізу та рекомендації готуються менеджером СЕМ або керівником групи внутрішніх аудиторів, рішення за рекомендаціями повинні бути прийняті вищим керівництвом. Трудовитрати спеціалістів на цьому етапі істотно залежать від успішності впровадження/функціонування СЕМ. Зазвичай на аналіз результатів і розробку рекомендацій достатньо 5-10 людино-днів. Мінімальні трудовитрати вищого керівництва (якщо немає необхідності в істотних змінах) складуть близько половини дня для кожного представника вищого керівництва, що бере участь у впровадженні СЕМ, додатково 1-2 дні для представника керівництва з СЕМ.

VI. Сертифікація СЕМ:

Можлива тривалість стадії: від 2 до 3 міс.

(до отримання сертифіката)

6.1. Сертифікація та інспекційні перевірки.

Система проведення екологічної сертифікації передбачає такий алгоритм: залучення третьої сторони – органу екологічної сертифікації (Всеукраїнська громадська організація «Жива планета»), процедура екологічного аудиту, використання переліку робіт з оцінки відповідності, які вказуються в договорі (схемі екологічної сертифікації).

Вартість екологічної сертифікації продукції залежить від кількості заявлених категорій (видів) продукції, найменувань, а також повноти даних. Наприклад, якщо мова йде про продукцію, яка вироблена за одним ТУ (ДСТУ, ГОСТ), то вона розглядається як продукція однієї категорії. Документальний аудит однієї категорії продукції коштує 8000 грн. За кожне найменування, яке має відмінності за рецептурою/складом додається від 150 до 1500 грн. (в залежності від ступеню розбіжності між найменуваннями кількості інгредієнтів, складників тощо). Тобто, якщо підприємство «Х» заявляє на сертифікацію 10 найменувань продукції в категорії, наприклад «косметична продукція» (мила, шампунів, гелів для душу), орієнтовна вартість документального аудиту може розраховуватись наступним чином:

- Максимальна: 8000 +10 х1500 = 23000 грн.
- Мінімальна: 8000 + 10х150 = 9500 грн.
- Середня: 8000+10х650 = 14500 грн.

Фактична ціна розраховується на основі первинного аналізу заявки на сертифікацію, до якої додаються протоколи випробувань на продукцію, а також надання вичерпних відповідей на всі питання стосовно екологічних аспектів виробництва.

Наведені вище оцінки зроблені для «нормальної» ситуації, коли діяльність з впровадження СЕМ здійснюється відповідно до плану. Однак нерідко трапляються непередбачені обставини, що впливають на впровадження СЕМ. Це обумовлено такими важливими чинниками:

- браком досвіду як у підприємств, так і у частини консультантів, що ускладнює надійне планування виділення ресурсів;
- досить великою тривалістю періоду, необхідного для впровадження СЕМ;

- швидкими змінами в економіці, ситуації на ринках і т.д.

Подібні труднощі можуть збільшити витрати на впровадження на 50-150% або більше. В той же час непередбачені витрати в розмірі 10-15% є нормальними для такого складного процесу.

4. ЕКОНОМІЧНИЙ ЕФЕКТ ВПРОВАДЖЕННЯ СЕМ

Як і будь-які інші інвестиції у розвиток систем менеджменту, вкладення в розвиток СЕМ окупаються за рахунок їх результатів, у тому числі непрямих, що виявляються в зміні ефективності та результативності організації. Так само, як і для будь-яких інших подібних інвестицій, їх ефективність і терміни повернення складно охарактеризувати з високим ступенем точності не тільки заздалегідь, але часто і за підсумками успішного завершення процесу модернізації системи менеджменту. Тим не менш, можна запропонувати одразу кілька підходів до оцінювання економічних результатів впровадження СЕМ.

➢ Одним з можливих підходів є врахування лише *прямих витрат* і безпосередньо пов'язаних з ними результатів. У якості витрат необхідно враховувати прямі витрати на консультантів і витрати часу персоналу, витрати на впровадження методів запобігання забруднення і традиційних методів зниження впливу. Як безпосередні переваги можна розглядати зниження платежів та штрафів за забруднення навколишнього середовища, а також економічні ефекти впровадження підходів запобігання впливу: зниження використання ресурсів і матеріалів, зниження витрат на поводження з сировинними та іншими матеріалами, а також відходами. При цьому слід враховувати економію у рамках всієї системи логістики підприємства (враховуючи витрати на транспортування, зберігання, поводження з відходами, транспортування надлишкової маси виробів і т.п.).

Практика показує, що для підприємств тільки систематичне застосування маловитратних методів запобігання забруднення здатне окупити вкладення на розвиток СЕМ за дуже короткі терміни. Якщо ж врахувати, що при зростанні масштабів підприємств витрати на впровадження ростуть повільніше, а масштаби переробки сировини та ресурсів значно збільшуються, то впровадження СЕМ лише за рахунок застосування підходів запобігання забруднення здатне дати дуже хороші економічні результати.

➢ Економічні ефекти впровадження СЕМ визначаються не тільки результатами застосування підходів запобігання забруднення. Більш того, можливості застосування цих методів істотно обмежені для організацій, які не займаються виробництвом або що не роблять послуг. У цьому випадку можна застосувати *інтегральний підхід* до оцінки економічних ефектів впровадження СЕМ. Для цього можна аналізувати біржові показники акціонерних компаній, що об'єднані в портфелі акцій з метою виключення індивідуальних особливостей.

Для аналізу ефективності вкладень в СЕМ розглянемо кілька підходів до

створення таких портфелів. Перший заснований на використанні рейтингу і індексу EcoVALUE'21, що розроблений компанією Innovest Strategic Value Advisers для ринку США. Рейтинг заснований на цілому ряді «екологічних» характеристик підприємства (більше 60 параметрів) п'яти основних категорій:

- системи менеджменту;
- еко-ефективність;
- операційні ризики;
- можливість використання переваг екологічно орієнтованих ринків;
- історичні відомості про аварії та порушення законодавства.

Оцінка за критеріями визначає рейтинг підприємства – від AAA (краще) до CCC (гірше). Таким чином, всі критерії рейтингу безпосередньо або опосередковано пов'язані з впровадженням і результативністю СЕМ.

➢ Загальну оцінку внеску екологічних та інших елементів сталого розвитку в ефективність і капіталізацію компанії дозволяють дати індекси, підтримувані Dow Jones Indexes і FTSE Group. Обидва індекси – *Dow Jones Sustainability Index (DJSI)* і *FTSE4Good* – незалежні, і виділяють компанії за розгорнутою системою критеріїв, що включає економічні, екологічні та соціальні аспекти сталого розвитку.

Таким чином, серйозну увагу і проактивний підхід до природоохоронної діяльності, розвиток систем екологічного менеджменту приносять організаціям помітні економічні переваги, що відбиваються не тільки в зниженні собівартості продукції та послуг і зниженні багатьох ризиків, а й у зростанні ринкової капіталізації.

Тема 5: «ЕКОЛОГО-ЕКОНОМІЧНІ АСПЕКТИ ФУНКЦІОНУВАННЯ ПІДПРИЄМСТВ»

1. *РЕСУРСОЗБЕРЕЖЕННЯ ЯК ЧИННИК ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СУСПІЛЬНОГО ВИРОБНИЦТВА*

Ресурсозбереження – це прогресивний напрям використання природно-ресурсного потенціалу, що забезпечує економію природних ресурсів та зростання виробництва продукції при тій самій кількості використаної сировини, палива, основних і допоміжних матеріалів.

Ресурсозбереження поступово здобуває статус основної ідеології розвитку промислового виробництва. Причинами таких змін є зростаючі з року в рік обсяги залучення природних ресурсів у господарський оборот, подорожчання продукції, що виготовляється на їх основі, внаслідок вичерпання й погіршення якості ресурсів, збільшення масштабів забруднення навколишнього середовища. Таким чином, метою ресурсозберігаючої діяльності є зниження ресурсоємності (або підвищення ресурсоефективності) виробництва й забезпечення максимального корисного ефекту споживача від використання одиниці продукції, супроводжується зменшенням техногенного навантаження на навколишнє природне середовище.

- За видами ресурсів, що зберігаються, ресурсозбереження може бути класифіковане на *матеріало-, водо-, енерго-, трудо-, фондозбереження, збереження фінансових, інформаційних та інших видів ресурсів*. Даний напрямок класифікації має важливе значення, оскільки збереження окремого виду ресурсу характеризується певною специфікою, вивчення якої надає можливість сформувати комплекс відповідних ресурсозберігаючих заходів, що забезпечують найвищу віддачу вкладених коштів, та застосувати адекватні економічні пільги. Наприклад, дослідження сутності та напрямків фондозбереження має пріоритетне значення для розвитку фондомістких виробництв, трудозбереження – для виробництв, що потребують залучення великої кількості робочої сили тощо.

За *змістом процесів* виділяють:

- *раціональне використання ресурсів* (насамперед матеріальних), що означає досягнення максимальної ефективності використання ресурсів в господарстві за існуючого рівня розвитку техніки та технології з одночасним зниженням техногенного впливу на навколишнє середовище. Отже, критерієм раціонального використання ресурсів є мінімізація сукупних витрат живої та уречевленої праці при виробництві максимальної кількості кінцевої продукції, що має високі споживчі властивості;
- *економію ресурсів,* що є відносним скороченням витрат ресурсів, яке виражається у зниженні їх питомих витрат на виробництво одиниці кінцевої продукції, виконання робіт та надання послуг встановленої якості з урахуванням

соціальних, екологічних та інших обмежень.

Таблиця 5.1

Класифікація видів та напрямків ресурсозбереження

Класифікаційна ознака	Вид ресурсозбереження
Види ресурсів, що зберігаються	– матеріалозбереження – водозбереження – енергозбереження – трудозбереження – фондозбереження – …
Зміст процесів ресурсозбереження	– раціональне використання ресурсів – економія ресурсів (пряма та непряма, структурна)
Можливість реалізації	– потенційне (теоретичне, технічно можливе та економічно доцільне) – фактичне
Масштаб	– глобальне – народногосподарське – регіональне – галузеве – локальне (рівень підприємства)
Стадії життєвого циклу ресурсу	– ресурсозбереження на стадії видобутку вихідної сировини – ресурсозбереження на стадії переробки сировини – ресурсозбереження на стадії виробництва ресурсу – ресурсозбереження на стадії споживання ресурсу – ресурсозбереження на стадії транспортування ресурсу – ресурсозбереження на стадії зберігання ресурсу – ресурсозбереження на стадії утилізації ресурсу
Стадії життєвого циклу продукції	– ресурсозбереження на стадії проектування дослідного зразка – ресурсозбереження на стадії виготовлення дослідного зразка та його випробувань – ресурсозбереження на стадії виробництва кінцевого продукту – ресурсозбереження на стадії споживання (експлуатації) продукту – ресурсозбереження на стадії утилізації продукту
Обсяги фінансування та результати	– велике ресурсозбереження – мале ресурсозбереження

Таким чином, економія ресурсів є кількісним результатом процесу раціоналізації їх використання (споживання) і з урахуванням сфер діяльності підприємства може набувати як прямої, так і непрямої форми. *Пряма* економія ресурсів виникає безпосередньо протягом виробничого циклу на підприємстві внаслідок прямого скорочення обсягу витрат ресурсів на одиницю виробленої продукції певної якості. *Непряма* економія пов’язана зі сферою обігу (реалізації готової продукції) і формується за рахунок раціоналізації розміщення та

зберігання виробничих та товарних запасів, використання вторинних ресурсів тощо. Виділяють ще один вид економії ресурсів – *структурну* економію, яка має місце в межах певної галузі або економіки країни в цілому і досягається внаслідок переходу від більш ресурсо- та енергоємної структури економіки (галузі) до менш ресурсоємної шляхом зміни міжгалузевих та внутрішньогалузевих пропорцій у напрямку розвитку нових ресурсоефективних виробництв та випуску ресурсоефективних видів продукції. Слід зазначити, що економія ресурсів не завжди означає їх раціональне використання, що, наприклад, має місце у випадку скорочення витрат (економії) на виготовлення одиниці продукції за рахунок зменшення кількості споживчих властивостей продукції або погіршення її якості. Однак раціоналізація використання ресурсів обов'язково спричиняє економію витрат суспільної праці.

➢ Відповідно до можливостей реалізації виділяють *потенційне (ресурсозберігаючий потенціал)* та *фактичне ресурсозбереження*.

Ресурсозберігаючий потенціал підприємства може бути визначений як кількісна та якісна оцінка результатів, які може забезпечити ресурсозберігаючий проект при оптимальному поєднанні засобів, що його забезпечують.

У сучасній науковій літературі зазвичай виділяють три види ресурсозберігаючого потенціалу:

1) *Теоретичний потенціал ресурсозбереження* визначається максимальною економією ресурсів, яка може бути одержана за рахунок ліквідації всіх видів втрат ресурсів у національному господарстві, галузі, на підприємстві.

2) Технічно можливий потенціал являє собою частину теоретичного потенціалу та визначається максимальними технічними можливостями ресурсозбереження, що можуть бути реалізовані за фіксований проміжок часу і залежать від темпів і досягнень науково-технічного прогресу.

3) *Економічно доцільний потенціал ресурсозбереження* – це частина технічно можливого потенціалу, яка може бути прибутково освоєна при достатніх обсягах капіталовкладень, тобто вартість реалізації ресурсозберігаючих заходів буде меншою, ніж вкладення у видобуток та постачання еквівалентної кількості ресурсів.

Фактичне ресурсозбереження може бути визначене як частина його економічно доцільного потенціалу, яка фактично зменшує ресурсоспоживання в даному році та залежить від зусиль та зацікавленості споживачів ресурсів у здійсненні ресурсозберігаючих заходів.

Слід зазначити, що бажаним орієнтиром є скорочення розриву між різними видами потенціалів ресурсозбереження і насамперед між економічно доцільним потенціалом та фактичним ресурсозбереженням, що свідчитиме про зростання свідомості суб'єктів господарювання та розуміння ними важливості, актуальності та прибутковості впровадження ресурсозберігаючих заходів.

➢ За масштабом ресурсозбереження поділяється на *глобальне, народногосподарське, регіональне, галузеве та локальне* (рівень підприємства).

Найбільш вузьким масштабом дії характеризується локальне

ресурсозбереження, що охоплює всі сфери діяльності підприємства і насамперед виробничий процес. Галузеве ресурсозбереження реалізується в межах галузі, на підприємствах якої здійснюються ресурсозберігаючі заходи, та сприяє зниженню ресурсоємності продукції конкретної галузі. Регіональне ресурсозбереження визначається рамками окремого регіону і передбачає зменшення ресурсоємності відповідно до діючої термінології усієї валової доданої вартості, виробленої у регіоні, тобто продукції всіх галузей матеріального виробництва. Народногосподарське ресурсозбереження охоплює рівень національної економіки і характеризує скорочення ресурсоємності валового внутрішнього продукту. Глобальне ресурсозбереження реалізується за участю світової спільноти і зазвичай охоплює проекти, наслідки впровадження яких зачіпають інтереси декількох країн, континентів, світу в цілому. Чим вищим є рівень впровадження ресурсозберігаючих заходів – від локального до глобального – тим масштабнішими є їх результати.

➢ За стадіями життєвого циклу ресурсу розрізняють *ресурсозбереження на стадіях видобутку і переробки вихідної сировини, виробництва, споживання, транспортування, зберігання та утилізації ресурсу*.

Зміст ресурсозбереження на стадії видобутку сировини полягає у більш повному та комплексному використанні існуючих родовищ корисних копалин, стимулюванні впровадження ресурсозберігаючих технологій видобутку сировини, комплексної переробки відпрацьованої породи, підвищення рівня вилучення корисних компонентів з породи, залучення нетрадиційних та альтернативних джерел отримання сировини та енергії, поліпшення рівня використання трудових, фінансових та інших видів ресурсів на цій стадії життєвого циклу ресурсу. Ресурсозбереження на стадії переробки вихідної сировини передбачає використання ресурсозберігаючих технологій переробки, комплексного використання сировини та відходів. Стадія виробництва ресурсу містить такі напрямки ресурсозбереження, як впровадження інноваційних ресурсо- та енергоефективних технологій виробництва ресурсів, стимулювання оновлення основних виробничих фондів, застосування нових методів та прийомів праці, автоматизацію та комп'ютеризацію виробництва, виготовлення ресурсів з кращими споживчими властивостями. Ресурсозбереження, що охоплює стадію споживання ресурсу, полягає у проведенні широкомасштабних заходів з реструктуризації економіки щодо зниження питомої ваги ресурсоємних та підвищення частки наукомістких галузей, впровадженні стандартів ресурсоспоживання, виходячи з науково обґрунтованих норм витрат ресурсів, економічному стимулюванні раціонального споживання ресурсів, зміні стилю споживання з переходом від споживання ресурсів до споживання послуг, що надаються цими ресурсами. На стадії транспортування ресурсозбереження містить заходи щодо скорочення втрат ресурсів при їх транспортуванні: виключення надлишкових та зменшення норм природних втрат ресурсів, освоєння нових ресурсозберігаючих технологій транспортування, ізоляція, герметизація транспортних систем; а також щодо раціоналізації та оптимізації

плану перевезень та ін. Стадія зберігання ресурсу характеризується такими ресурсозберігаючими заходами, як скорочення обсягів та витрат зберігання ресурсів, зменшення обсягів їх псування при зберіганні, впровадження ресурсозберігаючих технологій зберігання з дотриманням оптимальних умов зберігання (температури, вологості тощо). Ресурсозбереження на останній стадії – утилізації ресурсу – полягає у розвитку та впровадженні технологій переробки вторинних ресурсів, утилізації невикористаних відходів промислового виробництва та комунального господарства, використанні відходів одних галузей в інших, встановленні стандартів щодо обов'язкового мінімального вмісту вторинної сировини в товарній продукції.

Слід зазначити, що з точки зору ефективності ресурсозбереження на стадіях життєвого циклу ресурсів найбільшою результативністю характеризується ресурсозбереження на стадіях виробництва та споживання ресурсу, оскільки наслідки такого ресурсозбереження поширюються на інші стадії. Зокрема, скорочення споживання електроенергії при виготовленні машинобудівної продукції автоматично призводить до скорочення обсягів виробництва електроенергії, а отже, і обсягів видобутку та переробки вихідної сировини – палива, потрібного для отримання енергії.

Таким чином, розглянутий напрямок класифікації ресурсозбереження має важливе значення при оцінці ефективності ресурсозберігаючих заходів на державному рівні та обґрунтуванні характеру і розміру застосовуваних економічних пільг щодо стимулювання впровадження таких заходів.

➢ Відповідно до стадій життєвого циклу продукції виділяють *ресурсозбереження на стадії проектування дослідного зразка, його виготовлення та випробувань, виробництва кінцевого продукту, споживання (експлуатації) та утилізації продукту*.

Ресурсозбереження на стадії проектування дослідного зразка полягає в оптимізації конструкції та технології майбутнього виробу з максимальним урахуванням вимог ресурсозбереження. Вдосконалення ресурсозберігаючих характеристик виробу, технології, підбір найоптимальніших матеріалів (в тому числі виключення використання токсичних) для його виробництва складає зміст ресурсозбереження на етапі виготовлення та випробувань дослідного (промислового) зразка.

Ресурсозбереження на стадії виробництва кінцевого продукту характеризується подальшим пошуком штучних замінників природних матеріалів, які можна використовувати при виготовленні продукту з подальшою утилізацією, впровадженням ресурсозберігаючих заходів в рамках існуючої технології, підвищенням продуктивності праці, поліпшенням використання основних виробничих фондів тощо.

Ресурсозбереження на стадії споживання (експлуатації) передбачає здійснення заходів щодо раціональної експлуатації виробу споживачем, гарантійного обслуговування, своєчасного ремонту продукту для подовження його виробничого ресурсу. Стадія утилізації ресурсу характеризується

ресурсозбереженням в напрямку підвищення ступеня рециркуляції складових частин виробу, нейтралізації шкідливих компонентів продукту, застосуванні безвідходних технологій переробки вторинної сировини та ін.

Зазначений напрямок класифікації є важливим та має враховуватися при обґрунтуванні реалізації ресурсозберігаючих заходів на підприємстві. Це зумовлюється тим, що кінцеві витрати на виробництво продукції значною мірою залежать від характеру здійснення ресурсозбереження на окремих стадіях її життєвого циклу. Зокрема, найбільш ефективними, з цієї точки зору, є початкові стадії – проектування дослідного зразка, його виготовлення та випробувань, – що потребують витрачання порівняно невеликих коштів, проте визначають майже 90% майбутніх витрат на виробництво продукції.

➢ За обсягами фінансування та результатами розрізняють *велике (великовитратне)* та *мале (маловитратне) ресурсозбереження*. До малого ресурсозбереження належать ресурсозберігаючі заходи, які спрямовані на ліквідацію існуючих непродуктивних втрат ресурсів та енергії, швидко окупаються та не потребують значних фінансових вкладень. Серед таких заходів можна виділити певні підгрупи, зокрема:

1) заходи щодо зниження втрат ресурсів на об’єктах промисловості та житлово-комунального господарства;

2) нові методи переробки вторинних ресурсів;

3) заходи щодо підвищення надійності всіх систем транспортування ресурсів.

Прикладами зазначених заходів малого ресурсозбереження виступають балансування та децентралізація систем опалення, забезпечення своєчасного обслуговування та ремонту основних виробничих фондів, більш продуктивне використання вторинних енергетичних ресурсів – низькопотенційного тепла та ін. Основною позитивною рисою малого ресурсозбереження є порівняно невелика вартість його здійснення, проте й отримувані результати також не є масштабними – за різними оцінками вони складають від 5 до 30% економічно доцільного потенціалу ресурсозбереження. Реалізація решти цього потенціалу припадає на велике ресурсозбереження, яке має на меті здійснити структурну перебудову економіки країни в напрямку підвищення ресурсоефективності виробництва та потребує серйозних інвестицій. До заходів великого ресурсозбереження належать впровадження високопродуктивних наукомістких технологій виробництва сталі конверторним способом та установок безперервного її розливу, виробництво цегли з підвищеною пустотністю, використання відходів вуглезбагачення та золошлакових відходів, гідротермальних джерел енергії та ін. Реалізація зазначених заходів потребує великих коштів, що, наприклад, для України обчислюються мільярдами доларів США. Проте й результати є також вражаючими: зокрема, передбачається, що реалізація енергозберігаючого потенціалу України надасть можливість повністю виключити імпорт енергоресурсів у країну та перейти на самоенергозабезпечення.

Між великим та малим ресурсозбереженням існує тісний взаємозв’язок: у

світовій практиці джерелом фінансування заходів великого ресурсозбереження зазвичай виступають кошти, зекономлені внаслідок впровадження маловитратних ресурсозберігаючих заходів, тобто мале ресурсозбереження формує базу для здійснення великого ресурсозбереження. З огляду на це при реформуванні українського законодавства слід передбачити застосування адекватних економічних пільг, насамперед для малого ресурсозбереження.

2. *ВІДХОДИ ЯК ВТОРИННІ РЕСУРСИ*

Одноразове використання матеріалів та ресурсів призвело до масового накопичення відходів та виробництва стійких забруднювачів природного середовища. Відходами називають будь-які речовини, матеріали і предмети, що утворюються в процесі людської діяльності і далі не використовуються за місцем утворення чи виявлення та яких їх власник повинен позбутися шляхом утилізації або видалення. До відходів належать:

- залишки сировини, матеріалів, напівфабрикатів, утворені під час виробництва, які втратили цілком або частково вихідні споживчі властивості (відходи виробництва);
- розкривні і супутні гірничі породи, що видобуваються у процесі розроблення родовищ корисних копалин;
- залишкові продукти збагачення сировини (шлам, пил тощо);
- нові речовини та їх суміші, утворені в термічних, хімічних та інших процесах (шлак, зола, інші утворення, а також рідини та аерозолі);
- залишкові продукти сільськогосподарського виробництва (у т. ч. тваринництва);
- бракована, некондиційна продукція усіх видів економічної діяльності або продукція, забруднена небезпечними речовинами і непридатна до використання;
- неідентифікована продукція, застосування або вживання якої може спричинити непередбачені наслідки (мінеральні добрива, отрутохімікати та ін.);
- зіпсовані (пошкоджені), фізично або морально зношені вироби, які втратили свої споживчі властивості (відходи споживання);
- залишки продуктів харчування, побутових речей, пакувальних матеріалів тощо (побутові відходи);
- осади очисних промислових споруд, споруд комунальних та інших служб;
- залишки від медичного та ветеринарного обслуговування, медичної та хіміко-фармацевтичної промисловості, аптечної справи;
- матеріальні об’єкти та субстанції, радіоактивне забруднення яких перевищує межі, встановлені чинними нормами (радіоактивні відходи).

В окрему категорію відходів виділяють небезпечні відходи, що мають такі

фізичні, хімічні, біологічні чи інші властивості, які створюють або можуть створити значну небезпеку для навколишнього природного середовища і здоров'я людини та потребують спеціальних методів і засобів поводження з ними.

За своїм фізико-хімічним складом відходи діляться на: тверді, рідкі та газоподібні.

➢ До *газоподібних відходів* відносяться гази, що утворюються при розкладанні сміття або гази, що виходять з підприємств.

➢ *Рідкі відходи* – це, як правило, речовини, розчинені у воді, що скидається у відкриті водойми, каналізацію або надходять на очисні споруди, де вони перетворюються у тверді опади.

➢ *Тверді відходи* – категорія промислово-побутових відходів, які не можна видалити системами каналізації, а тільки вивезенням з подальшим захороненням або частковою утилізацією. Тверді відходи включають використані пакувальні матеріали, непридатні побутові та промислові прилади, папір, консервні банки, бите скло, сміття, старий одяг і взуття, іграшки, залишки їжі, металеві вироби, які не підлягають ремонту, уламки будівельних матеріалів і т.п., деталі й залишки індивідуальних транспортних засобів, меблів.

За даними ООН, в містах тверді відходи становлять щорічно більше 1000 кг на душу населення з тенденцією до збільшення.

Усі відходи в залежності від джерел їх утворення поділяються на промислові (виробничі) і побутові (комунальні).

➢ *Побутові відходи* – це всі відходи сфери споживання, які утворюються в житлових кварталах, організаціях, установах, торгових підприємствах і т.д., відходи опалювальних установок в житлових будинках, сміття з вулиць, будівництв, ремонтуються будівель і інше. Існує тенденція збільшення кількості побутових відходів, що вимагає вирішення питань вивезення, захоронення або утилізація на сміттєпереробних або спалюють сміття заводах.

➢ *Відходи виробництва* – залишки сировини, матеріалів або напівфабрикатів, які утворюються в процесі виготовлення продукції і втратили повністю або частково корисні або фізичні властивості, а також продукти, що утворилися в результаті фізико-хімічної переробки сировини, видобутку і збагачення корисних копалин, отримання яких не є метою даного виробничого процесу.

Виробничі відходи, в свою чергу, діляться на безповоротні, які не можуть бути використані при даному рівні розвитку техніки, і поворотні.

Таким чином, відходи слід розглядати з двох позицій:

По-перше, це – недовикористана сировина. Як відомо, в багатьох відвалах видобувних підприємств вміст корисних речовин більше, ніж в рудах, а на промислові чи побутові звалища попадає велика кількість паперу, пластмаси, металів, дерева. В даний час відходи є багатим невживаним ресурсом з точки зору сировинного потенціалу та одним з найбільш економічно вигідних видів сировини з точки зору її переробки.

По-друге, відходи – один із суттєвих джерел забруднення навколишнього

середовища (атмосфери, води, в тому числі підземної, ґрунту) шкідливими або навіть небезпечними речовинами, які вимагають виділення значних коштів на ліквідацію наслідків. Таким чином, накопичення відходів супроводжується подвійним економічним збитком.

Основним напрямом вирішення проблеми позбавлення відходів є застосування у всіх галузях господарства безвідходної технології, перехід на утилізаційні методи. На жаль, поки що для переважної більшості підприємств можна говорити лише про застосування маловідходної технології, і тому утворені виробничі та побутові відходи доводиться складувати.

3. ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ ТЕХНОЛОГІЙ ПЕРЕРОБКИ ТВЕРДИХ ПОБУТОВИХ ТА ВИРОБНИЧИХ ВІДХОДІВ (ТПВВ)

Практика показує, що не існує універсального методу поводження з твердими відходами, який би задовольняв сучасні екологічні та економічні вимоги. Найбільш прийнятним є комбінований метод, який передбачає використання відходів як джерела енергії та вторинної сировини. Саме комплексна переробка ТПВВ, що передбачає сортування, термообробку, ферментацію та інші процеси, забезпечує максимальну екологічну та економічну ефективність.

Найпоширенішими видами промислової переробки ТПВВ є *спалювання*, *ферментація*, *сортування* та *їх різні комбінації*.

Економічні показники різних технологій переробки ТПВВ (за даними європейських фірм) наведені у таблиці 5.2.

Аналізуючи наведені дані, слід зазначити, що кращими в економічному плані є комбінаційні технічні рішення, особливо комплексна переробка ТПВВ.

Для науково обґрунтованого вибору технології слід враховувати не лише економічні, а й екологічні фактори. Кінцеві продукти переробки й відходи виробництва мають бути безпечними для навколишнього середовища.

Серед існуючих технологій переробки ТПВВ найбільш небезпечним для довкілля є технології ферментації та спалювання вихідних ТПВВ. Основним недоліком технології *ферментації* вихідних ТПВВ без їх попереднього сортування та підготовки є велика кількість відходів, які підлягають складуванню на полігоні, а також доволі низька якість готового продукту. Він має поганий товарний вигляд, підвищений вміст важких металів. Підвищити ефективність технології можна за рахунок сортування ТПВВ перед ферментацією.

При використанні технології *спалювання* ТПВВ утворюються шлак й летюча зола, а також димові гази. Через підвищений вміст у шлаці важких металів його досить важко утилізувати. Попереднє сортування зменшує кількість шлаку та золи, до того ж переробка шлаку стає менш проблематичною.

За технологією *комплексної переробки* ТПВВ до термообробки надходять не вихідні ТПВВ, а їх збагачена фракція, з якої здебільшого видалені шкідливі

речовини. Обсяги димових газів і викиди пилу значно зменшуються.

Отже, сучасним економічним та екологічним вимогам найбільше відповідають технології комплексної переробки ТПВВ. Для практичного застосування комплексної переробки необхідні обґрунтування вибору технічних рішень та їх системне об'єднання. У результаті комплексної переробки ТПВВ утворюються шлаки, зола та відходи сортування, які є екологічно небезпечними і потребують знешкодження.

Таблиця 5.2

Економічна ефективність різних технологій переробки ТПВВ

Показник	Технологія					
	спалювання	*ферментація*	*сортування*	*сортування+ спалювання*	*сортування+ ферментація*	*комплексна переробка*
Капіталовкладення на 1 т ТПВВ, $/т	280	90	50	330	100	240
Експлуатаційні витрати на 1 т ТПВВ, $/т	9,6	10	3,2	12,8	8,7	13,5
Неутилізована фракція, що підлягає захороненню, %	30	30	95	15	55	8
Витрати на захоронення неутилізованої фракції, $/т	9	9	28,5	4,5	16,5	2,4
Капітальні витрати, $/т	28	9	5	33	10	24
Загальні витрати, $/т	46,6	28	36,7	50,3	35,2	39,9
Реалізація продукція з 1 т ТПВВ, $/т	23,7	9,2	11,4	33,9	18,7	30,2
Економічна ефективність технології, $/т	-22,9	-18,8	-25,3	-16,4	-16,5	-9,7

Існує декілька промислових і близьких до промислового застосування технологій знешкодження й переробки відходів, у складі яких переважають мінеральні речовини. Універсальним методом, який майже не залежить від складу відходів, є *електропереплавляння* з подальшим склінням. Недоліком застосування цієї технології є великі витрати електроенергії.

Для переробки летючої золи можна використовувати *технологію виробництва без випалювальних вогнетривів*.

Технології комплексної переробки ТПВВ можуть бути маловідходними, якщо у технологічну схему заводу внести виробництво будівельних матеріалів.

Таким чином, ключовим процесом у схемі комплексної переробки ТПВВ є сортування (у тому числі на основі селективного збору), яке якісно й кількісно змінює склад ТПВВ. При цьому не тільки підвищується частка вторинного використання багатьох компонентів ТПВВ, й значною мірою вирішуються питання видалення небезпечних побутових відходів і баластних компонентів,

оптимальної підготовки тих чи інших фракцій компонентів ТПВВ для подальшої переробки.

4. УТИЛІЗАЦІЯ ВІДХОДІВ ЯК ОДИН ІЗ ШЛЯХІВ ЕКОЛОГІЗАЦІЇ ВИРОБНИЦТВА

Сфера поводження з відходами охоплює всі види діяльності, пов'язані з утворенням, збиранням, зберіганням, використанням, знешкодженням, транспортуванням і захороненням відходів.

Утилізація відходів є важливим елементом в загальному ланцюзі створення систем безвідходних виробництв. Вона передбачає залучення різних типів відходів у нові технологічні цикли або їх використання в інших корисних цілях. Екологізація виробництва неможлива без доповнення виробничих комплексів спеціальними об'єктами, призначеними для переробки всіх видів промислових і побутових відходів.

Ступінь утилізації відходів кожного виробництва або виду діяльності слід розглядати як один з важливих показників, що характеризують екологічність відповідних виробництв, тобто ступінь їх впливу на навколишнє середовище і повноту використання природних ресурсів.

В цілому можна виділити два важливих аспекти утилізації відходів – екологічний і економічний.

➢ *Екологічний аспект* полягає в тому, що організація утилізації відходів сприяє скороченню виділення в навколишнє середовище шкідливих речовин, зниженню масштабів негативного впливу виробництва на стан ландшафту, тваринного і рослинного світу і т.д. Усе це супроводжується зниженням забруднення повітряного і водного басейнів, збереженням ландшафту, вивільненням території в результаті ліквідації відвалів і т.д.

➢ *Економічний аспект* утилізації відходів відображає передусім можливість отримання додаткового джерела тієї чи іншої корисної продукції для задоволення потреб народного господарства, можливість зниження собівартості одержуваної в результаті утилізації відходів продукції за рахунок використання більш дешевої сировини та ін.

5. СПОСОБИ УТИЛІЗАЦІЇ ПОБУТОВИХ ТА ВИРОБНИЧИХ ВІДХОДІВ

Утилізація – це перероблення відходів з метою раціонального використання. У цьому випадку відходи є вторинною сировиною.

Утилізацію поділяють на три різновиди: первинну, вторинну та змішану. Під *первинною утилізацією* розуміють використання відходів у різних галузях народного господарства без попередньої глибокої фізико-хімічної переробки; під *вторинною* – використання продуктів спеціальної переробки відходів. У

результаті процесів вторинної утилізації утворюються продукти іншого складу, ніж вихідні відходи. *Утилізація змішаного типу* включає як первинну, так і вторинну утилізацію.

Переваги і недоліки способів утилізації відходів:

➢ **1. Утилізація відходів: складування.**

Переваги

- Не вимагає постійних і великих капіталовкладень.
- Місця складування відходів можуть не оновлюватися десятиліттями.
- Дозволяють одночасно позбутися великої кількості твердих побутових чи промислових відходів.
- Результати руйнівного впливу звалищ на природу не видно відразу.

Недоліки

- Витрати на боротьбу з наслідками згубного впливу звалищ, тобто на охорону природи, охорону здоров'я, у багато разів перевищують витрати на будівництво заводів з переробки твердих побутових відходів.
- Звалища для утилізації відходів постійно розростаються і на них ідуть все нові величезні території. Кількість звалищ безперервно збільшується.
- Тверді побутові та промислові відходи, що розкладаються на звалищах, проникають у ґрунт, тим самим, заражаючи його. Отруйні випари забруднюють повітря. Залишки твердих побутових відходів потрапляють у водойми і згубно позначаються на стані води, шкодять флорі та фауні цих водойм. Всі ці наслідки негативно впливають на здоров'я людини, порушують обмінні процеси в природі.
- Наслідки руйнівного впливу звалищ на природу можуть виявитися необоротними в майбутньому.

➢ **2. Утилізація відходів: захоронення.**

Переваги

- Дозволяє забути про проблему утилізації відходів. Створюється видимість відсутності проблеми – якщо закопати тверді побутові відходи, то вони зникнуть.
- Не потрібні нові величезні території.
- Не вимагає постійних і великих капіталовкладень.

Недоліки

- Відходи, що знаходяться в ґрунті, отруюють її, потрапляючи через підземні води у водойми, представляють величезну небезпеку для людини і тварин.
- Підземні звалища не помітні, на перший погляд, але на поверхні землі над ними ґрунт отруєний і розпушений, він не придатний ні для будівництва, ні для землеробства, ні для випасу худоби. Більше того з поверхні ґрунтів над звалищами часто випаровуються їдкі токсичні речовини.
- Витрати на боротьбу з наслідками згубного впливу поховань відходів, тобто на охорону природи, охорону здоров'я, у багато разів перевищують витрати на будівництво заводів з переробки твердих побутових відходів.

➢ **3. Утилізація відходів: зливання водойми.**

Переваги

- Не вимагає великих одноразових капіталовкладень.
- Злиті відходи швидко поширюються по поверхні води, швидко осідають на дно, розчиняються, створюючи видимість чистоти.
- При блокуванні місць зливу відходів, отруйні речовини поширюються не відразу і не помітно.

Недоліки

- Затрати на очищення води, фільтрацію; збитки для риболовецької промисловості, водного транспорту у багато разів перевищать витрати на будівництво заводів з переробки та утилізації відходів.
- По поверхні води, по дну водойм продукти розкладання відходів поширюються на величезні відстані, отруюючи акваторію, роблячи її непридатною для життя риб, для використання в промисловості. Розчинені у воді їдкі, а часом і токсичні відходи вкрай небезпечні для тварин і людини.
- Блокування місць зливу відходів вселяє людям спокій, притупляє пильність, це призводить до того, що поширенню отруйних речовин ніхто не перешкоджає.

➢ **4. Утилізація відходів: спалювання.**

Переваги

- Дозволяє одноразово позбутися великої кількості сміття.
- Зручно у великих містах і на великих підприємствах, так як дозволяє позбуватися від відходів у міру їх надходження.
- Після спалювання відходів залишається отруйний попіл, який, згодом, теж доводиться утилізувати одним з вище перерахованих способів.

Недоліки

- Отруйні гази, що викидаються в атмосферу з димом, спричиняють важкі захворювання у людей, сприяють утворенню озонових дір.
- Через постійні викиди диму в атмосферу над містами та підприємствами утворюються щільні димові завіси.

➢ **5. Утилізація відходів: переробка.**

Не дивлячись, на всі перераховані вище способи утилізації, існує ще один спосіб – це вторинна переробка. Причому цей спосіб найбільш ефективний, так як він є не лише екологічно чистим, а й ресурсозберігаючим.

Приклад: Вторинна переробка поліетилентерефталату в Японії.

Компанія «Негдю Санге» в Японії з початку 80-х років почала виробляти зі старих поліетилентерефталанових виробів (ПЕТ) поліефірні волокна. Процес вторинного використання ПЕТ нескінченний. Виготовивши одного разу з відходів ПЕТ-килимок, його після зносу можна переробити в килимове покриття для багажників автомобілів, і так далі. Японська фірма «Мідзуно» з вторинного поліефіру (вміст більше 50%) виробляє спортивний одяг для школярів, кросівки зі штучної шкіри (40% вторинного поліефіру). Фірма «Гундзе» з ефірного матеріалу

виробляє скатертини, кухонні рукавиці, ковпачки для чайників, підставки і т.д. Компанія «Одзакі Седзі» з пряжі, що складається з 70% поліефіру і 30% вовни, виготовляє шкільну форму, причому на виготовлення дорослого комплекту форми йде близько 15 пластикових пляшок. Корпорація «Лайон Офіс Профктс» пішла далі – вона виробляє тканинні покриття і матеріал подушок для офісних стільців, полиці для папок і книг зі стовідсотково вторинної пластмаси. Причому стільці легко розбираються, і більшість їх деталей можна використовувати повторно.

Але вдруге переробляти можна не тільки поліетилентерефталат. Так вдруге можна використовувати скло, металобрухт і ті ж харчові відходи.

Тема 6: «ОЦІНЮВАННЯ ЕКОЛОГО-ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА»

1. ЕКОНОМІЧНЕ РЕГУЛЮВАННЯ ЕКОЛОГІЧНОЇ ДІЯЛЬНОСТІ.

Засади економічного механізму забезпечення охорони навколишнього природного середовища зафіксовані в X розділі Закону України «Про охорону навколишнього середовища». Перевага надається екологічному нормуванню, лімітуванню, ліцензуванню, експертизі, контролю, тобто забезпеченню виконання відповідних стандартів і норм примусом із боку держави, що не спонукає підприємства, установи й організації до здійснення природоохоронної діяльності.

На сучасному етапі розвитку економіки можна виділити такі елементи економічного механізму регулювання природоохоронної діяльності:

- плата за природокористування;
- система економічного стимулювання природоохоронної діяльності;
- плата за забруднення навколишнього середовища та розміщення відходів;
- створення ринку природних ресурсів;
- удосконалення системи ціноутворення з урахуванням екологічних факторів, особливо на продукцію природо експлуатуючих галузей народного господарства;
- створення екологічних фондів;
- екологічне програмування;
- торгівля ліцензіями;
- платежі за заставу;
- екологічне страхування.

Основною метою економічних механізмів природокористування та природоохоронної діяльності є:

- стимулювання шляхом впровадження еколого-економічних інструментів природокористувачів до зменшення шкідливого впливу на довкілля, раціонального та ощадливого використання природних ресурсів і зменшення енерго- і ресурсомісткості одиниці продукції;
- створення за рахунок коштів, отриманих від екологічних зборів і платежів, незалежного від державного та місцевих бюджетів джерела фінансування природоохоронних заходів і робіт.

Економічний механізм екологічного регулювання в Україні ґрунтується на концепції платності природокористування.

Система платежів за користування природними ресурсами включає в себе не тільки способи визначення розмірів плати, а також механізми її встановлення, вилучення й використання.

Розрізняють шість видів платежів за ресурсами:

1. Платежі за право користування природними ресурсами.

2. Плата за відтворення та охорону природних ресурсів.

3. Рентні платежі за експлуатацію кращих природних ресурсів за якістю чи за місцем їх розташування стосовно ринку.

4. Штрафні платежі за понаднормове використання природних ресурсів.

5. Компенсаційні платежі за вибуття природних ресурсів із цільового використання або погіршення їхньої якості, спричинене діяльністю цих підприємств.

6. Плата підприємств за використання середовища для розміщення відходів виробництва.

Плата за користування природними ресурсами повинна залежити від умов, які визначають попит і пропозицію на цей ресурс на конкретній території, і вилучатися у вигляді конкретного податку (збору) або плати за ліцензію, що дає таке право, чи у вигляді орендної плати.

Використання природних ресурсів в Україні здійснюється в порядку загального та спеціального використання. Законодавством України громадянам гарантується право загального використання природних ресурсів для задоволення життєво необхідних потреб (естетичних, оздоровчих, рекреаційних, матеріальних) безоплатно, без закріплення цих ресурсів за окремими особами й надання відповідних дозволів.

У порядку спеціального використання природних ресурсів громадянам, підприємствам, установам, організаціям надаються у володіння, користування або оренду природні ресурси на підставі спеціальних дозволів у формі ліцензій, зареєстрованих в установленому порядку за плату для здійснення виробничої діяльності, а у випадках, передбачених законодавством – на пільгових умовах.

Ліцензія є документом, який засвідчує право її власника на використання природних ресурсів у визначених межах, з відповідно вказаною метою протягом встановленого строку під час додержання ним заздалегідь визначених вимог та умов.

Штраф – це покарання винного, а не відшкодування збитків, завданих природному середовищу. Суттєвим недоліком штрафних санкцій є також обмежений характер їхньої дії. Штраф платиться один раз, а порушення навколишнього природного середовища тривають.

Плата за відтворення (компенсацію) природного ресурсу повинна залежати від середовища утворюючої ролі й визначатися затратами на підтримання заданого рівня якості навколишнього природного середовища з урахуванням встановлених для даного регіону пріоритетів розвитку та фактора часу.

Платежі на відтворення й охорону природних ресурсів – це компенсація затрат природних ресурсів (вилучення) у процесі виробництва.

Критерієм для розрахунку платежів за забруднення є збитки від цього. Ці збитки проявляються рівночасно в моральному, соціальному, естетичному, натуральному, економічному аспектах. Здебільшого оцінюються економічні збитки.

Економічні збитки від шкідливого впливу на навколишнє середовище

відходів виробництва – фактичні або можливі витрати на компенсацію цих утрат.

Забруднення навколишнього середовища призводить до виникнення двох видів витрат: на попередження впливу на забруднення середовища та на попередження впливу на забруднення середовища на них.

Економічні збитки величина комплексна. Найчастіше їх виражають сумою основних локальних збитків:

a) від погіршення здоров'я населення;

b) комунальному господарству;

c) сільському та лісовому господарствам;

d) промисловості.

Платежі від забруднення навколишнього природного середовища та раціональне використання природних ресурсів виконують такі функції:

- перенесення економічного тягаря збитків, пов'язаних із забрудненням навколишнього природного середовища, на ті суб'єкти господарювання, що спричиняють ці збитки (вилучення частини прибутку, який отримано унаслідок експлуатації навколишнього середовища та компенсація збитків, що завдаються цією експлуатацією);
- узгодження розміру прибутків і фондів матеріального заохочення з ефективністю природоохоронної діяльності;
- спонукання підприємства до зниження збитків (відповідно, негативного техногенного навантаження на природне середовище) шляхом ефективного освоєння коштів на спорудження й обслуговування природоохоронних об'єктів, на придбання обладнання та приладів зі знешкодження забруднюючих речовин.

В Україні фінансування заходів щодо охорони навколишнього природного середовища здійснюється за рахунок:

- державного бюджету України та місцевих бюджетів;
- коштів підприємств, установ та організацій;
- позабюджетних фондів охорони навколишнього природного середовища;
- добровільних внесків та інших коштів.

Нормативи плати за використання природних ресурсів визначаються з урахуванням їхнього географічного положення, поширення, якості, можливості відтворення, доступності, комплексності, продуктивності, можливості утилізації, відходів, умов переробки.

Економічні оцінки природних ресурсів і плата за природні ресурси часто збігаються, але це не означає, що вони є тотожними за економічним змістом. Більшість дослідників сходяться на думці, що показники економічної оцінки мають бути порівняльними, тобто давати змогу порівнювати різні джерела однойменних ресурсів і варіанти їх використання.

2. ПЛАТЕЖІ ЗА ЗАБРУДНЕННЯ НАВКОЛИШНЬОГО СЕРЕДОВИЩА ПІДПРИЄМСТВА.

Платежі за забруднення навколишнього середовища є складовою частиною фінансового механізму охорони довкілля та раціонального використання природних ресурсів. Основу платежів становлять нормативи плати за забруднення навколишнього середовища.

Згідно з Методикою визначення розмірів плати і стягнення платежів за забруднення навколишнього середовища України нормативи встановлюються за:

- викиди в атмосферу забруднювальних речовин стаціонарними і пересувними джерелами забруднення;
- скиди забруднювальних речовин у поверхневі води, територіальні та внутрішні морські води, а також підземні горизонти, в тому числі скиди, що проводяться підприємствами через систему комунальної каналізації;
- розміщення відходів промислового, сільськогосподарського, будівельного та іншого виробництва.

Характер забруднення навколишнього середовища дуже різноманітний і не завжди піддається кількісному обліку. Втрати від забруднення можна класифікувати за двома видами: економічний і соціальний.

Економічні втрати спричиняються через погіршення виробництва певних об'єктів і втрат продукції; соціальні — як наслідок негативного впливу на здоров'я та життєдіяльність людини (хвороби, втрати працездатності, велика смертність).

Сучасна політика держав в галузі охорони навколишнього середовища від забруднення будується на принципі «забруднювач платить». В цьому принципі відображена політика покладення на забруднювачів відповідальності за всі дії, що спричиняють шкоду навколишньому середовищу.

Вперше на міжнародному рівні принцип «забруднювач платить» був обґрунтований Організацією економічного співтовариства і розвитку в 1972 році. З цього часу вказаний принцип став активно використовуватись в законодавчій практиці європейських та інших країн світу.

В Україні принцип «забруднювач платить» було запроваджено в 1991 році Законом України «Про охорону навколишнього природного середовища», стаття 44 якого встановила, що в Україні здійснюється плата за забруднення навколишнього природного середовища. Безпосередньо механізм визначення плати і стягнення платежів за забруднення довкілля був урегульований Постановою Кабінету Міністрів України від 13 січня 1992 р. та відповідною

Постановою від 1 березня 1999 року, якими затверджено Порядок встановлення нормативів збору і стягнення платежів за забруднення навколишнього середовища.

В системі регулювання суспільних відносин в галузі охорони довкілля плата за забруднення несе велике різноманітне навантаження — стимулююче, координаційне, контролююче та компенсаційне.

Стимулюючий бік плати за забруднення виявляється в її впливі на економічні інтереси екологічно небезпечних підприємств шляхом підвищення або

зменшення економічного тиску на них в залежності від обсягів викидів (скидів) в довкілля (чим більше обсяг викиду — тим вища плата). Для цього використовуються два види плати:

а) за лімітові викиди (скиди) — в межах встановлених лімітів (тимчасового походження) викидів (скидів) забруднюючих речовин та згідно з дозволами на розміщення відходів в навколишньому середовищі. Щодо цих лімітованих викидів (скидів) встановлюються фіксовані нормативи плати;

б) за перевищення лімітів викидів (скидів), розміщення забруднювальних речовин. Тут плата визначається в кратному розмірі відносно до фіксованих платежів.

Розміри платежів за забруднення навколишнього природного середовища встановлюються на підставі лімітів та фактичних обсягів викидів і скидів забруднювальних речовин, розміщення відходів, а також базових нормативів плати за них і відповідних регулювальних коефіцієнтів.

Плата за забруднення навколишнього середовища в межах установлених лімітів корегується за регіонами України із застосуванням коефіцієнтів, що враховують територіальні екологічні особливості, та коефіцієнтів індексації базових нормативів плати.

За понадлімітні викиди і скиди забруднювальних речовин і розміщення відходів установлюється підвищений розмір плати на підставі базового нормативу плати, коефіцієнта індексації, коефіцієнтів, що враховують територіальні екологічні особливості, і коефіцієнтів кратності плати за понадлімітні викиди і скиди забруднювальних речовин і розміщення відходів. У разі відсутності на підприємстві затверджених у встановленому порядку лімітів викидів і скидів забруднювальних речовин та розміщення відходів нормативи плати за викиди і скиди забруднювальних речовин та розміщення відходів установлюються як за понадлімітні.

Платежі підприємств за викиди і скиди забруднювальних речовин і розміщення відходів у межах встановлених лімітів (тимчасово погоджених величин) відносяться на витрати виробництва, а при перевищенні лімітів провадяться за рахунок прибутку, що залишається у розпорядженні підприємств.

Крім цього, законом також передбачено платежі за пошкодження природних ресурсів (зниження родючості ґрунтів, продуктивності лісу і водоймищ) відповідно до встановлених нормативів.

Відповідні платежі стягуються з підприємств незалежно від форм власності і відомчої належності. Внесення плати за забруднення не звільняє підприємства від дотримання заходів по охороні навколишнього середовища, а також сплати штрафних санкцій за екологічні правопорушення і від повного відшкодування шкоди.

Водні ресурси. Платежі за скиди забруднювальних речовин у поверхневі води, територіальні та внутрішні морські води, а також підземні горизонти компенсують економічні збитки від негативного впливу забруднених вод на здоров’я людей, об’єкти житлово-комунального господарства,

сільськогосподарські угіддя, водні, лісові, рибні і рекреаційні ресурси.

Складовими розміру платежу за скиди забруднювальних речовин у поверхневі води, територіальні та внутрішні морські води, а також підземні горизонти є:

- плата в межах установлених лімітів (тимчасово погоджених) скидів забруднювальних речовин;
- плата за перевищення лімітів скидів забруднювальних речовин.

До 1991 року в Україні економічні санкції за скидання забруднювальних речовин у водні об'єкти не застосовувались.

В 1992—1993 рр. Міністерством охорони навколишнього природного середовища затверджені «Базові нормативи плати за забруднення навколишнього природного середовища України» та «Методика визначення розмірів плати і стягнення платежів за забруднення навколишнього природного середовища».

Сьогодні ці нормативні акти є тими документами для регламентації, які визначають правові, організаційні та економічні умови функціонування механізму плати за екологічні порушення при водокористуванні.

При введенні базових нормативів плати за забруднення вод було значно скорочено (з 200 до 27) перелік визначених і встановлених раніше ставок плати. Речовини, які не ввійшли до цього переліку, визначались за таблицею гранично допустимих концентрацій (ГДК) у воді забруднювальних речовин та класу їх небезпечності. Це в свою чергу спонукало водокористувачів до розроблення екологічних нормативів гранично допустимих скидів (ГДС) забруднювальних речовин.

На сьогодні діють ставки базових нормативів плати за скиди забруднювальних речовин у поверхневі, територіальні і внутрішні морські води та у підземні горизонти.

Ліміти скидів забруднювальних речовин визначаються для підприємств з урахуванням гранично допустимих обсягів скидів по кожному інгредієнту і доводяться до них як тимчасово погоджені величини скидів забруднювальних речовин по кожному інгредієнту в тоннах за рік.

Тимчасово погоджені скиди (ТПС) — це кількість забруднювальних речовин, що скидаються у водні об'єкти з окремого джерела забруднення за одиницю часу. ТПС встановлюється на відповідний термін — до досягнення гранично допустимих скидів (ГДС). Гранично допустимі скиди з урахуванням дії інших джерел забруднення та перспективи розвитку підприємства не перевищують встановлених норм екологічної безпеки людини.

Ліміти скидів забруднювальних речовин у водні об'єкти загальнодержавного значення встановлюються на 1 рік органами Міністерства охорони навколишнього природного середовища України у формі видачі підприємствам відповідних дозволів; для водних об'єктів місцевого значення вони встановлюються для підприємств за поданням органів Міністерства охорони навколишнього природного середовища України у порядку, що визначається органами місцевої влади.

Нормативом плати за скиди забруднювальних речовин є розмір плати за 1 т конкретної речовини.

За скиди забруднювальних речовин у межах визначених лімітів встановлюються базові нормативи плати і коефіцієнти, що враховують територіальні екологічні особливості.

За понадлімітні скиди забруднювальних речовин встановлюється підвищений розмір плати на підставі базових нормативів плати, коефіцієнтів, що враховують територіальні екологічні особливості, і коефіцієнтів кратності плати за понадлімітні скиди забруднювальних речовин.

Коефіцієнт кратності плати за понадлімітні скиди забруднювальних речовин встановлюється радами народних депутатів базового рівня (село, селище, місто) в межах від 1 до 5, у разі відсутності на підприємстві затверджених лімітів скидів забруднювальних речовин плата за ці скиди стягується як за понадлімітні.

Платежі підприємств за скиди забруднювальних речовин у межах лімітів відносяться на собівартість продукції, а та частина загальної суми, що припадає на понадлімітне забруднення, здійснюється за рахунок доходів підприємства.

Збитки від забруднення атмосфери. Платежі за викиди в атмосферу забруднювальних речовин стаціонарними джерелами забруднення компенсують економічні збитки від негативного впливу забрудненого атмосферного повітря на здоров'я людей, об'єкти житлово-комунального господарства (житловий фонд, міський транспорт, зелені насадження тощо), сільськогосподарські угіддя, водні, лісові, рибні і рекреаційні ресурси, основні фонди промисловості і транспорту.

Складовими розміру платежу за викиди в атмосферу забруднювальних речовин стаціонарними джерелами забруднення є:

- плата в межах установлених лімітів (тимчасово погоджених) викидів забруднювальних речовин;
- плата за перевищення лімітів викидів забруднювальних речовин.

Платежі за викиди в атмосферу забруднювальних речовин пересувними джерелами забруднення компенсують економічні збитки від негативного впливу забрудненого атмосферного повітря на здоров'я людей, об'єкти житлово-комунального господарства, сільськогосподарські угіддя, лісові, водні, рибні і рекреаційні ресурси, основні фонди промисловості і транспорту.

Розмір платежу за викиди в атмосферу забруднювальних речовин пересувними джерелами забруднення встановлюється на підставі діючих базових нормативів плати за ці викиди та кількості використаного палива.

Платежі за розміщення відходів у навколишньому середовищі компенсують економічні збитки від негативного впливу відходів на здоров'я людей, об'єкти житлово-комунального господарства, сільськогосподарські угіддя, водні, лісові, рибні, рекреаційні ресурси, основні фонди промисловості і транспорту.

Складовими розміру платежів за розміщення відходів у навколишньому середовищі є:

плата в межах установлених лімітів розміщення (згідно з дозволами на розміщення) відходів у навколишньому середовищі;

плата за перевищення лімітів розміщення відходів у навколишньому середовищі.

Головними критеріями визначення економічних збитків є негативні зміни середовища в результаті антропогенної діяльності. При такому підході більш ємним стає поняття забруднення середовища. Економічні збитки як параметр, який відбиває взаємодію виробництва і середовища, може бути розрахований відносно об'єктів господарської діяльності і елементів довкілля, що передбачає наявність системи показників.

Структура показників, які дозволяють оцінити натуральні збитки від забруднення середовища, вельми різноманітна, і формування її у кожному конкретному випадку прямо залежить від обґрунтованої номенклатури одиничних натуральних збитків, що підлягають оцінці. Кожний показник має самостійне значення і не може розглядатися як проста арифметична сума попередніх. При визначенні економічних збитків у конкретному випадку необхідний індивідуальний підхід.

Для інтегрування і застосування в економічних розрахунках натуральні одиничні збитки мають бути приведені до вигляду, який дозволяє їх порівнювати, тобто необхідно провести вартісну оцінку натуральних збитків. З одного боку, вартісні показники відповідають натуральним збиткам, з іншого – розрізняють фактичний, можливий (потенційний) та відвернений збитки.

Фактичні збитки – це втрати і додаткові витрати, які склалися в умовах забруднення середовища. Можливі (потенційні) збитки – економічні збитки, які сформуються в результаті надходження забруднюючих речовин від об'єктів у прогнозному періоді.

Відвернені збитки – це зниження можливих (потенційних) збитків у результаті проектування або проведення заходів із захисту довкілля.

Економічні збитки як комплексний показник, що відбиває особливості взаємодії виробництва з середовищем і здійснює вплив на головні характеристики виробничої діяльності, виконує такі функції:

- облікову – проявляється у тому, що збитки є мірою оцінки впливу господарської діяльності на середовище;
- інвестиційну – виходить з того, що яким би чином не оцінювалися економічні збитки, вони у будь-якому випадку, визначаються розмірами додаткових вкладень матеріальних і трудових витрат, виступають як поточні витрати та капітальні вкладення;
- обмежувальну – проявляється в тому, що об'єкти-забруднювачі прямо (у вигляді штрафів) або побічно (у вигляді подорожчання вихідної сировини, підвищення захворюваності працюючих тощо) відчувають наслідки своєї діяльності. Це потребує відповідних заходів (удосконалення технологій, створення маловідходних виробництв, будівництва очисних споруд тощо) з метою скорочення негативних наслідків власної діяльності;
- стимулюючу – тісно пов'язана з розглянутою функцією. Різного роду

платежі та штрафи, які визначають на основі економічних збитків, стимулюють скорочення забруднення і, відповідно, зменшують витрати об'єктів на компенсацію збитків.

У той же час збитки дозволяють приймати обґрунтовані з економіко-екологічної точки зору рішення щодо можливості і необхідності функціонування об'єктів, черговості освоєння інвестицій на об'єктах.

Економічні збитки як прямі втрати і додаткові витрати, можуть бути завдані населенню безпосередньо, а також опосередковано в результаті зміни умов функціонування господарських об'єктів як наслідок деградації якості середовища. При цьому зміни виробничо-економічних та екологічних властивостей, які визначають натуральні збитки, можуть бути тимчасовими та безповоротними, такими, що завдаються безпосередньо природним ресурсам та побічно через умови їхнього існування.

Основна особливість збитків – це те, що вони завдаються реципієнтам безпосередньо, але для суб'єкта забруднення є зовнішнім (екстерніальним) ефектом, що потребує спеціальних регуляторів для запобігання його прояву у зв'язку з тим, що як реципієнти, так і суспільство в цілому не зацікавлені у формуванні економічних збитків. До таких регуляторів належать платежі за забруднення, фінансування заходів щодо запобігання та ліквідації наслідків забруднення, скорочення негативних наслідків зміни якості середовища.

На території України існують єдині правила встановлення плати за викиди й скиди забруднюючих речовин у навколишнє природне середовище та розміщення в ньому відходів промислового, сільськогосподарського, будівельного та інших виробництв, а також стягнення відповідних платежів з підприємств, установ і організацій. Плата за забруднення навколишнього середовища встановлюється за:

- викиди в атмосферу забруднюючих речовин стаціонарними і пересувними джерелами забруднення;
- скиди забруднюючих речовин у поверхневі води, територіальні та внутрішні морські води, а також підземні горизонти, в тому числі скиди, що здійснюються підприємствами через систему комунальної каналізації;
- розміщення відходів у НПС.

Платежі за викиди й скиди забруднюючих речовин і розміщення відходів у навколишньому природному середовищі стягуються з підприємств незалежно від форм власності й відомчої приналежності. Стягнення платежів не звільняє підприємства від відшкодування збитків, заподіяних порушенням природоохоронного законодавства. Розрізняють дві категорії платежів за забруднення навколишнього середовища:

- платежі за нормативно-допустиме забруднення, тобто за викиди (скиди) речовин в межах норм лімітів (ГДВ, ГДС);
- платежі за нормативні постійні та разові (залпові) викиди (скиди);
- штрафні санкції.

Ліміти розміщення відходів у НПС визначаються для підприємств як

фізичний обсяг відходів за класами їхньої токсичності згідно з дозволами на розміщення, що видаються у встановленому порядку і доводяться в тоннах на рік.

За понадлімітні викиди і скиди забруднюючих речовин і розміщення відходів встановлюється підвищений розмір плати на підставі базових нормативів плати, коефіцієнтів, що враховують територіальні екологічні особливості, і коефіцієнтів кратності плати за понадлімітні викиди й скиди забруднюючих речовин і розміщення відходів.

Коефіцієнти кратності плати за понадлімітні викиди і скиди забруднюючих речовин і розміщення відходів встановлюється радами народних депутатів базового рівня в межах від 1 до 5.

У разі відсутності на підприємстві затверджених у встановленому порядку лімітів викидів і скидів забруднюючих речовин і розміщення відходів, плата за викиди й скиди забруднюючих речовин і розміщення відходів стягується як понадлімітна.

Платежі підприємств за викиди й скиди забруднюючих речовин і розміщення відходів у межах лімітів відносяться на витрати виробництва, а за понадлімітні вилучаються за рахунок прибутку, що залишається в розпорядженні підприємства.

Платежі за забруднення НПС підприємства (крім розташованих у містах республіканського підпорядкування) перераховують у таких розмірах:

- 70 % – у позабюджетні фонди охорони НПС рад народних депутатів базового рівня на окремі рахунки;
- 20 % – у позабюджетні фонди охорони НПС держави та обласних рад народних депутатів на окремі рахунки;
- 10 % – на рахунок державного позабюджетного фонду охорони НПС Міністерства охорони навколишнього середовища України.

3. РОЗРАХУНОК ПЛАТЕЖІВ ЗА ВИКОРИСТАННЯ ПРИРОДНИХ РЕСУРСІВ.

Протягом останніх років в Україні продовжувалась робота з вдосконалення економічного механізму природокористування та природоохоронної діяльності. Не менш важливим напрямом роботи було забезпечення фінансування природоохоронної сфери, головним чином, за рахунок впроваджених зборів за забруднення довкілля та спеціальне використання природних ресурсів. Зокрема, впроваджено базові нормативи плати за користування надрами за видобування корисних копалин та нормативи плати за спеціальне використання водних ресурсів, які затверджені постановами Кабінету Міністрів України від 12 вересня 1997 р. № 1014 та від 8 лютого 1997р. №164.

До цього часу в Україні діяли Тимчасовий порядок справляння плати за спеціальне використання надр при видобуванні корисних копалин та Тимчасові нормативи плати за спеціальне використання прісних поверхневих та підземних

водних ресурсів.

Розвиток економічної реформи в Україні та недосконалість діючого Тимчасового порядку, зокрема, єдиного для всіх видів корисних копалин нормативу в розмірі 1 відсотку ціни реалізованої мінеральної сировини (для вугільної промисловості застосовувався коефіцієнт 0,5), вимагав створення механізму, який відповідав би міжнародним стандартам.

Розроблені нормативи плати за користування надрами для видобування корисних копалин, диференційовані залежно від їх видів, є мінімальною величиною плати, яку користувачі надр мають вносити незалежно від умов і результатів господарювання. Вони розглядаються як базові і в подальшому мають диференціюватися залежно від геологічних особливостей родовищ та умов їх експлуатації.

Зміни в ціноутворенні з часу введення в дію Тимчасових нормативів плати за спеціальне використання водних ресурсів та аналіз практики застосування цих нормативів вимагали запровадження нових постійних нормативів плати.

Сьогодні впроваджені і діють чотири категорії нормативів плати за використання водних ресурсів:

- для поверхневих водних об'єктів, які диференційовані по басейнах рік, включаючи притоки всіх порядків;
- для підземних джерел, які диференційовані по регіонах України. Автономна Республіка Крим, області, райони;
- для потреб гідроенергетики;
- для потреб водного транспорту.

Аналіз діючої в Україні системи плати за спеціальне використання природних ресурсів, зокрема водних І надр, свідчить про те що в порівнянні з зарубіжними це достатньо розвинуті системи.

Проте міністерство продовжує роботу з розвитку і вдосконаленню платежів, зокрема по розробленню:

а) нормативів плати для річок у басейнах основних рік України та їх притоках;

б) нормативів плати за користування надрами для видобування корисних копалин, диференційованих залежно від геологічних особливостей родовищ та умов їх експлуатації;

в) нормативів плати за користування надрами, яке не пов'язане з видобуванням корисних копалин (наприклад підземні нафто-газосховища, склади та ін.).

Що стосується фінансування природоохоронної діяльності, то з метою встановлення єдиного порядку формування видатків, що передбачаються у державному та місцевих бюджетах на природоохоронні заходи, та їх ефективного використання Кабінет Міністрів України за поданням Мінекобезпеки затвердив постановою від 9 липня 1997 р. № 732 Порядок формування головного розділу «Охорона навколишнього природного середовища та ядерна безпека» державного бюджету та фінансування з нього видатків на здійснення природоохоронних

видатків.

Цією ж постановою Раді Міністрів Автономної Республіки Крим, обласним, Київській та Севастопольській міським державним адміністраціям доручено розробити та затвердити порядок формування головного розділу «Охорона навколишнього природного середовища та ядерна безпека» місцевих бюджетів та фінансування з них видатків на здійснення природоохоронних заходів.

Законом України «Про охорону навколишнього природного середовища» визначено, що ресурсні платежі є цільовими і повинні повертатись на відновлення та підтримання цих ресурсів у належному стані.

Важливим джерелом доповнення до фінансування природоохоронної діяльності із Державного бюджету стали Державний, республіканський АР Крим та місцеві фонди охорони навколишнього природного середовища.

З метою забезпечення повноти надходжень коштів до фондів охорони довкілля досягнуто домовленості, що контроль за своєчасністю справляння зборів за забруднення довкілля спільно із місцевими природоохоронними органами здійснюватиме і Державна податкова адміністрація. Саме збори за забруднення довкілля становлять головне джерело формування цих фондів.

Як правило, система зборів за використання природних ресурсів формується на основі декількох ключових елементів:

- *ліцензій* на використання природних ресурсів, тобто дозволів на використання певних кількостей конкретних видів ресурсів; розробляються і затверджуються екологічними підрозділами національних і місцевих рівнів;
- *нормативів* використання природних ресурсів;
- *порядку* зборів;
- *ставок* зборів (платежів) за використання природних ресурсів;
- *системи розподілу* зібраних коштів між різними рівнями господарювання.

Основні компоненти ПЛАТНОГО ПРИРОДОКОРИСТУВАННЯ в Україні:

- *ліцензії* на використання ресурсів;
- *нормативи* використання ресурсів;
- *порядок* збору платежів;
- *ставки* платежів;
- *система розподілення* зібраних коштів.

Плата (збори) за землю. Установлюються три види плати:

(а) за використання земель сільськогосподарського призначення;

(б) плата за використання земель населених пунктів;

(в) плата за вилучення угідь, що надані під непрофільне використання

Плата за використання земель сільськогосподарського призначення.

Ставка земельного податку з одного гектара сільськогосподарських угідь встановлюється у відсотках від їхньої *грошової оцінки* в таких розмірах:

- для ріллі, косовиць і пасовищ - 0,1;
- для багаторічних насаджень - 0,03.

При цьому даються такі визначення використаних термінів:

земельний податок - обов'язковий платіж, що справляється з юридичних і фізичних осіб за користування земельними ділянками;

ставка податку — законодавче визначений річний розмір плати за одиницю площі оподаткованої земельної ділянки;

грошова оцінка - капіталізований рентний дохід із земельної ділянки; розраховується індивідуально за видами земель залежно від їхньої якості, природних умов і розташування ділянок; про величину *грошової оцінки* землі в Україні можна судити з табл. 6.2.

Плата за використання земель населених пунктів.

Ставка земельного податку з земель, грошову оцінку яких визначено, встановлюється в розмірі 1% від їх грошової оцінки.

Для земельних ділянок, грошова оцінка яких не встановлена, встановлюються середні ставки податку залежно від розміру населеного пункту (чисельність населення). Зокрема, для невеликих населених пунктів вона змінюється від 1,5 коп. за 1 м^2 (для пункту в 0,2 тис. чол.) до 4,8 коп. за 1 м^2(для пункту в 10-20 тис. чол.).

У населених пунктах, що належать до категорії курортних, розмір ставок коректується застосуванням поправочного коефіцієнта: Південний берег Криму - 3,0; Південно-Східне узбережжя Криму л 2,5; Західне узбережжя Криму — 2,2; Чорноморське узбережжя Миколаївської, Одеської і Херсонської областей - 2,0; гірські райони і передгір'я Закарпатської, Львівської, Івано-Франківської і Чернівецької обл. - 2,3; узбережжя Азовського моря — 1,5.

У тому випадку, якщо розмір зайнятих ділянок землі *перевищує норми відведення,* ставки податків за наднормативні площі зайнятих земель збільшуються в 5 разів.

Податок за земельні ділянки на територіях та об'єктах природоохоронного, оздоровчого та рекреаційного призначення, зайняті виробничими, культурно-побутовими, господарськими будівлями і спорудами, що не пов'язані з функціональним призначенням цих об'єктів, справляється у 5-кратному розмірі відповідно до встановленого земельного податку.

Плата (збори) за вилучення угідь під непрофільне використання. У Законі «Про плату за землю» цей розділ формулюється так: «Плата за землі промисловості, транспорту, зв'язку, оборони та іншого призначення, а також за землі природоохоронного, оздоровчого, рекреаційного, історико-культурного призначення та за землі лісового і водного фондів (за межами населених пунктів)».

- *Земельний податок* за зазначений вид вилучення земель справляється в розрахунку 5% від грошової оцінки одиниці площі *ріллі* по області.
- Для *залізничного транспорту і військових з'єднань* величина податку встановлена в розмірі 0,02% грошової оцінки *ріллі* по області.
- За *тимчасове* вилучення земель природоохоронного, оздоровчого, рекреаційного й історико-культурного призначення розмір плати становить 50% від грошової оцінки одиниці площі *ріллі* по області.

- Податок за вилучення *лісових угідь* прирівнюється до *плати за використання лісових ресурсів.* У тому випадку, якщо землі *лісового фонду* вилучаються під виробничі, культурно-побутові, житлові і господарські будинки і спорудження, розмір земельного податку становить 0,3% від грошової оцінки одиниці площі ріллі по області.
- Земельний податок за ділянки *водного фонду* складає 0,3% від грошової оцінки одиниці площі *ріллі* по області.

Платежі (збори) за використання надр. Цей вид платежів умовно можна розділити на такі види: а) збір за видачу ліцензій на користування надрами; б) плата за користування надрами; в) відрахування за геологорозвідувальні роботи, що виконуються за рахунок державного бюджету; г) плата за використання підземного простору; ґ) акцизний збір.

(а) Збір за видачу ліцензій справляється, виходячи з розмірів неоподаткованого мінімуму доходів громадян.

(б) Плата за користування надрами.

Установлення зборів за використання *мінеральних ресурсів* пов'язане з реалізацією права державної власності на мінеральні ресурси і необхідністю компенсації витрат на геологорозвідувальні роботи. За допомогою зазначених платежів мають вирішуватися завдання:

- створення джерел фінансування геологорозвідувальних робіт;
- вирівнювання умов господарювання для підприємств, що освоюють різні за якістю родовища;
- узгодження загальнодержавних і регіональних інтересів через відповідний розподіл коштів;
- фінансування заходів з охорони надр та навколишнього природного середовища, а також соціально-економічної та екологічної реабілітації гірничодобувних регіонів;
- формування фонду коштів для дотації за розробку родовищ корисних копалин, що обумовлена суспільними потребами.

(в) Нормативи відрахування за геологорозвідувальні робо ти, що виконуються за рахунок державного бюджету.

(г) Плата за використання підземного простору. Порядок і ставки плати встановлені Постановою Кабінету Міністрів України від 08.11.2000 .№1682. Річні нормативи плати встановлюються окремо для кожного виду використання підземного простору в гривнях на одиницю виміру.

Під об'єкти підземного простору можуть використовуватися природні геологічні утворення: пористі чи тріщинуваті утворення (пласти-колектори; створені та існуючі гірничі виробки (відпрацьовані і пристосовані); природні порожнини (печери).

Плата за використання водних ресурсів. Система плати за водні ресурси була введена Водним кодексом України в 1995 році. Ставки плати кілька разів коректувалися й уточнювалися.

Повна ставка плати (збору) за використання водних ресурсів є сумою двох

ставок:

- за використання води як природного ресурсу і формування доступних для використання ресурсів у системі водопостачання; визначається виходячи з рентної оцінки джерела за економічною ефективністю використання води замикаючими (за соціально-економічним ефектом) водокористувачами;
- за забір води, її очищення і розподіл між водокористувачами в системі водопостачання.
- норматив плати (збору) за спеціальне використання водних ресурсів для потреб *гідроелектроенергетики* становить 0,7грн. за 100 $м^3$ води, пропущеної через турбіни (крім ГАЕС, що функціонують у комплексі з ГЕС);
- нормативи плати (збору) за спеціальне використання водних ресурсів для потреб транспорту становлять:
  - вантажний транспорт - *1,25 коп. за 1 тонно-добу експлуатації флоту;*
  - пасажирський флот - 0,14 коп. за 1 місце-добу експлуатації флоту.

Плата (збори) за спеціальне використання лісових ресурсів. Ставки платежів, на основі яких здійснюється збір за використання лісових ресурсів, називаються *таксами.* Вони були затверджені Постановою КМ України від 20.01.1997 р. №44. *Такси* передбачають попенну оплату, і застосовуються під час відпуску будь-яким заготівельником деревини лісових порід на пні.

Такса — *це* вид ставок за використання лісових ресурсів, що передбачає оплату за кожне дерево, залежно від його діаметра, висоти, якості, зручності заготівель і місця розташування.

При таксації ліси України поділяються на два лісотаксові пояси:

- до *першого* пояса віднесено всі ліси, крім лісів Закарпатської, Івано-Франківської, Чернівецької областей та лісів гірської зони Львівської області;
- до *другого* пояса відносяться ліси Закарпатської, Івано-Франківської, Чернівецької областей та ліси гірської зони Львівської області; такси для цього пояса в середньому на 15% нижчі, ніж для першого.

Залежно від місця розташування ліси поділяються на п'ять лісотаксових *розрядів.* Розряд лісу визначається відстанню від лісосіки до пункту, звідки вивозиться деревина: 1-й розряд - до 10км; 2-й - 10,1-25 км; 3-й - 25,1-40 км; 4-й - 40,1-60 км; 5-й — 60,1 км і більше.

Зазначена відстань може корегуватися залежно від геоморфологічних особливостей місцевості помноженням на відповідні коефіцієнти (що може збільшувати розрахунковий розряд і, отже, знижувати розмір такси):

- ліси з рівнинним рельєфом - 1,10;
- ліси з горбистим рельєфом або ліси, понад 50% площі яких зайнято болотами, - 1,25;
- ліси з гірським рельєфом - 1,5.

Такси встановлюються по кожній лісовій породі і диференціюються залежно від розміру деревини; за цим параметром деревина поділяється на три групи:

велика - відрізки стовбура (у верхньому перетині без кори) діаметром від 25 см і більше;

середня - діаметр від 13 до 24 см;

дрібна - діаметр від 3 до 12 см.

Окремо встановлюються такси для некондиційної, так званої «дров'яної» деревини (вони становлять 25% від такс дрібної ділової деревини). У табл. 7.7 як приклад показані такси для двох характерних порід, які є представниками основних порід (сосна) і неосновних порід (самшит).

Плата (збір) за спеціальне використання об'єктів тваринного світу.

Мисливське господарство. Положення про мисливське господарство і порядок здійснення полювання затверджені Постановою КМ України від 20.07.1996 р. №780.

Положенням обумовлені види мисливських тварин в Україні. Серед основних з них можна назвати:

а) птаха: гагара, лебідь, гусак, качка, дрохва, стрепет, кулик, голуб і ін.;

б) звірі: кріт, кріль, дикий заєць, ондатра, лисиця, вовк, ведмідь, куниця, горностай, барсук, бобер, видра, кабан, лань, олень, козуля, лось, зубр та ін.

Обов'язковими елементами полювання є: одержання *ліцензії* (дозволу) на відстріл, де обумовлені терміни і норми відстрілу; і *оплата* права полювання. Для дрібних тварин (заєць, птах) застосовуються спеціальні картки, за якими можна відстрілювати обумовлену кількість особин у день. Для зайця, наприклад, вартість картки (за якою можна в день відстрілювати 1 особину) коштує 10 грн.

Для великих тварин *плата* за полювання стягується, умовно кажучи в два етапи. На першому купується *ліцензія* на право (але не гарантію) відстрілу.

Вбитий звір продовжує вважатися власністю держави і може бути придбаний мисливцем за діючими на момент полювання розцінкам зі знижкою 30%. Це другий етап оплати. У деяких областях України (наприклад. Волинської обл.) розроблений і впроваджений ще один вид плати - *за використання мисливських угідь.*

Вилов диких тварин. Плата за даним видом діяльності передбачається, головним чином, для тих видів тварин, що можуть становити інтерес з погляду комерційного бізнесу, тобто вилову з метою подальшого продажу. Реалізація зазначеного бізнесу повинна здійснюватися на основі спеціальних дозволів і лише за тими видам тварин, що не занесені в Червону книгу. Тимчасові нормативи плати затверджені Постановою КМ України від 25.01.1996 р. №123 у доларах СІЛА (виплачуються в національній валюті за офіційним курсом Нацбанку на момент оплати). Перелік диких тварин, передбачений даною постановою, включає понад 100 найменувань різних біологічних видів: ссавців, птахів, земноводних, змій, молюсків, метеликів, жуків та інших комах.

Плата за вилучення пташиних яєць встановлена на рівні 50% від величини

плати за відповідний вид. Від плати звільняються наукові установи, зоопарки, а також підприємства і громадяни, що здійснюють спеціальне регулювання чисельності тварин.

Використання риб й інших водних живих ресурсів. Використання зазначених ресурсів регулюється спеціальними дозволами в межах установлених лімітів (квот). Плата (збір) за спеціальне використання рибних і інших водних живих ресурсів зараховується в держбюджет України.

Плата за спеціальне використання рибних та інших водних ресурсів здійснюється в такому порядку: авансовий платіж (до 10% вартості квот) сплачується в момент одержання підприємствами квот вилову; щоквартально здійснюється плата за фактичний вилов живих ресурсів; повний розрахунок за всю квоту після закінчення року. Плата за вилов у межах встановлених квот відноситься на витрати виробництва, а за понадлімітне використання ресурсів плата справляється з прибутку підприємств.

В Україні встановлені збори за такі види природних ресурсів:

• земельні; • мінеральні; • водні; • лісові; • тваринні; • рослинні; • радіочастотний ресурс* *Розподіл зборів.* Співвідношення між частками відрахувань, що перерозподіляються на різні рівні господарювання, для зазначених видів платежів за природні ресурси має такий вигляд (%):

	У держбюджет	В обласні, місцеві бюджети
за землю	30	70
за надра	40	60
за воду	80	20
за лісові ресурси	80	20
за рибні й ін. водні живі ресурси	100	-

Платежі за використання радіочастотного ресурсу України. Ставки одноразових платежів за видачу ліцензій на використання радіочастотного ресурсу України, введені Постановою КМУ від 14.02.2001 № 140. Величина ставки за 1 МГц смуги радіочастот (у гривнях) диференційовані залежно від виду використання ефіру, частотного діапазону і регіону (міст і областей країни).

4. ВИЗНАЧЕННЯ ВИТРАТ НА ВПРОВАДЖЕННЯ СИСТЕМИ ЕКОЛОГІЧНОГО МЕНЕДЖМЕНТУ

Впровадження системи екологічного менеджменту є одним із найвагоміших інструментів на шляху зменшення забруднення навколишнього середовища від підприємств. Метою впровадження СЕМ на підприємстві є мінімізація негативних наслідків його діяльності на навколишнє середовище, досягнення високого рівня екологічної безпеки процесів виробництва технічного обслуговування і ремонту транспортних засобів та послуг, що надаються. При цьому реалізація цих завдань

повинна бути узгоджена з досягненням підприємством інших його пріоритетних цілей, включаючи забезпечення поточної та довгострокової конкурентоспроможності.

У відповідності до рекомендацій ISO 14000 розрізняють такі види діяльності природоохоронного характеру: спрямовані на формування природоохоронної політики, цілей і задач підприємства; пов'язані з організацією природоохоронних функцій підприємства; спрямовані на здійснення планування екологічних заходів щодо всього життєвого циклу продукції і реалізацію розроблених планів; спрямовані на проведення екологічного моніторингу; пов'язані з виявленням оцінки та компенсації соціально-економіко-екологічного збитку, обумовленого забрудненням навколишнього середовища і вилученням природних ресурсів з господарського обігу. Аналіз витрат за названими видами діяльності дає уявлення про загальні витрати підприємства у галузі охорони навколишнього середовища і раціонального використання природних ресурсів.

Витрати являють собою такі, що пов’ язані із забезпеченням та гарантуванням задовільних екологічних показників, а також ті, які пов’язані з втратами у випадках, коли задовільні показники не досягнуто; тобто їх можна умовно поділити на дві загальні групи: витрати, викликані забрудненням навколишнього природного середовища та витрати на запобігання й виявлення випадків забруднення.

Витрати на впровадження СЕМ складаються з витрат (планові витрати на управління навколишнім середовищем, що включають витрати на запобіжні дії та витрати на оцінювання якості навколишнього середовища) й втрат (неочікувані витрати, спричинених дефектами, які усунені в процесі виробництва або після його завершення).

Підсумовуючи викладене, можна отримати структуру витрат на впровадження та функціонування СЕМ (рис. 1).

Варто звернути увагу на декілька важливих аспектів. По-перше, фінансовими ресурсами необхідні витрати не обмежуються, окрім них потрібно враховувати необхідні організаційні і інформаційні ресурси, необхідний час. По-друге, досить помітний вклад дають трудовитрати співробітників організації. По-третє, витрати на підтримку і розвиток СЕМ необхідні і після її впровадження. По-четверте, істотно простіше впроваджувати СЕМ в умовах системи враховувати те, що характер і обсяг витрат залежить від вибраного підходу до впровадження СЕМ (зокрема - від ролі консультантів) і від нього ж, у свою чергу, залежить результативність СЕМ і можливі переваги.

Рис. 6.1. Структура витрат на забезпечення впровадження СЕМ

Витрати на впровадження та функціонування СЕМ можуть бути розділені на три види: витрати самого підприємства, витрати постачальників і споживачів, спільні витрати підприємства і постачальників. При цьому витрати підприємства включають в себе прямі і додаткові витрати. Прямі витрати складаються з чотирьох видів витрат.

Перший вид - попереджувальні витрати (підготовку контролю якості процесів створення екологічно безпечних об'єктів, витрати на обладнання, що використовується для управління екологічною діяльністю; витрати на роботу з кадрами, витрати на заходи в рамках СЕМ підприємства).

Другий вид прямих витрат підприємства - оціночні витрати. (витрати на попередній екологічний аналіз і контроль; витрати на відрядження до постачальників для перевірки екологічної якості компонентів і сировини; витрати на лабораторні перевірки вимірювальних приладів та їх обслуговування; витрати на технічний контроль; витрати на випробування, проведені на фірмі-виробнику; витрати на самоконтроль (перевірку працівниками якості своєї роботи і технологічного процесу); витрати на плановий нагляд за якістю послуг і системою якості; витрати на сертифікацію; витрати на аналіз даних контролю та випробувань; витрати на випробування об'єктів на стадії їх використання за призначенням).

Третій вид прямих витрат підприємства - витрати, пов'язані з внутрішніми, в межах підприємства, відмовами.

Четвертий вид аналізованих витрат - витрати через зовнішні (які відбуваються поза підприємством) відмови.

Крім прямих витрат транспортні підприємства несуть додаткові витрати, пов'язані з якістю обладнання та засобів, що ними експлуатуються і обслуговуються, а також рівнем технологій обслуговування та ремонту. Вони

діляться на непрямі і непередбачені витрати. Непрямі витрати (на додаткові операції в технології, що пов'язані з невпевненістю в екологічній якості, на додаткові операції в контролі і випробуваннях, що пов'язані з невпевненістю в екологічній якості, на матеріали, що витрачені через недосконаліть конструкцій; на матеріали, що витрачені внаслідок недосконалості технологій, на обладнання, що витрачається через недосконаліть конструкцій та технологій; на енергію, що витрачається через недосконаліть конструкцій та технологій; на робочу силу, що використовується через недосконаліть конструкцій і технологій).

Непередбачені додаткові витрати (неплановими витратами через низьку екологічну якість.

Даний вид витрат орієнтовно прогнозується на основі минулого досвіду з урахуванням ймовірності їх зниження в результаті екологічних заходів.

Загальний вид витрат виробників і постачальників компонентів і матеріалів, пов'язаний з необхідністю створення системи інформаційного забезпечення органів з сертифікації, товариств споживачів, банків і кредиторів, посередницьких фірм, комерційних видань, а також органів, що контролюють безпеку населення та навколишнього середовища, достовірність та оперативність інформації про якість послуг.

5. ЦИВІЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА ШКОДУ, ЗАПОДІЯНУ ВНАСЛІДОК ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ОХОРОНУ НАВКОЛИШНЬОГО ПРИРОДНОГО СЕРЕДОВИЩА

Підприємства, установи, організації та громадяни зобов'язані відшкодовувати шкоду, заподіяну ними внаслідок порушення законодавства про охорону навколишнього природного середовища, у порядку та розмірах, встановлених законодавством України (частина 3 статті 68 Закону України про охорону навколишнього природного середовища").

За загальним правилом застосування до винних осіб кримінальної або адміністративної відповідальності не звільняє їх від відшкодування шкоди, завданої порушенням законодавства про охорону навколишнього природного середовища. Ця шкода характеризується як загальними ознаками "шкоди", так і особливими, які властиві лише екологічній шкоді. Загальне визначення шкоди зводиться до віднесення до неї будь-якого знецінення, погіршення, зменшення, знищення блага, що охороняється законом, або ж до розуміння її як несприятливих наслідків, що виникають у результаті порушення майнових або особистих немайнових прав потерпілого. Відповідно до цього визначається й екологічна шкода як сукупність негативних змін у якості та структурі навколишнього природного середовища, або його окремих елементів: псування, знищення, руйнування об'єктів природи, порушення екологічних зв'язків і систем, загальне погіршення стану природного середовища тощо.

Одним із найбільш дискусійних є питання про структуру екологічної

шкоди. Так, гіа думку В.Л. Мунтяна, шкода, заподіяна природним об'єктам, поділяється на дві самостійні частини. Перша складається з вартості матеріально-грошових затрат на природоохоронні заходи на відновлення порушеного стану природи. Друга частина шкоди включає втрати в природному середовищі, що стали результатом виключення життєво важливих функцій окремих його елементів або комплексів. Такі втрати, будучи не відновлювальними, відносно невідновлювальними або важко відновлювальними, не мають грошової оцінки. Як зазначає В.Л. Мунтян, ця шкода дістала назву екологічної на відміну від економічної, яка може бути виражена в грошовій оцінці.

Розвиваючи зазначену концепцію, В.В. Петров також вважав, що шкода, заподіяна порушенням екологічного законодавства, поділяється на економічну й екологічну. Економічна виявляється в загибелі, пошкодженні, знищенні матеріальних цінностей, у неотриманні доходів від використання природного об'єкта, а екологічна - у виснаженні природного середовища, порушенні його екологічних зв'язків. На думку В.В. Петрова, на відміну від економічної шкоди, що виявляється у вартості втрат матеріальних цінностей і передбачуваних доходів, екологічна шкода являє собою складне структурне утворення, що має дві самостійні частини: вартість матеріально-грошових витрат, що використовувалися на охорону природного об'єкта, якому заподіяна шкода, витрат на відновлення порушеного стану природного середовища тощо; вартість екологічних втрат природного середовища, що виникли внаслідок повного чи часткового відключення виконуваної нею життєзабезпечуючих функцій. Такі втрати поділяються на відновлювальні в результаті господарської діяльності, відносно відновлювальні, коли відновлення природних об'єктів пов'язане з тривалими строками (відновлення лісової рослинності), невідновлювальні. Удосконалюючи цю концепцію, Е.М. Жевлаков виділяв "шкоду екологічну та шкоду антропологічну, а також; економічну шкоду, що заподіюється матеріальним інтересам природокористувачів".

Свій погляд на зазначене питання має С.В. Гавриш. При його розгляді він робить акцент на наслідках шкоди - поєднує у собі різні види збитків - природі, людині, економічним структурам. Відповідно до цього виділяється збиток біологічний (збиток екосистем, природному середовищу), який є первинним, а також особистий збиток (збиток життю і здоров'ю людини), економічний збиток (матеріальній сфері життя людей).

По суті, усі зазначені оцінки шкоди, що заподіюється навколишньому природному середовищу, відрізняються між; собою головним чином ступенем диференціації наслідків цієї шкоди. При цьому всі вони збігаються у тому, що оцінка даного роду шкоди має бути комплексною, ураховувати всі аспекти її впливу на стан довкілля, людину безпосередньо, матеріальні інтереси природокористувачів.

З огляду на зазначене можна виділити наступні ключові моменти оцінки та відшкодування шкоди, що заподіюється порушеннями екологічного законодавства.

Найбільш значущими є екологічні наслідки шкоди, що завдається навколишньому природному середовищу. Наприклад, знищення чи пошкодження лісових культур на значних площах лісу негативно впливає на лісові екосистеми, на виконання лісами клімато-регулюючих, водоохоронних та інших функцій. Унаслідок цього можуть погіршуватися екологічні умови життєдіяльності людини, погіршуватися стан інших об'єктів природи.

Відшкодуванню підлягає лише та шкода, що піддається обрахуванню та вираженню або в натуральних або у вартісних показниках. Відшкодування шкоди має здійснюватися шляхом відшкодування її в натурі або відшкодування збитків у повному обсязі (частина 1 статті 1192 Цивільного кодексу України).

Відшкодування в натурі шкоди полягає в тому, що винна особа зобов'язана своїми силами й засобами усунути негативні наслідки заподіяної шкоди (здійснити лісонасадження, рекультивацію землі тощо). Проте покладання на правопорушника обов'язку щодо відшкодування шкоди в натурі можливо лише в тому випадку, коли він має відповідну кваліфікацію, досвід, матеріально-технічну базу для здійснення відповідних природно-відновлювальних робіт, або ж зазначені умови не мають значення в тих чи інших випадках (наприклад, при відновленні лісогосподарських знаків).

Якщо правопорушника не можна зобов'язати відшкодувати шкоду в натурі, то на нього покладається відшкодування збитків у повному обсязі (компенсація збитків). При обрахуванні обсягу відшкодування слід ураховувати: невикористані витрати матеріальних засобів і праці, що раніше вкладені у природний об'єкт (земельну ділянку, ліс, водний об'єкт), витрати на відтворення природних ресурсів (риб, лісу, джерел водопостачання тощо), а також не отримані природо-користувачами доходи.

Важливу роль в обрахуванні обсягу відшкодування виконують спеціальні такси. їх використання зумовлено складністю вирахування втрат, викликаних знищенням або пошкодженням лісу й інших природних ресурсів, необхідністю забезпечувати однаковість відшкодування шкоди у типових випадках.

Зокрема, такси для обчислення розміру шкоди, заподіяної лісовому господарству, затверджені Постановою Кабінету Міністрів України № 1464 від 5 грудня 1996 р. Ці такси (містяться у додатках до Постанови) визначають розмір шкоди, заподіяної лісовому господарству підприємствами, установами, організаціями та громадянами: пошкодженням дерев і чагарників до ступеня неприпинення росту; знищенням або пошкодженням лісових культур, насаджень і молодняку природного походження та самосіву на землях, призначених для лісовідновлення та лісорозведення; знищенням або пошкодженням сіянців і саджанців у лісових насадженнях і на плантаціях; самовільним сінокосінням, випасанням худоби; знищенням і пошкодженням лісогосподарських і відмежувальних знаків; знищенням або пошкодженням мурашників; пошкодженням сіножатей і пасовищних угідь; знищенням або пошкодженням лісо-осушувальних каналів, дренажних систем і шляхів; незаконною рубкою і пошкодженням дерев і чагарників до ступеня припинення росту; самовільною

заготівлею (збиранням) недеревних рослинних ресурсів у порядку спеціального використання, а також загального використання на ділянках, де це заборонено чи допускається тільки за спеціальним дозволом. Кратність розміру такс визначається пропорційно до неоподатковуваних мінімумів доходів громадян та з урахуванням діаметру дерев і залежно від того, у лісах якої групи була заподіяна шкода. Так, за пошкодження дерев і чагарників до ступеня неприпинення росту одного дерева діаметром до 10 см (у корі біля шийки кореня в сантиметрах) - 0,2 щодо лісів першої групи та 0,1 щодо лісів другої групи; до 12,0 неоподатковуваних мінімумів доходів громадян - залежно від групи лісів і т. ін. Передбачено також підвищення розмірів стягнення залежно від породи та якості знищених або пошкоджених дерев і чагарників, а також; здійснення цих правопорушень у гірських лісах Карпат і Криму. Ураховуються при визначенні розміру відшкодування й умови відтворення лісових культур (у природних умовах чи на землях, призначених для лісовідновлення та лісорозведення).

Такси для обчислення розміру компенсації за шкоду, заподіяну знищенням чи пошкодженням рослин з числа видів, занесених до Червоної книги України, Європейського червоного списку тварин і рослин, що перебувають під загрозою зникнення у світовому масштабі, і знищенням їх місцезростання, визначені Постановою Кабінету Міністрів України № 399 від 1 червня 1993 року (у редакції постанови Кабінету Міністрів України № 398 від 16 березня 1999 р.). Для цих видів рослин передбачені більш значні розміри стягнень за заподіяну їм шкоду.

Постановами Кабінету Міністрів України затверджені також такси для обчислення розміру відшкодування збитків, заподіяних унаслідок забруднення із суден, кораблів та інших плавучих засобів територіальних і внутрішніх морських вод України (№ 484 від 3 липня 1995 р.), такси для обчислення розміру відшкодування шкоди, заподіяної порушенням природоохоронного законодавства у межах територій та об'єктів природно-заповідного фонду України (№ 521 від 21 квітня 1998 р.), такси для обчислення розміру шкоди, заподіяної зеленим насадженням у межах міст та інших населених пунктів (№ 559 від 8 квітня 1999 р.) та інші.

МОДУЛЬ 2

Тема 7. ТЕОРЕТИЧНІ ЗАСАДИ ЕКОНОМІЧНОЇ БЕЗПЕКИ БІЗНЕСУ

1. ЕВОЛЮЦІЯ ПОНЯТТЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Як відомо, виробнича система будь-якого суспільства складається з сотень тисяч господарюючих суб'єктів. Тому успішне, повноцінне і ефективне вирішення завдань, які стоять перед економікою держави в цілому, багато в чому залежить від результативності діяльності її виробничих одиниць. Якщо економіка опирається на потужну виробничу базу, на високо розвинуті продуктивні сили та виробничі відносини, здатні успішно добиватися поставлених цілей, то і вся сукупність економічних потреб суспільства буде задовольнятися своєчасно і повною мірою.

Умови ринкової економіки, в яких здійснюють свою діяльність підприємства різних організаційно-правових форм, в значній мірі невизначені і непередбачувані. Тривала і дуже глибока економічна криза породила багато небезпек підприємницькій діяльності і загроз бізнесу, загалом, окремі з яких зароджуються лише зараз. Крім того, на розвиток підприємництва впливають і такі чинники, як нестабільна політична і соціально-економічна ситуація в країні, міжнаціональні, регіональні, територіальні конфлікти, недосконаліть комерційного законодавства, криміналізація суспільства, шахрайство, корупція тощо. Усе це різко загострило проблему забезпечення безпеки підприємства.

У 90-і роки XX ст. у всіх сферах життя України почалися соціально-економічні перетворення, що особливо яскраво позначилися на розвитку економічного середовища країни. Головними напрямками цих перетворень стали формування недержавного сектора в економіці, зміна форм і способів державного регулювання діяльності підприємств, що дозволило використовувати в управлінні підприємствами підходи і принципи, які сформувалися і використовуються в управлінні в розвитих країнах.

Українська економіка успадкувала від колишнього СРСР один з найвищих у світовій економіці рівень концентрації і централізації виробництва, що визначило вибір основної форми реформування економіки – акціонування підприємств. За даними Держкомстату, у 1990 р. підприємства з числом зайнятих більш 1000 чоловік (16,4%) випускали близько 74% промислової продукції. Особливо великі підприємства (понад 10 000 працюючих) виготовляли майже 20% всього обсягу продукції промисловості.

До початку нового тисячоліття в Україні було зареєстровано 12030 відкритих і 22320 закритих акціонерних товариств. Акціонерні товариства

займають домінуюче положення серед всіх інших організаційно-правових форм діяльності підприємств не тільки в українській економіці, але й у країнах з розвинутими ринковими відносинами. Так, в економіці США питома вага продукції корпорацій у валовому внутрішньому національному доході складає близько 90%. В українській економіці з урахуванням складностей перехідного періоду питома вага продукції акціонерних товариств у вартості національного продукту менша. До кінця минулого сторіччя акціонерні підприємства виготовляли в Україні близько 60% загального обсягу промислової продукції. У промисловості України більше 6,0 тис. промислових підприємств (70,2% загальної кількості) працюють у недержавному секторі.

Наслідком зміни сфер і способів державного регулювання діяльності підприємств є значне посилення впливу зовнішнього середовища, перетворення його в головний фактор, що обумовлює стратегію і ділову політику підприємств. У сучасній управлінській літературі зовнішнє середовище визначається як сукупність змінних, що знаходяться за межами підприємства і не є сферою безпосереднього впливу з боку його менеджменту.

В умовах планової економіки зовнішнє середовище підприємств практично цілком було стабільним і прогнозованим, а функції контролю і регулювання діяльності підприємств закріплені за відповідними органами державного управління (міністерствами). В умовах ринкових відносин, що характеризуються високим рівнем невизначеності, зовнішнім середовищем, що постійно змінюється, внутрішнє середовище кожного підприємства формується під впливом змінних зовнішньої середовища, що здійснюють безпосередній вплив на організацію управління і на всі процеси, що протікають на підприємстві. Під впливом зовнішнього середовища змінюються мета діяльності, виробнича база, управління підприємством, організація виробництва, праці і управління, а також протікають основні процеси, що забезпечують розширене відтворення капіталу - інноваційні, інвестиційні, і формуються ринкові позиції підприємства. У цих умовах підприємство розглядається у виді складної ієрархічної системи, тісно взаємодіючої з зовнішнім середовищем.

Вплив зовнішнього середовища на діяльність підприємства може носити різний характер. Найзагальніша систематизація цих впливів дозволяє виділити прямі і непрямі, контрольовані і неконтрольоване впливи, впливи загального і приватного характеру, реально здійснюваний вплив і потенційно можливий вплив, цілеспрямований вплив конкретного елемента зовнішнього середовища і впливу стихійного характеру, що є результатом випадкових процесів і явищ у зовнішнім середовищі.

Прямий вплив зовнішнього середовища виявляється в таких формах, як поведінка постачальників матеріалів, капіталу; зміна процентної ставки інвестицій; зміна законодавства по господарських питаннях, постанови і заходи, впроваджені місцевими органами управління; кон'юнктура ринку (наприклад, розміщення і поводження споживачів; склад і поводження конкурентів).

Непрямий вплив здійснюють, наприклад, політична обстановка в країні або

рівень розвитку науково-технічного прогресу.

Контрольованість впливу зовнішнього середовища визначається здатністю підприємства діяти на цей вплив. Так, підприємство може самостійно здійснювати вибір постачальників матеріальних ресурсів, засобів виробництва і капіталу або впливати на створення суспільної думки про підприємство і його продукцію, але не в змозі контролювати поведінку постачальників матеріалів, рівень інтенсивності конкуренції в галузі або регіоні, а також поводження конкурентів.

Фактори загального характеру впливають на діяльність підприємства в цілому, наприклад, ріст темпів інфляції, падіння попиту на продукцію підприємства, зміна вимог споживачів до якості продукції припускають перегляд практично всіх аспектів діяльності підприємства, тоді як впливи приватного характеру впливають на який-небудь окремий аспект діяльності підприємства. Так, наприклад, зміна вимог покупців до упакування і доставки продукції, зміни умов постачання і транспортування споживаних матеріалів змушують підприємство переглянути окремі аспекти діяльності.

Негативні результати взаємодії підприємства із суб'єктами зовнішнього середовища можуть негативно вплинути на діяльність підприємства. У зв'язку з цим виникає поняття економічної безпеки підприємства як безпеки його взаємодії із суб'єктами зовнішнього середовища.

Підприємство – це не тільки будівлі, споруди, засоби виробництва, робоча сила тощо, це, перш за все, живий суспільний організм, який виготовляє продукцію, знаходячись в постійних інформативно-виробничих сплетіннях зв'язків і відносин в певному навколишньому середовищі. В найзагальнішому розумінні, підприємство – самостійний господарюючий суб'єкт з правом юридичної особи, який на основі ресурсів, що є у нього (або закріплених за ним), виготовляє й реалізує продукцію, виконує роботи і надає послуги. Все це повинно враховуватися при забезпеченні його безпеки.

Підтвердженням актуальності цієї проблеми - проблеми забезпечення економічної безпеки підприємства - і усвідомлення цієї актуальності керівниками підприємств є *створення в організаційній структурі управління підприємствами* (правда, поки що це відноситься переважно до великих фінансово-промислових конгломератів) спеціальних підрозділів, покликаних забезпечити їхню економічну безпеку. Для досягнення найбільшої ефективності одні автори рекомендують *створення власної служби безпеки* і пропонують варіанти цих структур. Інші пропонують використовувати "*міжоб'єктну систему безпеки недержавних об'єктів економіки*" аналогічну існуючої в США. Однак, справедливо буде помітити, що найчастіше функції цих служб *зводяться до безпеки підприємства як такої*, оскільки ці структурні підрозділи не мають розробленої й ефективно функціонуючої наукової системи оцінки економічної безпеки і її рівня, теоретичної бази своєї роботи, що істотно знижує результативність таких структурних підрозділів.

Первісне *поняття економічної безпеки* розглядалося як *забезпечення умов збереження комерційної таємниці й іншої секретної інформації підприємства*.

Такому трактуванню економічної безпеки присвячені публікації початку 90-х років минулого сторіччя. На перших етапах ринкових перетворень у зв'язку зі зміною поняття власності, самостійним виходом підприємств на зовнішній ринок, прагненням до максимізації прибутку, виробництвом конкурентоздатної продукції, питання збереження комерційної таємниці в діяльності підприємств набуло особливої актуальності. Кожне підприємство прагнуло захищати свої комерційні таємниці, інтелектуальну власність і взагалі інформацію як найкоштовніший товар. *Забезпечення економічної безпеки розглядалося насамперед як захист інформації.*

Визнаючи, що збереження інформації є одним з важливих аспектів економічної безпеки підприємства, необхідно відзначити, що зведення проблеми економічної безпеки підприємства тільки до захисту комерційної таємниці являє собою занадто спрощений варіант вирішення такої проблеми. Тому отримав визнання інший підхід до трактування поняття економічної безпеки підприємства. Різкий спад виробництва в цілому по країні, а головне - зміна економічних функцій держави, що уже не було основним інвестором і споживачем продукції, змусили подивитися набагато ширше на проблему економічної безпеки підприємств. Відповідно до цього погляду економічна безпека підприємства обумовлена впливом зовнішнього середовища, що у ринковій економіці увесь час змінюється, ніколи не залишається стабільним, постійним або незмінним. Саме з позицій впливу зовнішнього середовища, захисту підприємств від його негативного впливу і розглядається зміст категорії економічної безпеки підприємства, у тому числі й у нечисленних поки публікаціях вітчизняних учених-економістів.

Поняття «безпека підприємства» є досить широким і багатогранним. В найвужчому розумінні і його можна представити як відсутність різного роду небезпек і загроз або наявність можливостей по їх попередженню, захисту інтересів, недопущення збитків більше критичної межі. Це вимагає копіткої повсякденної роботи відповідного персоналу, служб безпеки, які б організували беззбиткову роботу підприємства, збереження майна, недопущення розголошування таємниці, припинення чинників насильних злочинів, збереження інтелектуальної власності тощо.

Економічна, фінансова, майнова безпека – це матеріальна база безпеки підприємства в цілому. Розробка теорії безпеки підприємництва знаходиться на початковій стадії. В даний час у науковій літературі, навіть спеціальній, суть теорії економічної безпеки підприємництва, його складових, індикаторів розкривається вкрай рідко. У визначеннях дане поняття виражається або не завжди чітко, або неповно. Дуже часто забезпечення економічної безпеки бізнесу зводиться до протистояння, захисту від різного роду економічних злочинів. Поза сумнівом, що це важливо, але не можна зводити поняття «економічної безпеки підприємства» лише до такого захисту.

При визначенні поняття *"економічна безпека"* стала переважати думка, що його зміст відбиває такий стан підприємства, що забезпечує здатність

протистояти несприятливим зовнішнім впливам. У цьому зв'язку економічна безпека підприємства стала розглядатися набагато ширше - як *можливість забезпечення його стійкості в різноманітних, у тому числі й у несприятливих умовах, що складаються в зовнішнім середовищі,* незалежністю від характеру його впливу на діяльність підприємства, масштабу і характеру внутрішніх змін. Так, *економічна безпека підприємства* визначена як "захищеність його діяльності від негативних впливів зовнішнього середовища, а також як здатність швидко усунути різноманітні загрози або пристосуватися до існуючих умов, що не позначаються негативно на його діяльності". Існує ще одне визначення економічної безпеки підприємства як "кількісної і якісної характеристики властивої фірмі, що відбиває здатність "самовиживання" і розвитку в умовах виникнення зовнішньої і внутрішньої економічної загрози".

У рамках підходу до економічної безпеки підприємства як до стану, обумовленому впливом зовнішнього середовища, слід зазначити *ресурсно-функціональний підхід.* Автори цього підходу економічну безпеку підприємства розглядають як *"стан найбільш ефективного використання корпоративних ресурсів для запобігання загроз і забезпечення стабільного функціонування підприємства в даний час і в майбутньому"* З цією метою розглядається сукупність процесів, що протікають в організації, із усіма їхніми характерними рисами і взаємозв'язками, які складають єдину системну групу з погляду їхньої функціональної ролі в забезпеченні економічної безпеки підприємства і відіграють важливу роль у забезпеченні економічної безпеки підприємства. У *ресурсно-функціональному підході як основні напрямки економічної безпеки підприємства розрізняють сім функціональних складових: інтелектуально-кадрову, фінансову, технологічну, правову, екологічну, інформаційну і силову.*

На нашу думку, *економічна безпека підприємства* – це такий стан господарюючого суб'єкта, при якому він при найефективнішому використанні корпоративних ресурсів досягає попередження чи послаблення зовнішніх і внутрішніх негативних впливів, здійснює адекватний захист від існуючих небезпек і загроз та забезпечує досягнення цілей бізнесу в умовах конкуренції й господарського ризику.

Таким чином, *економічну безпеку підприємства* можна розглядати як практичне використання ефективних принципів сучасного менеджменту та своєчасну реакцію на зміни в зовнішньому середовищі, що забезпечують адаптацію підприємства до умов його існування. Звідси *економічну безпеку підприємства* слід розглядати як еволюційний розвиток ситуаційного підходу до управління. *Економічна безпека* викликає усе більшу зацікавленість підприємств, що стикаються з труднощами при реалізації принципово нових підходів до управління підприємствами, при організації управління підприємством у ринкових умовах.

Таке розуміння економічної безпеки підприємства дозволяє показати, що виробниче підприємство знаходиться в ситуації невизначеності, непередбачуваності, зміни як внутрішніх умов господарювання, так і зовнішніх:

політичних, макроекономічних, екологічних, правових; ухвалює ризикові рішення в умовах жорсткої конкуренції, добивається попередження, послаблення або захисту від існуючих або прогнозованих небезпек або загроз; і це переконливо свідчить, що в даних умовах воно забезпечує досягнення цілей бізнесу. Тобто в даній ситуації корпоративні ресурси підприємства (земля, капітал, кадровий потенціал, підприємницькі здібності менеджерів, інформація, інтелектуальна власність, технологія і т.д.) використовуються в першу чергу для досягнення цілей бізнесу, а не тільки для запобігання небезпек і загроз. І такий шлях – це шлях досягнення стратегічних цілей підприємницької діяльності та забезпечення стійкого інтенсивного розвитку підприємства.

2. ЗМІСТОВНО-ТИПОЛОГІЧНА ХАРАКТЕРИСТИКА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Економічна безпека підприємства – економічний стан підприємства, сталий по відношенню до внутрішніх і зовнішніх змін фінансово-господарської діяльності, не пов'язаний з форс-мажорними обставинами. Економічна безпека підприємства являє собою створення таких умов його діяльності, за яких забезпечується надійний захист економічних інтересів підприємства від різних загроз.

Головною метою економічної безпеки підприємства є гарантування його стабільного та максимально ефективного функціонування. Система захисту економічної безпеки підприємства може включати такі напрямки:

- захист матеріальних і фінансових цінностей;
- захист інтелектуальної власності;
- захист інформаційного середовища;
- захист персоналу;
- захист навколишнього середовища.

Результатом забезпечення економічної безпеки підприємства є стабільність (надійність) його функціонування, ефективність фінансово-економічної діяльності та особиста безпека персоналу.

Необхідність постійного дотримання економічної безпеки зумовлюється об'єктивною потребою кожного суб'єкта господарювання у забезпеченні стабільного функціонування і досягнення цілей діяльності.

Рівень економічної безпеки підприємства залежить від того, наскільки ефективно його керівництво і спеціалісти (менеджери) будуть спроможні сформувати мету та функціональні ознаки (критерії) формування системи економічної безпеки підприємства. Саме це дозволить уникнути можливих загроз і ліквідувати шкідливі наслідки окремих негативних впливів складових зовнішнього та внутрішнього середовища (рис 7.1).

Джерелами негативних впливів на економічну безпеку підприємства (організації) можуть бути:

1) свідомі чи несвідомі дії окремих посадових осіб і суб'єктів господарювання (органів державної влади, міжнародних організацій, підприємств-конкурентів);

2) збіг об'єктивних обставин (стан фінансової кон'юнктури на ринках даного підприємства, наукові відкриття та технологічні розробки, форс-мажорні обставини тощо).

Залежно від суб'єктної обумовленості негативні впливи на економічну безпеку можуть бути об'єктивними і суб'єктивними. *Об'єктивними* вважаються такі негативні впливи, що виникають не з вини самого підприємства або його окремих працівників. *Суб'єктивні впливи* мають місце внаслідок неефективної роботи підприємства в цілому або його окремих працівників (передусім керівників і функціональних менеджерів).

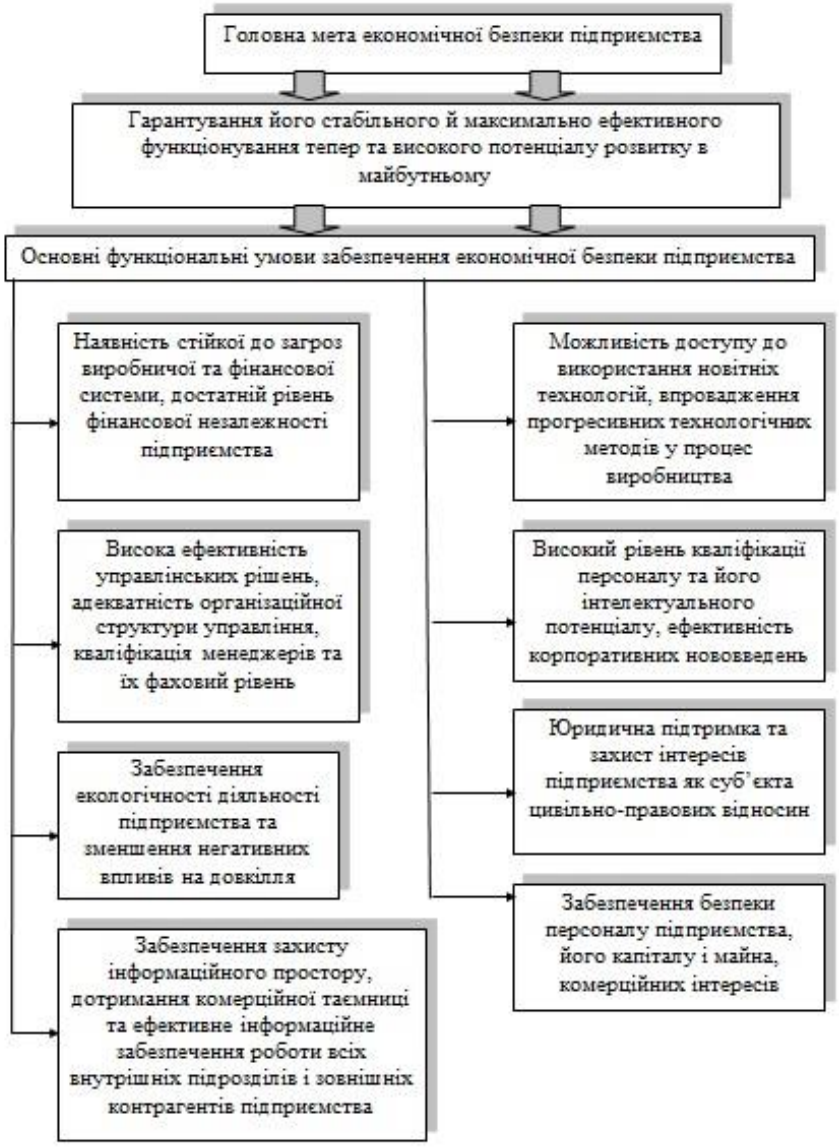


Рис. 7.1 – Мета й функціональні умови забезпечення економічної безпеки підприємства

3. ОСНОВНІ ФУНКЦІОНАЛЬНІ СКЛАДОВІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Категорія економічної безпеки підприємства є інтегральною, системною величиною. У значній мірі, це пов'язано з внутрішньою організацією діяльності конкретного підприємства, якій притаманні: ієрархічність, багатокритеріальність, автономність та динамічність розвитку, певний ступінь невизначеності й ризику, а також здатність до самоорганізації та адаптації.

Виходячи із позицій системного аналізу, вважаємо за доцільне провести класифікацію функціональних складових економічної безпеки підприємства за видовою ознакою (рис. 7.2).

Загальну схему процесу організації фінансової складової економічної безпеки підприємства подано на рис. 7.3.

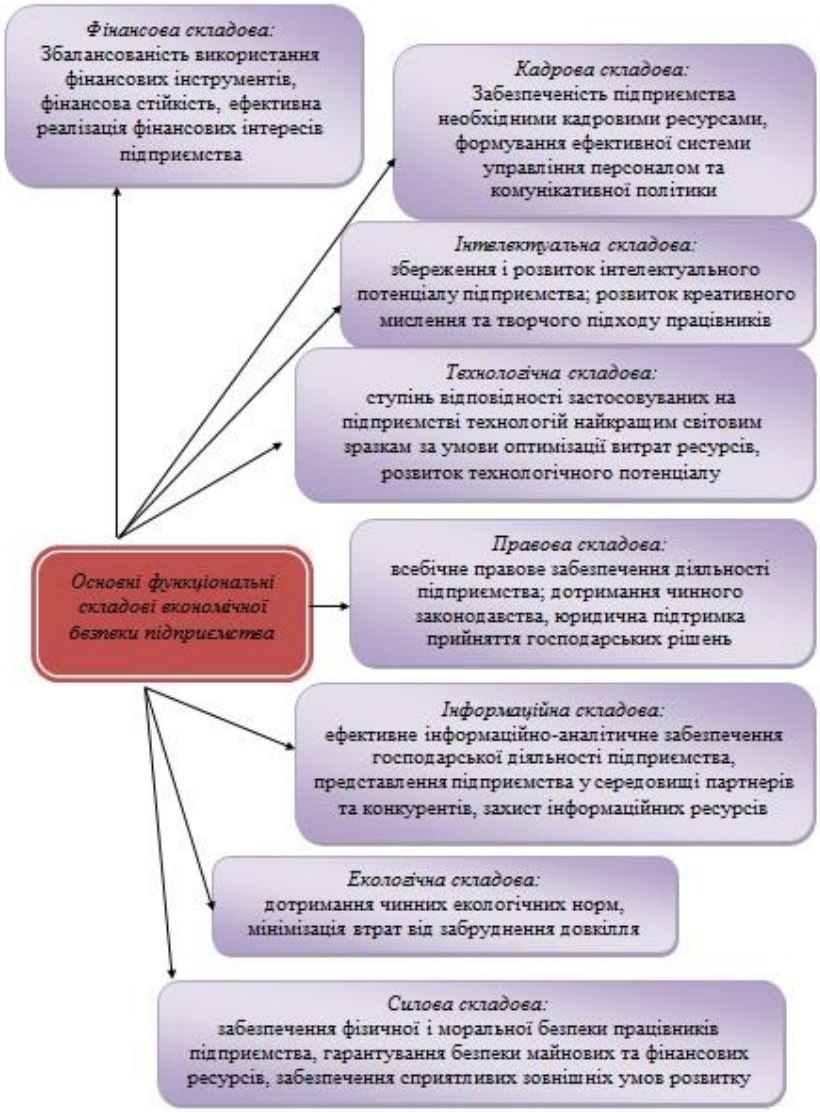


Рис. 7.2. Структура функціональних складових економічної безпеки підприємства

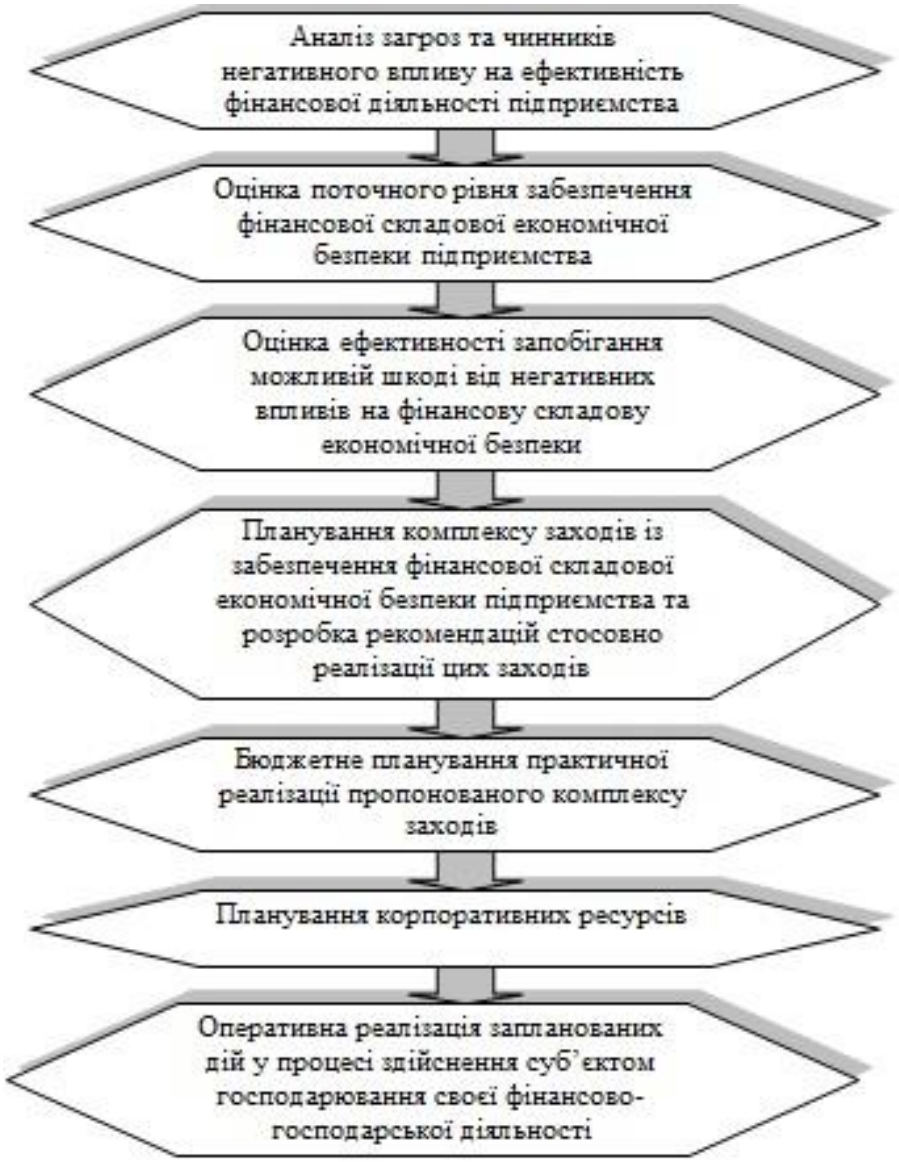


Рис. 7.3. Типова схема охорони фінансової складової економічної безпеки підприємства

Ефективність запобігання очевидним і потенційно можливим загрозам (втратам) економічній безпеці підприємства і визначає дієвість діяльності відповідних служб підприємства.

Спочатку оцінюються загрози економічній безпеці підприємства фінансового характеру, що включають:

- *внутрішні негативні дії (неефективне* фінансове планування та управління активами; малоефективна ринкова стратегія; нераціональна цінова й кадрова політика);
- *зовнішні негативні дії* (спекулятивні операції на ринку цінних паперів; цінова та інші форми конкуренції; лобіювання конкурентами недостатньо продуманих рішень органів влади);

- *форс-мажорні обставини* (стихійне лихо, страйки, військові конфлікти) та обставини, наближені до форс-мажорних (законодавчі акти, ембарго, блокада, зміна курсу валют тощо).

У процесі оцінки поточного рівня забезпечення фінансової складової економічної безпеки підлягають аналізу:

- *фінансова звітність і результати роботи підприємства (організації)* — платоспроможність, фінансова незалежність, структура й використання капіталу та прибутку;
- *ринок цінних паперів підприємства (організації)* — інвестиційні посередники та інвестори цінних паперів, курс акцій і лістинг.
- *конкурентний стан підприємства (організації) на ринку* — частка ринку даного суб'єкта господарювання; рівень застосовуваних технологій і менеджменту;
- *ринок цінних паперів підприємства (організації)* — оператори та інвестори цінних паперів, курс акцій і лістинг.

Сутнісну характеристику всього циклу охорони інтелектуальної та кадрової складових економічної безпеки підприємства (організації) наведено на рис. 7.4.

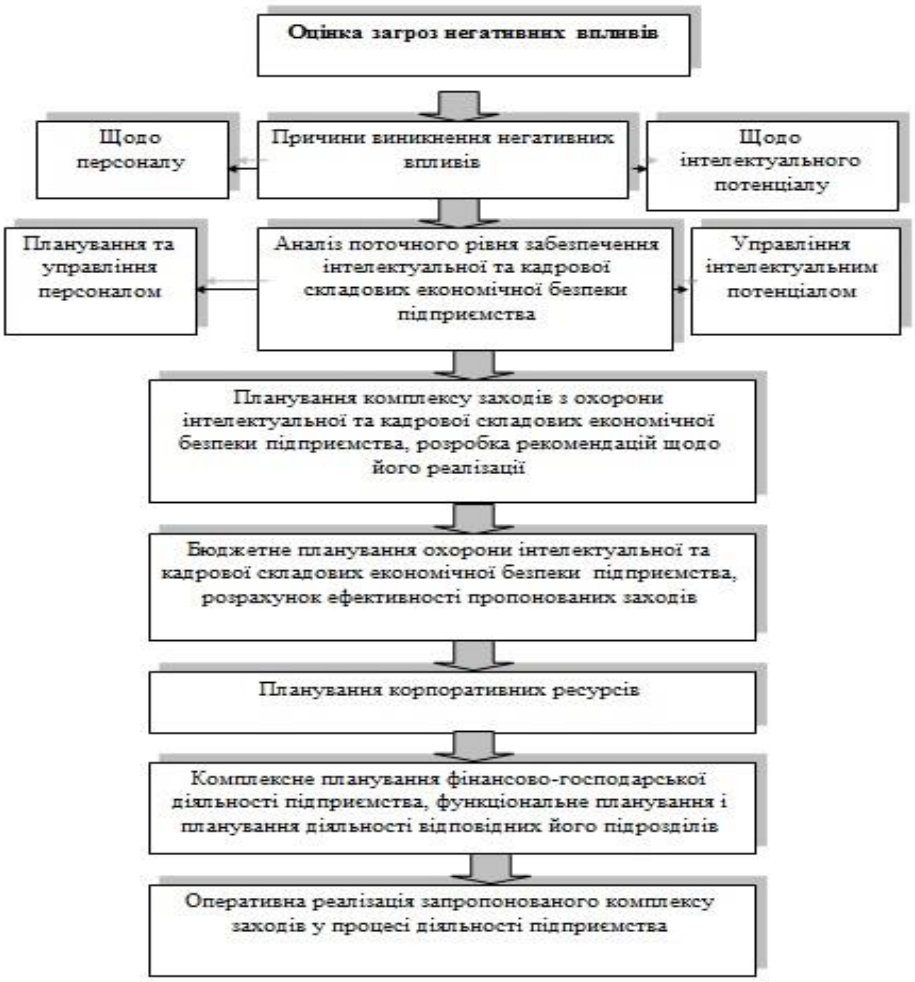


Рис. 7.4. Схема дій з охорони інтелектуальної та кадрової складових економічної безпеки підприємства

Охорона інтелектуальної та кадрової складових економічної безпеки охоплює взаємопов'язані і водночас самостійні напрями діяльності відповідного суб'єкта господарювання:

- *перший* — спрямованість на роботу з персоналом фірми та підвищення ефективності діяльності всіх категорій персоналу;
- *другий* — націленість на збереження й розвиток інтелектуального потенціалу, тобто сукупності прав на інтелектуальну власність або на її використання (у тому числі патентів і ліцензій), та на поповнення знань і професійного досвіду працівників підприємства (організації).

На першій стадії процесу охорони цієї складової економічної безпеки здійснюється оцінка загроз негативних дій і можливої шкоди від таких дій. З-поміж основних негативних впливів на економічну безпеку підприємства виокремлюють недостатню кваліфікацію працівників, їхнє небажання або нездатність забезпечувати максимальну користь своєму підприємству. Ці обставини можуть зумовлюватися низьким рівнем управління персоналом, браком коштів на оплату його праці чи нераціональним їх витрачанням.

Процес планування та управління персоналом, спрямований на охорону належного рівня економічної безпеки, має охоплювати організацію добору, найму, навчання й мотивації праці працівників, включаючи матеріальні та моральні стимули, престижність професії, волю до творчості, забезпечення соціальними благами.

Важливою ланкою встановлення нормального рівня економічної безпеки є оцінка ефективності заходів, яка здійснюється через зіставлення загальної величини витрат на запобіжні заходи і втрат, яких могло б зазнати підприємство (організація).

Технологічна складова відображає технологічний потенціал підприємства і характеризує ступінь його захищеності.

Процес охорони техніко-технологічної складової економічної безпеки передбачає здійснення кількох послідовних етапів.

Перший етап охоплює аналіз ринку технологій стосовно виробництва продукції (збирання та аналіз інформації щодо особливостей технологічних процесів на аналогічних підприємствах і нових розробок у даній галузі, а також технологій, спроможних здійснити інтервенцію на галузевий технологічний ринок).

Другий етап — це аналіз конкретних технологічних процесів і пошук внутрішніх резервів поліпшення використовуваних технологій.

Третій етап передбачає здійснення:

а) аналізу товарних ринків за профілем продукції, що виготовляється підприємством, і ринків товарів-замінників;

б) оцінку перспектив розвитку ринків продукції підприємства;

в) прогнозування можливої специфіки необхідних технологічних процесів для випуску конкурентоспроможних товарів.

Четвертий етап присвячено переважно розробці технологічної стратегії

підприємства, а саме:

1)виявленню перспективних товарів з групи (номенклатури, асортименту), що виготовляється підприємством;

2)плануванню комплексу технологій для виробництва перспективних товарних позицій;

3)бюджетуванню технологічного розвитку підприємства на засаді оптимізації витрат за програмою, вибору альтернатив, опрацювання власних розробок або придбання патентів і необхідного устаткування на ринку;

4)розробці загального плану технологічного розвитку підприємства;

5)складанню плану власних корпоративних НДДКР згідно з планом технологічного розвитку підприємства.

П'ятий етап — оперативна реалізація плану технологічного розвитку підприємства в процесі здійснення ним виробничо-господарської діяльності.

Шостий етап є завершальним. На цьому етапі аналізуються результати практичної реалізації заходів щодо охорони техніко-технологічної складової економічної безпеки на підставі спеціальної карти розрахунків ефективності таких заходів.

Основними загрозами *правової* складової безпеки є недостатня правова захищеність інтересів підприємства в договірній та іншій діловій документації, а саме: порушення юридичних прав підприємства та його працівників, навмисне чи випадкове розголошення відомостей, що являють собою комерційну таємницю, порушення норм патентного права, ліцензійних договорів тощо.

Протидіяти цим загрозам повинна юридична та патентно-ліцензійна служби підприємства, основними функціями яких є правове забезпечення діяльності підприємства, юридична підтримка договірної документації, супровід судових та арбітражних розглядів, правові тренінги персоналу, ведення патентного фонду підприємства, контроль порушень норм патентного права, перегляд матеріалів, які призначені для передачі засобам масової інформації.

Типову схему охорони політико-правової складової економічної безпеки підприємства представлено на рис.7.5.

Рис. 7.5. Типова схема охорони правової безпеки підприємства (організації)

Для того, щоб вітчизняним підприємствам претендувати на гідне місце у світовому інформаційному просторі, ефективно використовувати глобальні інформаційні ресурси для власного соціально-економічного розвитку слід передбачити заходи щодо забезпечення *інформаційної безпеки*, яка характеризується рівнем захисту вітчизняних інтелектуальних прав власності, заходами по попередженню відтоку секретної інформації. Сьогодні, на жаль, не приділяється достатньої уваги інформаційній політиці в цілому і, зокрема, в контексті економічної безпеки підприємства. Вітчизняні товаровиробники не презентовані в достатній мірі в міжнародних інформаційних мережах, що не дає змоги створювати й утримувати позитивний імідж держави та її підприємств за кордоном, демонструвати їх потенціал та конкурентні переваги.

Проблему інформаційної безпеки підприємства можна досить умовно сегментувати на три складові:

- проблема захисту авторських прав,

- безпека інформаційного обміну,
- електронна комерція.

Інтернет поставив всю концепцію захисту авторського права з ніг на голову. Існуючі юридичні механізми, більшість з яких розроблена ще в дев'ятнадцятому столітті, абсолютно не витримують технологічного прогресу. Очевидно, що традиційними методами цю проблему навряд чи можна вирішити.

На сьогодні актуальною проблемою для вітчизняних підприємств є безпека інформаційного обміну. Internet в усьому світі призвів до появи нових засобів фінансових розрахунків. Завдяки цьому багато фінансових послуг стали тепер доступними користувачам прямо вдома або на робочому місці. Усі організації одержали можливість пропонувати свої товари та послуги по всій земній кулі, незважаючи на кордони і відстані. Сучасні технології дозволили створити віртуальні магазини, банки, біржі - цілий світ електронної комерції, що доповнює, а часом і приходить на зміну звичній економічній інфраструктурі. За численними прогнозами, співвідношення між звичайною й електронною комерцією буде в найближчі десятиліття швидко змінюватися на користь останньої.

Згідно поширеній думці, Україна безнадійно відстала від розвинутих країн у сфері електронної комерції. Проте це не зовсім справедливо. Деякі форми фінансових розрахунків у Internet виникли зовсім нещодавно, інші знаходяться на стадії розробки. У нашої країни є реальна можливість не припустити істотного відставання, щонайменше у найважливіших сферах електронної комерції. Найбільшою мірою це стосується розрахунків у Internet за допомогою *пластикових карт.*

Тому основними функціями відповідних служб підприємства, що в сукупності характеризують процес охорони інформаційної складової економічної безпеки підприємства (організації) повинні бути:

- збирання всіх видів інформації, що стосується діяльності фірми (інформація щодо всіх видів ринків; інформація, що характеризує політичні події й тенденції макроекономічного розвитку світової та національної економік; корисна науково-технічна інформація);
- аналіз одержуваної інформації з обов'язковим дотриманням загальновживаних принципів (систематизації, безперервності надходження, всебічного характеру аналітичних процесів) і методів (локальних із специфічних проблем, загальнокорпоративних) організації робіт;
- прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів на даному підприємстві, в країні тау світі стосовно конкретної сфери бізнесу (діяльності), а також показників, яких необхідно досягти суб'єкту господарювання (наприклад, у сферах технологічного розвитку, виробництва, фінансів);
- оцінка рівня економічної безпеки за всіма складовими та в цілому, розробка рекомендацій для підвищення цього рівня на конкретному суб'єкті господарювання;

- інші види діяльності з розробки інформаційної складової економічної безпеки (зв'язок із громадськістю, формування сприятливого іміджу, захист конфіденційної інформації).

Екологічна складова економічної безпеки є переконливою умовою забезпечення сталого розвитку вітчизняних підприємств. Згідно офіційно прийнятого визначення МАГАТЕ, *екологічна безпека* являє собою захист осіб або навколишнього середовища від надмірних несприятливих впливів. Не дивлячись на те, що протягом останнього десятиліття пройшов значний спад виробництва у всіх галузях народного господарства, ситуація в даній сфері не змінилася. При цьому по даній складовій економічної безпеки спостерігається чітка диференціація екологічних регіонів. З однієї сторони, у всіх східних, центральних та південних областях з великою концентрацією промислового виробництва, як правило, спостерігається несприятлива ситуація щодо забезпечення екологічної складової. З іншої сторони, в західних та північних областях її стан є задовільним.

Проблему охорони екологічної безпеки суспільства з боку підприємства, що виробляє на комерційній основі ту чи іншу продукцію, можна вирішити тільки через ретельне дотримання національних (міжнародних) норм мінімально-допустимого вмісту шкідливих речовин, які потрапляють у навколишнє середовище, а також дотримання екологічних параметрів продукції, що виготовляється.

Підприємства-продуценти добровільно не здійснюватимуть заходів із забезпечення екологічного контролю за виробничими процесами та виготовленою продукцією, оскільки це пов'язано з додатковими витратами на очисні споруди та ефективні екологічно чисті технології. Єдиним чинником, що спонукає підприємства до належної екологізації виробництва, є застосування відчутних штрафів за порушення екологічного законодавства.

Способи забезпечення екологічної складової економічної безпеки підприємства:

- На підставі загальних стратегічних рекомендацій, опрацьованих за результатами аналізу карти розрахунку ефективності здійснюваних заходів, *планується комплекс заходів для розробки екологічної складової економічної безпеки в майбутньому.*
- План забезпечення екологічної складової є частиною загального плану (програми) досягнення належного рівня економічної безпеки в цілому. *Він має вигляд логічного сценарію здійснення необхідного комплексу заходів у календарній послідовності з доданням розрахунку ефективності практичної реалізації цих заходів.*
- *Алгоритм процесу охорони екологічної складової економічної безпеки* полягає в проведенні таких послідовних дій:

1)розрахунок карти ефективності здійснюваних заходів для охорони екологічної складової економічної безпеки на підставі звітних даних про фінансово-господарську діяльність підприємства (організації);

2)аналіз виконаних розрахунків і розробка рекомендацій для підвищення

ефективності здійснюваних заходів;

3) розробка альтернативних сценаріїв реалізації запланованих заходів;

4) вибір пріоритетного сценарію на засаді порівняння розрахунків ефективності запланованих заходів;

5) передача вибраного планового сценарію в складі загального плану охорони економічної безпеки в підрозділи, які здійснюють функціональне планування фінансово-господарської діяльності підприємства (організації);

6) практичне здійснення запланованих заходів.

Дії, які негативно впливають на рівень силової складової економічної безпеки підприємства , зумовлюються рядом причин, а саме:

- низьким рівнем корпоративної культури підприємств-конкурентів та використання ними неринкових методів впливу на діяльність підприємства;
- високим рівнем криміналізації економіки в окремих регіонах України;
- комерційними мотивами посягань на життя та здоров'я керівників та працівників підприємства;
- цільовими впливами з метою погіршення іміджу підприємства та впливу на обсяги реалізації його продукції.

Загальну схему організації силової складової економічної безпеки підприємства представлено на рис. 7.6.

Рис. 7.6 – Загальна схема організації силової складової економічної безпеки підприємства (організації)

4.ІНТЕГРАЛЬНИЙ ПОКАЗНИК ДЛЯ ВИЗНАЧЕННЯ РІВНЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Комплексне аналізування економічної безпеки підприємства може бути здійснено лише на базі дослідження інтегральних показників ефективності розвитку окремих функціональних складових. Тому вважаємо доцільним виокремити певну послідовність організаційних рівнів управління розвитком підприємства, серед яких виділимо три основних:

- інституційний рівень – рівень обґрунтування рішень щодо комплексного і збалансованого виробничо-господарського розвитку підприємства в цілому;
- організаційний рівень – рівень обґрунтування рішень щодо розвитку окремих функціональних напрямків;
- фінансово-виробничий рівень – рівень обґрунтування рішень щодо розвитку окремих підрозділів.

Ефективність забезпечення економічної безпеки кожного з цих рівнів може й повинна бути оцінена взаємодоповнюючою сукупністю (комплексом) часткових критеріїв і показників та на їх основі – інтегральним показником. Таким чином, забезпечення підбору критеріїв і показників на основі принципу комплексності, тобто взаємозв'язку, взаємодоповнення, є основною засадою формування кожного інтегрального показника.

Структура підбору критеріїв і показників визначається структурою цілей управління системою економічної безпеки підприємства. Кількість і порядок розрахунку інтегральних індексів з позицій соціально-економічного розвитку підприємства визначається кількістю і порядком узгодження функціональних складових.

Під інтегральним показником економічної безпеки підприємства ($I_{ЕкБ}$) слід розуміти результат оцінювання ієрархічної структури взаємопов'язаних функціональних складових виробничо-господарської діяльності підприємства, який ґрунтується на стандартизації досліджуваних показників та зведенні їх до одного виду шляхом застосування системи багатовимірних середніх величин. Суть багатовимірної середньої полягає в заміні індивідуальних значень множини показників окремого елемента визначеної сукупності відносними (індексними) величинами. Базою порівняння можуть бути середні значення показників по сукупності в цілому, або еталонні (нормативні) значення.

Рівень економічної безпеки підприємства пропонуємо оцінювати на підставі визначення інтегрального показника за допомогою зважування й підсумовування окремих функціональних критеріїв. Для визначення $I_{ЕкБ}$ пропонуємо здійснити розрахунок інтегрального показника розвитку певної функціональної складової ($I_Ф$) підприємства на основі використання показників його звітності. В якості бази порівняння пропонуємо використати нормативні значення розрахованих показників.

Оскільки не всі функціональні складові мають однакову стратегічну вагу та значимість в оцінці інтегрального показника економічної безпеки підприємства, пропонуємо розрахувати коефіцієнти стратегічної ваги функціональних складових на

основі проведення експертного оцінювання. Цей розрахунок пропонуємо здійснювати в два етапи. Перший етап передбачає вибір групи експертів і проведення ними оцінювання стратегічної ваги функціональних складових за чотирибальною шкалою. На другому етапі отримані бали за допомогою визначення відносних величин буде перетворено в коефіцієнти стратегічної ваги кожної складової.

Інтегральний показник економічної безпеки підприємства можна розрахувати за формулою:

$$I_{ЕкБ} = \sum_{i=1}^{N} I_{Фi} \cdot W_i \ , \qquad (7.1)$$

де $I_{Фi}$ – величина окремого критерію за і-тою функціональною складовою економічної безпеки підприємства;

W_i – вага і- тої складової в загальній оцінці інтегрального показника економічної безпеки;

N – кількість функціональних складових економічної безпеки підприємства.

Приклад визначення основних показників, що визначають рівень економічної безпеки підприємства за окремими функціональними складовими представлено у таблиці 7.1.

Таблиця 7.1

Основні показники, що визначають рівень економічної безпеки підприємства

Показники-коефіцієнти	*Методика розрахунку*	*Оптимальне значення*	*Приклад розрахунку*	
			За базисний період	*За звітний період*
Фінансова складова економічної безпеки підприємства				
Концентрації власного капіталу (автономії, незалежності)	Власний капітал / Сума господарських коштів (Валюта балансу)	Більше 0,6	0,561	0,486
Фінансової залежності	Валюта балансу / Власний капітал	Більше 1	1,784	2,056
Маневрування власного капіталу	Власні кошти / Власний капітал	0,4 - 0,6	0,465	0,429
Структури довгострокових вкладень	Довгострокові зобов"язання / необоротні активи	Збільшення	0,212	0,252
Довгострокового залучення позичених коштів	Довгострокові зобов"язання / Власний капітал	Зменшення	0,242	0,287

Показники-коефіцієнти	*Методика розрахунку*	*Оптимальне значення*	*Приклад розрахунку*	
			За базисний період	*За звітний період*
Співвідношення власних і залучених коштів	Залучений капітал / Власний капітал	Зменшення	0,259	0,298
Співвідношення необоротних і власних коштів	Необоротні кошти / Власний капітал	Більше 0,5 - 0,8	1,140	1,139
Стабільності економічного зростання	(Чистий прибуток - сума виплачених дивідендів) / Власний капітал	Зростання	0,001	0,001
Чистої виручки	(Чистий прибуток + амортизаційні відрахування) / Виручка від реалізації продукції	Збільшення	0,048	0,059
Інтелектуальна й кадрова складові економічної безпеки підприємства				
Плинності кадрів	Сума прибулих та вибулих працівників / Середньоспискова чисельність працюючих	Зниження	0,090	0,089
Середній тарифний розряд	(Сума добутків кількості працівників відповідного розряду та номера розряду) / Середньоспискова чисельність працівників	Зростання	3,474	3,476
Зміни фонду оплати праці	Фонд оплати праці за звітний період / Фонд оплати праці за попередній період	Більше 1	1,207	1,309

Показники-коефіцієнти	*Методика розрахунку*	*Оптимальне значення*	*Приклад розрахунку*	
			За базисний період	*За звітний період*
Технологічна складова економічної безпеки підприємства				
Загальний коефіцієнт надходження основних засобів	Повна вартість основних засобів, що надійшли / Повна вартість основних засобів на кінець періоду	Зростання	1,183	1,167
Загальний коефіцієнт вибуття основних засобів	Обсяг вибулих основних засобів / Загальна вартість основних засобів на початок періоду	Зростання	0,101	0,108
Коефіцієнт приросту основних засобів	Частка фондів, що надійшли і вибули до їх вартості на початок періоду	Зростання	1,257	1,248
Фондовіддача	Обсяг випущеної продукції / Середньорічна вартість основних виробничих фондів	Зростання	1,258	1,311
Фондомісткість	Середньорічна вартість основних виробничих фондів / Обсяг випущеної продукції	Зниження	0,795	0,763
Фондоозброєність	Середньорічна вартість основних виробничих фондів / Середньоспискова чисельність працюючих	Зростання	40,596	41,635

За результатами проведених розрахунків складаємо карту функціонального аналізу економічної безпеки підприємства (табл. 7.2).

Таблиця 7.2.

Карта функціонального аналізу економічної безпеки підприємства

Функціональні складові економічної безпеки підприємства та назва показника, який аналізується	*Негативні впливи («+» негативний вплив має місце, «–» коефіцієнт перебуває в межах оптимального значення)*	*Заходи для усунення негативних впливів*
Фінансова складова економічної безпеки підприємства		
Концентрації власного капіталу (автономії, незалежності)	+	Збільшення частки власного капіталу шляхом додаткової емісії акцій.
Фінансової залежності	–	–
Маневрування власного капіталу	–	–
Структури довгострокових вкладень	–	–
Довгострокового залучення позичених коштів	+	Зменшення обсягів залучення кредитних ресурсів.
Співвідношення власних і залучених коштів	+	Збільшення частки власних коштів.
Співвідношення необоротних і власних коштів	+	Збільшити обсяг власних коштів, спрямованих на фінансування оборотного капіталу.
Стабільності економічного зростання	+	Підвищити рівень фінансової стійкості.
Чистої виручки	–	
Інтелектуальна й кадрова складові економічної безпеки підприємства		
Плинності кадрів	–	–
Середній тарифний розряд	–	–
Зміни фонду оплати праці	–	–
Техніко-технологічна складова економічної безпеки підприємства		

Функціональні складові економічної безпеки підприємства та назва показника, який аналізується	*Негативні впливи («+» негативний вплив має місце, «–» коефіцієнт перебуває в межах оптимального значення)*	*Заходи для усунення негативних впливів*
Загальний коефіцієнт надходження основних засобів	+	Провести оновлення застарілої технологічної бази
Загальний коефіцієнт вибуття основних засобів	–	–
Коефіцієнт приросту основних засобів	+	Здійснити придбання або оновлення діючих виробничих потужностей.
Фондовіддача	–	–
Фондомісткість	–	–
Фондоозброєність	–	–

Проведене дослідження дає підстави для таких висновків:

- проблема розроблення методичних підходів до оцінювання інтегрального показника економічної безпеки, які б могли здійснюватися в автоматизованому режимі і давали змогу здійснювати комплексне оцінювання перспектив розвитку організації, є актуальною й важливою для здійснення процесів економічного оцінювання та організування вітчизняних підприємств;
- запропоновані методичні положення дозволяють здійснювати економічне оцінювання доцільності функціонування окремої функціональної складової та визначати ступінь її стратегічного впливу на діяльність підприємства в цілому;
- результати розрахунків, проведених на основі показників фінансової звітності дають кількісні орієнтири щодо оцінювання інтегрального показника економічної безпеки підприємства;
- практична реалізація викладених методичних підходів сприятиме підвищенню обґрунтованості рішень щодо стратегічних і поточних напрямів діяльності вітчизняних консорціумів.

Тема 8. ОСНОВНІ МЕТОДОЛОГІЧНІ ПОЛОЖЕННЯ ФОРМУВАННЯ БЕЗПЕКИ БІЗНЕСУ

1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ПОЛОЖЕННЯ БЕЗПЕКИ ПІДПРИЄМСТВА, ЇЇ МЕТА, ЗАВДАННЯ ТА ФУНКЦІЇ

У ринковій економіці підприємницькі структури володіють повною економічною самостійністю. Вони самостійно визначають економічну політику, формують портфель замовлень, організовують виробництво і збут продукції, повністю відповідають за результати господарської діяльності. Все це, поза сумнівом, актуалізує проблему забезпечення економічної безпеки бізнесу.

У зв'язку з цим очевидно, що забезпечення економічної безпеки виробничої діяльності вимагає, щоб на підприємстві була створена власна система безпеки. Даючи характеристику системі безпеки підприємства, відразу визначимо деякі, на наш погляд, *важливі методологічні положення.*

По-перше, система безпеки підприємства не може бути шаблонною. Вона повинна бути унікальною на кожному підприємстві, оскільки залежить від рівня розвитку і структури виробничого потенціалу, ефективності його використовування і спрямованості виробничої діяльності, якісного стану кадрів, виробничої дисципліни, стану навколишнього середовища, ризику виробництва і т.д.

По-друге, система безпеки підприємства є самостійною, відособленою від аналогічних систем інших виробничих одиниць. Але її відособленість відносна, оскільки система безпеки підприємства – це складовий елемент безпеки більш високого рівня – міста, регіону, країни. Дуже багато завдань безпеки підприємства не можуть бути вирішені самостійно, без рішень, що приймаються на більш високому системному рівні, і перш за все державному. Саме на цьому рівні ухвалюються найважливіші політичні, макроекономічні, правові і інші рішення, що створюють середовище безпеки виробничої діяльності. Служба безпеки конкретного підприємства залежить також і від активності служб безпеки конкурентних підприємств, вона створюється і функціонує на основі прийнятих законодавчих актів, залежить від можливостей придбання засобів захисту, рівня підготовки і кваліфікації кадрів тощо.

По-третє, система безпеки підприємства повинна бути комплексною. Вона покликана забезпечити безпеку економічну, науково-технічну, кадрову, інтелектуальну, екологічну, інформаційну, фізичну, техногенну, пожежну і ін.. А, отже, у її складі повинні бути відповідні елементи, органи, сили, засоби.

Створення системи безпеки підприємства і організація її успішного функціонування повинні спиратися на методологічні основи наукової теорії безпеки.

Метою системи безпеки є своєчасне виявлення і запобігання як зовнішніх,

так і внутрішніх небезпек і загроз, забезпечення захищеності діяльності підприємства і досягнення ним цілей бізнесу.

Безумовно, що досягнення поставленої мети можливе лише на основі вирішення *комплексу завдань*, серед яких виділяють:

1) Виявлення реальних і прогнозування потенційних небезпек і загроз підприємству;
2) Знаходження способів їх запобігання, ослаблення або ліквідації наслідків їх дії.
3) Знаходження сил і засобів, необхідних для забезпечення безпеки підприємства.
4) Організація взаємодії з правоохоронними і контрольними органами в цілях запобігання і припинення правопорушень, направлених проти інтересів підприємства.
5) Створення власної служби безпеки підприємства і ін.

Система безпеки підприємства покликана виконувати певні *функції*, серед яких виділяють наступні:

1) Прогнозування ситуації реальної небезпеки.
2) Виявлення, попередження та послаблення небезпек і загроз.
3) Забезпечення захищеності діяльності підприємства і його персоналу.
4) Збереження майна підприємства.
5) Створення здорового конкурентного середовища.
6) Ліквідація наслідків завданого збитку і ін.

2. *РЕАЛІЗАЦІЯ ІНТЕРЕСІВ ПІДПРИЄМСТВА ЯК ОСНОВА ЗАБЕЗПЕЧЕННЯ ЙОГО ЕКОНОМІЧНОЇ БЕЗПЕКИ.*

Економічна безпека підприємства є комплексним поняттям і пов'язана не стільки з внутрішнім станом самого підприємства, скільки з впливом зовнішнього середовища, з його суб'єктами, з якими підприємство вступає у взаємодію. У зв'язку з цим, імовірно, більш точно стверджувати, що *економічна безпека підприємства* відбиває погодженість, збалансованість інтересів підприємства й інтересів суб'єктів зовнішнього середовища. З цих позицій *економічна безпека підприємства* може розглядатися як практичне втілення положень теорії ресурсної взаємозалежності, відповідно до якої у своїй діяльності підприємство повинне брати до уваги не тільки свої, але й інтереси партнерів, коло яких може бути дуже широким. Саме з погляду узгодження інтересів підприємства і взаємодіючих з ним суб'єктів зовнішнього середовища і передбачається досліджувати поняття економічної безпеки підприємства.

Економічну безпеку підприємства можна розглядати як міру гармонізації в часі і просторі економічних інтересів підприємства з інтересами пов'язаних з ним суб'єктів зовнішнього середовища, що діють поза межами підприємства.

Запропоноване розуміння економічної безпеки підприємства дозволяє

стверджувати, що *воно знаходиться в економічній безпеці*, якщо його *економічні інтереси гармонізовані з інтересами суб'єктів зовнішнього середовища* - споживачів, постачальників, конкурентів, інвесторів, держави і суспільства в цілому. *Укрупнена систематизація суб'єктів зовнішнього середовища*, які взаємодіють з підприємством, може бути представлена наступними напрямками:

1. Фінансове забезпечення. Суб'єкти: фінансові посередники; інвестори; ринок фінансів.

2. Забезпечення кадрами. Суб'єкти: ринок робочої сили; експерти та консультанти; консалтингові фірми.

3. Ресурсне забезпечення. Суб'єкти: постачальники матеріалів; постачальники обладнання; інноваційні фірми.

4. Реалізація продукції. Суб'єкти: ринкові контрагенти; споживачі; маркетингові фірми.

З приведеного розуміння економічної безпеки підприємства, як міри гармонізації інтересів підприємства з інтересами пов'язаних з ним суб'єктів зовнішнього середовища, випливає, що досліджується зміст базового поняття економічної безпеки із поняттям "інтереси підприємства", а також органічно пов'язаного з ним критерію дотримання інтересів підприємства.

Виходячи зі значення слова "*інтерес*", обумовленого як користь, вигода, прибуток, можливим є розглядати *інтереси підприємства як його взаємодію із суб'єктами зовнішнього середовища, здійснювану постійно або протягом визначеного проміжку часу, примусово або на вибір підприємства, результати якого забезпечують одержання прибутку*.

Інтереси підприємств невід'ємні від їхніх суб'єктів, оскільки інтереси підприємства - це персоніфікована категорія. Інтересів узагалі не існує. У зв'язку з цим необхідно виділити *суб'єкти* інтересів підприємства. *Персоніфікація суб'єктів інтересів підприємства* обумовлена такими факторами як *форма власності на засоби виробництва* та, відповідно, *організаційно-правова форма діяльності підприємства*, і самим видом інтересів. Відповідно до названих факторів ієрархія суб'єктів інтересів підприємства може бути представлена в такий спосіб:

- власник засобів виробництва,
- керівництво підприємства,
- команда управління підприємством,
- персонал підприємства.

Суб'єкт контролю формує систему інтересів підприємства і, отже, впливає на його економічну безпеку. Реальний контроль над діяльністю підприємства може здійснюватися сторонніми структурами, наприклад, кредиторами.

Важливим є збіг або розбіжність інтересів контролюючого суб'єкта і підприємства. Якщо їхній інтереси збігаються, якщо контролюючий суб'єкт має в структурі капіталу підприємства значні за обсягом інвестиції, наприклад, у формі кредитів, якщо контролюючий суб'єкт зацікавлений у стійкому і динамічному розвитку підприємства, то тоді наявність контролюючого суб'єкта не можна

вважати негативним фактором у розвитку підприємства. Особливу актуальність питання виявлення контролюючого суб'єкта мають для підприємств, що діють у формі акціонерного товариства.

Власник засобів виробництва є новим для української економіки учасником виробничих відносин. Його відносини з керівництвом підприємства, у тому числі й в області формулювання і захисту економічних інтересів підприємства, складаються по-різному. Дослідження співвідношення інтересів власника засобів виробництва і керівництва підприємством, що з'явилися в економіці України внаслідок приватизації державного майна акціонерних товариств, що заслуговує на особливу увагу.

У діючому українському законодавстві *поняття контролю над акціонованим підприємством* тісним образом пов'язане *з володінням контрольним пакетом акцій або найбільшою кількістю голосів* (ст.1.26 Закону України "Про оподаткування прибутку підприємств" (1997 р.). Таким чином, *поняття контрольного пакета акцій і контролю над діяльністю акціонерного товариства ототожнюються, причому друге поняття випливає з першого.*

Однак у практиці корпоративних відносин не тільки в українських, але і закордонних акціонерних товариствах ці теоретичні схеми змінюються. Аналіз складу акціонерів і їхніх основних груп з погляду зазначеного критерію надає можливість визначити суб'єкти контролю над діяльністю акціонерного товариства. Акціонери-працівники підприємства є однієї з великих груп акціонерів-інсайдерів. В Україні нараховується близько 25 млн. індивідуальних акціонерів, що складає близько 50% населення країни, тоді як у США, відповідно, 51,4 млн. акціонерів і 21,1%, у Великобританії - 9 млн. і 15,8%, у Японії - 11 млн. і 9%, у Німеччині - 4,5 млн. і 5,5%5. В акціонерних товариствах інсайдерського типу реальний контроль над їхньою діяльністю належить акціонерам-адміністраторам. Право таких акціонерів на контроль над діяльністю акціонерного суспільства формально відсутній, але де-факто саме вони реально впливають на підприємницьке використання того корпоративного майна, співвласниками якого є всі акціонери, а також визначають склад інтересів підприємства і формують систему їхнього захисту. Акціонування підприємств вивело їх зі сфери контролю держави і створило можливості для розвитку підприємства в інтересах групи людей, що реально визначають ділову політикові акціонованого підприємства, але далеко не завжди зацікавлених у такому його розвитку, що враховувало би інтереси всіх акціонерів.

У таких умовах *економічна безпека акціонерних товариств інсайдерського типу* багато в чому, якщо не цілком, *залежить від рівня компетентності і сумлінності їхніх керівників*, від їхньої готовності приймати і реалізовувати управлінські рішення, спрямовані на захист інтересів всіх акціонерів. Якщо рівень компетентності і професіоналізму керівників і фахівців акціонерного товариства ще можна установити, хоча в цьому випадку досить великий вплив суб'єктивної оцінки, то набагато складніше визначити відповідність прийнятих рішень інтересам всіх акціонерів. Оцінити таку відповідність ні кількісно, ні якісно

практично неможливо, тим більше, що реально ніякої відповідальності акціонери-адміністратори перед всіма акціонерами не несуть.

У випадку наявності великих аутсайдерів у списку акціонерів економічну безпеку суспільства оцінити однозначно позитивно або негативно навряд чи можливо. З одного боку, поява таких акціонерів, особливо якщо вона супроводжується менеджерським талантом, здатна вплинути на характер і якість стратегічних рішень підприємства. З іншого боку, присутність такого акціонера може супроводжуватися такими особливостями, як орієнтація в проведенні дивідендної політики на фінансування інвестиційних проектів і програм, зміна стратегічної орієнтації в діяльності підприємства, що у випадку управлінських помилок може привести якщо не до банкрутства підприємства, то до значного погіршення фінансових результатів і, отже, до зниження економічної безпеки. У зв'язку з цим для визначення впливу великого акціонера-аутсайдера на економічну безпеку підприємства необхідне ретельне дослідження відповідності його інтересів інтересам розвитку акціонерного товариства, всебічна оцінка впливу рішень, прийнятих під впливом і тиском такого акціонера з погляду економічної безпеки підприємства. Особливу роль серед акціонерів відіграє держава, у зв'язку з чим оцінці пакета акцій держави і рівневі управління їм надається особливе значення. В Україні держава залишила за собою пакети акцій значної кількості акціонованих підприємств. Так, на початку 2002 р. вона володіла акціями 6265 українських акціонерних товариств, причому в 3385 з них, що складає 54%, пакет акцій держави перевищував 25% акціонерного капіталу. Однак дотепер в Україні відсутній діючий механізм управління державними пакетами акцій в акціонованих підприємствах. У зв'язку цим контроль над діяльністю акціонерного товариства, як і в попередніх випадках, належить, по суті, акціонерам-адміністраторам.

Внаслідок значної кількості суб'єктів зовнішнього середовища, з якими прямо або опосередковано взаємодіє підприємство, інтереси підприємства дуже різноманітні і кожне підприємство характеризується сукупністю тільки йому властивих інтересів, певним чином співвідносних між собою, що мають різний статус і належать різним суб'єктам. Інтереси підприємства не залишаються постійними і з часом змінюються, різноманітність і мобільність інтересів підприємства обумовлюють необхідність їхньої систематизації по ряду ознак і упорядкування на основі цієї систематизації. Тому доцільно провести систематизацію інтересів підприємства відповідно до певних ознак:

1. Вид інтересів: економічні, соціальні, екологічні, політичні.
2. Природа інтересів: добровільні (природні), примусові.
3. Ступінь значимості інтересів: глобальні, пріоритетні, другорядні.
4. Розподіл інтересів у часі: поточні, стратегічні.
5. Локалізація інтересів: галузеві, регіональні, функціональні.

Економічні інтереси підприємства обумовлені насамперед його позицією на ринку і станом конкурентоздатності його товарів. Вони представлені рядом економічних показників, такими як контрольована частка ринку, обсяг продажів,

ціна товарів, витрати на виробництво і прибуток.

Соціальні інтереси підприємства пов'язані з процесами розширеного відтворення робочої сили. Будь-яке підприємство зацікавлене в соціальній стабільності суспільства, що, зокрема, обумовлена такими факторами, як наявність робочих місць, навантаження на одне робоче місце, можливість одержання роботи відповідно до професії або спеціальністю, рівень оплати праці і своєчасність виплати заробітної плати, наявність житла, якість медичного обслуговування, можливість одержання соціальних пільг і т п.

Наявність *політичних інтересів* у підприємства обумовлена тим, що на його діяльність впливає і політична ситуація, що складається в країні або в регіоні. Деякою мірою способи управління економікою, методи і форми державного регулювання діяльності підприємств і є результатом політичних цілей і задач уряду, що знаходиться у влади.

Поява *екологічних інтересів* підприємства обумовлена рядом передумов, серед яких доцільно виділити соціальні, економічні і духовні.

Соціальні передумови носять переважно суспільний характер, оскільки забруднення навколишнього середовища приводить до підвищення рівня захворюваності населення, погіршує умови його життя, що, в остаточному підсумку, знижує продуктивність праці працездатного населення і веде до значних втрат. Вітчизняна статистика свідчить, що щорічно атмосфера, водні і земельні ресурси України забруднюються близько 100 млн. т шкідливих речовин. Загальна маса накопичених на території України відходів - більш 5 млрд. т, а площа земель, зайнята ними, складає вже 160 тис. га. Незважаючи на падіння темпів виробництва, продовжується процес прогресуючого нагромадження відходів і в промисловому, і в побутовому секторах: якщо в 1990 р. на один жителя припадало 318 т накопичених відходів, то в 2014 р. - понад 400 т. І тільки частина відходів, що не перевищує 10-12% їхніх утворень, знаходить застосування як вторинні ресурси.

Економічна природа екологічних інтересів підприємств стає усе більш очевидною. Більш того, набирає сили процес екологізації економіки, еколого-правові обмеження діяльності підприємств стають усе більш чіткими, завдяки чому удосконалюється механізм еколого-економічних відносин між державою і підприємствами. Економічні методи боротьби з екологічними правопорушеннями покликані стимулювати зацікавленість підприємств у виконанні екологічних законів, зробити вигідної для підприємств природоохоронну діяльність і підсилити економічну відповідальність підприємств за порушення природоохоронного законодавства.

Духовні передумови виникнення екологічних інтересів підприємства носять сугубо особистісний характер і обумовлені усвідомленням керівниками і власниками підприємств необхідності зниження шкідливого впливу діяльності підприємства на навколишнє середовище. Однак домінуючою передумовою екологічних інтересів підприємства є все-таки поява додаткових економічних витрат, зв'язаних з компенсацією нанесеного навколишньому середовищу збитку

й оплатою за перевищення граничнодопустимих концентрацій шкідливих речовин або погроза зупинки підприємства. Так, тільки протягом 1996-2007 рр. через порушення природоохоронного законодавства зупинена виробнича діяльність 772 господарських об'єктів України.

По своїй природі інтереси підприємства можуть бути добровільними (*природними) і примусовими*. *Природні* інтереси підприємства представлені його взаємодією із суб'єктами зовнішнього середовища, обумовленим потребами процесу виробництва і реалізації продукції, розширеного відтворення капіталу і робочої сили. Ці потреби задовольняються в ході взаємодії з такими суб'єктами зовнішнього середовища, як споживачі продукції, постачальники матеріальних ресурсів, засобів виробництва і капіталу і т.п. Характерною рисою природних інтересів підприємства є можливість при зниженні рівня дотримання інтересів змінити суб'єкт взаємодії й організувати взаємодію з іншим суб'єктом зовнішнього середовища.

Вимушеність інтересів підприємства обумовлена тим, що взаємодія підприємства із суб'єктом зовнішнього середовища носить вимушений характер, заснований або на використанні адміністративних методів управління, або на безальтернативності дій підприємства. Прикладом першого типу взаємодії є сплата підприємством податків у бюджети різних рівнів і відрахування в різного роду позабюджетні фонди. Як приклад взаємодії другого типу можна привести взаємодія підприємства з монополістами - природної монополії або монополіями, утвореними внаслідок безконтрольної концентрації виробництва або капіталу. Як правило, примусові інтереси підприємства ведуть до втрати частини його доходу внаслідок домінування інтересів партнера над інтересами підприємства. Особливістю вимушених інтересів підприємства є неможливість заміни суб'єкта взаємодії.

Розмаїтість і безліч інтересів підприємства обумовлюють необхідність їх впорядкування за ступенем їх значимості. З цього погляду можуть бути виділені *глобальний інтерес підприємства, пріоритетні і другорядні інтереси.*

Глобальний інтерес підприємства пов'язаний зі стадією, що завершує процес виробництва, - стадією обміну, у результаті якої підприємство одержує доход від реалізації своєї продукції, робіт або послуг. У зв'язку з цим глобальний інтерес підприємства обумовлений його положенням на ринку - займаною ринковою нішею, наявністю і використанням конкурентних переваг.

До *пріоритетних інтересів підприємства* відносяться ті, дотримання яких робить найбільш значний вплив на величину прибутку підприємства.

Пріоритетними інтересами підприємства можуть бути різні їхні види - економічні, соціальні або екологічні.

Другорядні інтереси підприємства не роблять істотного впливу на величину його прибутку, і, обумовлені загальною ситуацією в суспільстві загалом й в економіці країни, зокрема . Так, наприклад, надлишок робочої сили на ринку праці Луганської області і ріст безробіття, у тому числі і прихованого, обумовили другорядний характер соціальних інтересів більшості підприємств даного регіону.

З позиції розподілу інтересів підприємства в часі можна виділити *поточні і стратегічні інтереси підприємства.*

Поточні інтереси підприємства представлені існуючими взаємодіями підприємства із суб'єктами зовнішнього середовища, що забезпечують підприємству доход визначеної величини.

Стратегічні інтереси підприємства варто розглядати як його потенційно можливу взаємодію із суб'єктами зовнішнього середовища, що не здійснюються в даний час, але передбачаються як ймовірні в майбутньому. Стратегічні інтереси підприємства формуються виходячи з прогнозування стану зовнішнього середовища, одним з найважливіших аспектів якого є прогнозування інтересів найбільш значимих для економічної безпеки суб'єктів зовнішнього середовища.

Поточні і стратегічні інтереси підприємства можуть відповідати один одному, тобто стратегічні інтереси в цьому випадку можуть розглядатися як продовження поточних інтересів з деяким ступенем їхнього коректування.

З погляду локалізації інтересів підприємства можна виділити *галузеві, регіональні і функціональні інтереси. Галузеві інтереси* підприємства можна розглядати як взаємодії підприємства з підприємствами, їхніми об'єднаннями, науковими інститутами тієї галузі, до якої воно відноситься. Така взаємодія може здійснюватися, наприклад, у формі кооперування або комбінування виробництва, створення на тимчасовій або постійній основі галузевих об'єднань з різним рівнем централізації управління. Разом з тим галузеві інтереси підприємства найчастіше носять непрямий, опосередкований характер, оскільки обумовлені конкурентною боротьбою з виробниками аналогічної або взаємозамінної продукції.

Регіональні інтереси підприємства обумовлені його взаємодією із суб'єктами зовнішнього середовища, розташованими в одному з розглянутим підприємством регіоні. У цьому випадку мова йде про постачальників і покупців продукції підприємства, організаціях, що представляють ринкову інфраструктуру, наприклад, відділеннях або філіях банків, а також організаціях регіональної інфраструктури, наприклад, міських або обласних центрах зайнятості.

Функціональні інтереси підприємства розглядаються як його взаємодія із суб'єктами зовнішнього середовища по різних функціональних областях діяльності. Прикладами такої взаємодії є пошук партнерів по спільній реалізації інвестиційних або інноваційних проектів, а також звертання підприємства до маркетингових фірм або рекламних агентств.

Безліч різноманітних інтересів підприємства складають систему інтересів підприємства, що знаходяться у взаємозв'язку і взаємозумовленості. Система інтересів підприємства повинна бути досить різнобічною за орієнтацією і враховувати етап життєвого циклу підприємства - етап становлення, активного росту або зміни стратегії розвитку і ділової політики.

3. ОСНОВНІ ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

На основі проведеного дослідження доцільно виокремити ряд принципів, на яких будується процес формування системи інтересів підприємства та забезпечення його економічної безпеки:

1) *Комплексність, або системність.* Цей принцип припускає створення такої системи безпеки, яка б забезпечила захищеність підприємства, його майна, персоналу, інформації, різних сфер діяльності від всіляких небезпек і загроз, форс-мажорних обставин, тобто система безпеки (її складові елементи, сили, засоби) повинна бути достатньою, щоб забезпечити економічну, екологічну, науково-технічну, кадрову, пожежну і інші види безпеки. В забезпеченні безпеки підприємства повинні брати участь не тільки штатні співробітники і спеціальні служби, а практично всі підприємства, що служать. Організаційною формою комплексного використовування сил і засобів повинна стати програма забезпечення безпеки підприємства.

2) *Пріоритет заходів попередження (своєчасність).* Система безпеки повинна бути побудована так, щоб вона могла на ранніх стадіях виявляти різні деструктивні чинники, вживати заходів по запобіганню їх шкідливої дії і нанесення збитку підприємству. Реалізація даного принципу економічно є вигіднішою, ніж усунення завданого збитку.

3) *Безперервність.* Система безпеки повинна бути побудована так, щоб вона діяла, постійно захищаючи інтереси підприємства в умовах ризику і протидії зловмисникам.

4) *Законність.* Всі дії по забезпеченню безпеки підприємства повинні здійснюватися на основі чинного законодавства і не суперечити йому. Ті заходи безпеки, які розробляються на самому підприємстві, також повинні опиратися і здійснюватися в рамках чинних правових норм.

5) *Плановість*. Даний принцип вносить організованість у функціонування системи безпеки. Він дозволяє кожному учаснику процесу діяти логічно послідовно, строго виконуючи покладені на нього обов'язки. Діяльність по забезпеченню безпеки організовується на основі єдиного задуму, висловленого в комплексній програмі і конкретних планах по окремих напрямах і підвидах безпеки.

6) *Економність.* Система безпеки повинна бути побудована так, щоб витрати на її забезпечення були економічно доцільними, а вартість витрат була оптимальною і не перевищувала той рівень, при якому втрачається економічне значення їх вживання.

7) *Взаємодія.* Для забезпечення безпеки підприємства необхідно, щоб зусилля всіх осіб, підрозділів, служб були скоординовані. Тобто всі суб'єкти, учасники даного процесу повинні взаємодіяти один з одним, чітко знати, хто за що відповідає і хто що робить. Принцип взаємодії припускає також встановлення тісних ділових контактів і узгодження дій із зовнішніми організаціями (правоохоронними органами, місцевими або районними службами безпеки, органами влади і т.д.), здатними надати необхідне сприяння в забезпеченні

безпеки підприємства. Виконати це завдання може комітет (група, порада і ін..) безпеки підприємства.

8) *Поєднання гласності і конфіденційності.* Система основних заходів безпеки повинна бути відома всім співробітникам підприємства; її вимоги повинні виконуватися. Це дасть можливість своєчасно виявити і запобігти потенційним і реальним небезпекам і загрозам. І водночас, цілий ряд способів, сил, засобів, методів забезпечення безпеки повинні бути законспірованими і відомими дуже вузькому колу фахівців, що дозволить більш ефективно боротися як з внутрішніми, так і зовнішніми загрозами, своєчасно запобігати заподіянню шкоди підприємству.

9) *Компетентність.* Питання забезпечення безпеки підприємства є життєво важливим. В результаті навмисних дій зловмисників, несумлінної конкуренції, ухвалення катастрофічно ризикованих рішень тощо підприємству може бути завдано непоправного збитку. Тому питаннями забезпечення безпеки підприємства повинні займатися не дилетанти, а професіонали, глибоко обізнані і досвідчені в даній справі; такі, що уміють своєчасно оцінити обставини і прийняти правильне рішення. Система безпеки підприємства повинна будуватися відповідно до політики і стратегії безпеки, що проводиться на підприємстві.

4. ПОЛІТИКА, СИСТЕМА ТА СТРАТЕГІЇ БЕЗПЕКИ ПІДПРИЄМСТВА. ОБ'ЄКТИ І СУБ'ЄКТИ БЕЗПЕКИ

Політика безпеки підприємства – це система поглядів, заходів, рішень, дій в області безпеки, які створюють сприятливі умови для досягнення цілей бізнесу, тобто політика безпеки дозволяє підприємству виконувати виробничу програму, випускати конкурентоздатну продукцію (товари, послуги, роботи), підвищувати ефективність виробництва, примножувати власність, одержувати прибуток тощо.

Під стратегією безпеки розуміється сукупність найбільш значущих рішень, направлених на забезпечення програмного рівня безпеки функціонування підприємства. Стратегії безпеки за своїм змістом бувають різними. На практиці, можна виділити три типи стратегій безпеки підприємства:

1) Стратегія безпеки, пов'язана з необхідністю раптово реагувати на реально виниклі загрози виробничої діяльності, майну, персоналу і т.д. Тобто в даному випадку діє принцип «загроза - віддзеркалення». Створені (часто поспішно) для вирішення цього завдання підрозділи, служби, виділені сили і засоби можуть послабити або запобігти дії загроз; однак підприємству можуть бути завдані і значні збитки.

2) Стратегія безпеки, орієнтована на прогнозування, завчасне виявлення небезпек і загроз, цілеспрямоване дослідження економічної і криміногенної ситуацій як усередині підприємства, так і в навколишньому середовищі. Виділені для вирішення цього завдання фахівці, створені підрозділи і служби безпеки дають можливість усвідомлено і цілеспрямовано проводити роботу із створення

сприятливих умов для підприємницької діяльності.

3) Стратегія безпеки, спрямована на відшкодування (відновлення, компенсацію) нанесеного збитку. Дана стратегія може вважатися прийнятною лише тоді, коли збиток значний, або тоді, коли немає можливості здійснити стратегії першого або другого типу.

Слід також відмітити, що *система безпеки підприємства* є відмежованою безліччю взаємозв'язаних елементів, що забезпечують безпеку підприємства і досягнення ним цілей бізнесу. Складовими елементами такої системи є об'єкт і суб'єкт безпеки, механізм управління безпекою, а також стратегічні дії по управлінню безпекою.

Об'єктом безпеки виступає все те, на що направлені зусилля по забезпеченню безпеки. До об'єктів слід віднести:

а) різні види діяльності підприємства (виробнича, комерційна, постачальницька, управлінська і ін.);

б) майно і ресурси підприємства (фінансові, матеріально-технічні, інформаційні, інтелектуальні і ін.);

в) персонал фірми, її керівників, акціонерів, різні структурні підрозділи, служби, партнерів, співробітників, що володіють інформацією, що становить комерційну таємницю і ін.

Суб'єктами безпеки підприємства є ті особи, підрозділи, служби, органи, відомства, установи, які безпосередньо займаються забезпеченням безпеки бізнесу. Оскільки діяльність по забезпеченню безпеки підприємства багатоаспектна, цю задачу неможливо вирішити за допомогою одного чи двох органів. Як правило, до суб'єктів безпеки підприємства відносяться багато органів, які можна класифікувати за різними ознаками:

1) Залежно від приналежності: на суб'єкти, що займаються цією діяльністю безпосередньо на підприємстві, і зовнішні органи і організації.

2) Залежно від безпосередньої участі: на спеціальні суб'єкти і решта персоналу фірми.

3) Залежно від дії (впливу) на об'єкт безпеки: на суб'єкти прямого і непрямого призначення.

4) Залежно від легітимності: на офіційні органи і кримінальні структури («дахи»).

5) Залежно від рівня підпорядкованості: на державні органи і недержавні.

Синтезувавши представлену класифікацію суб'єктів безпеки, виділимо дві групи і дамо їм характеристику.

Отже, *до першої групи* відносяться ті суб'єкти, які входять в структуру самого підприємства і вирішують завдання по забезпеченню його безпеки. До складу цієї групи входять спеціальні суб'єкти (служба безпеки, або охорона, пожежна команда, рятувальна служба), а також решту персоналу фірми, який також піклується про безпеку свого підприємства.

До другої групи відносяться ті суб'єкти, які знаходяться за межами підприємства і не підкоряються його керівництву. Це перш за все державні

органи, які створюють умови забезпечення безпеки підприємства. До них відносяться:

- законодавчі органи – приймають закони, що створюють правову основу діяльності по забезпеченню безпеки на рівні держави, регіону, підприємства і особи;
- виконавські органи влади – проводять політику, деталізують механізми безпеки;
- судові органи – забезпечують дотримання законних прав підприємства і його співробітників;
- державні інститути – здійснюють охорону кордону, митний, валютно-експортний, податковий контроль і т.п.;
- правоохоронні органи – ведуть боротьбу з правопорушеннями і злочинами;
- система наукових установ – реалізує завдання по наукових опрацьовуваннях проблем безпеки і підготовки кадрів в даній галузі.

З початком ринкових реформ паралельно з державними стали утворюватися недержавні організації, агентства, установи. Це різні приватні охоронні і детективні організації, аналітичні центри, інформаційні служби, учбові, наукові і консультаційні організації тощо. Вони, як правило, за відповідну плату надають послуги з охорони об'єктів, забезпечують захист інформації, комерційної таємниці, накопичують інформацію про конкурентів, ненадійних партнерів тощо.

5. *ФОРМУВАННЯ МЕХАНІЗМУ УПРАВЛІННЯ БЕЗПЕКОЮ ПІДПРИЄМСТВА*

Криміналізація господарського життя привела до того, що на ринку охоронних послуг з'явилися і кримінальні структури, так звані «дахи», які на основі погроз, шантажу, насильства, погромів, експлуатуючи підприємців, втягують їх в кримінальний бізнес. Як правило, «дах» забезпечує організована злочинна група, яка за винагороду організовує прикриття підприємству або окремій особі, що має істотні доходи. Найпоширенішими видами послуг «даху» є: захист від домагань, нападів і ін. організованих злочинних груп; забезпечення особистої безпеки підприємців; протидія конкурентам фірми; залагоджування суперечок з партнерами; стягнення боргів з боржників тощо.

Механізм управління безпекою підприємства є об'єктивно обумовленою послідовністю дій по забезпеченню економічної безпеки підприємства. До основних його елементів можна віднести: визначення потреб в забезпеченні безпеки, сил і засобів, а також організаційно-господарського механізму, формулювання цілей і задач забезпечення безпеки. Проведення в життя вироблених заходів забезпечує досягнення поставлених цілей.

Формування системи безпеки, і перш за все створення її органів (суб'єктів), залежить від розмірів підприємства, його економічних, фінансових, виробничо-

технічних, інформаційних, інтелектуальних, професійних, організаційних і інших можливостей. Як показує досвід, малі підприємства частіше за все користуються послугами зовнішніх спеціалізованих приватних організацій: консалтингових, охоронних, інформаційних і ін. До них відносяться: реєстраційні палати, фірми по підбору і атестації кадрів, кредитні бюро, що надають інформаційні послуги з ділового реноме партнерів, центри маркетингових досліджень, приватні охоронні і детективні організації і ін.

Середні підприємства можуть використовувати комбіновану систему безпеки. З одного боку, у разі потреби вони можуть одержувати послуги від зовнішніх організацій, а з іншого – активно опиратися на можливості своїх служб і підрозділів, зокрема, юридичної, фінансової, маркетингу, охорони, техніки безпеки, кадрів, економічного аналізу, пропускного режиму, діловодства і ін. В цілях підвищення ефективності діяльності служб і підрозділів по захисту економічних інтересів фірми на підприємстві повинен бути створений координуючий орган або призначений один із керівників, відповідальний за економічну безпеку.

Для крупного підприємства найбільш доцільним є створення власної служби безпеки. Як правило, всю діяльність по забезпеченню безпеки координує один з керівників підприємства. Для вироблення пропозицій і виконання консультативних функцій може створюватися рада з безпеки.

Служба безпеки може включати рызноманытны відділи, групи, підрозділи. До найбільш важливих з них можна віднести наступні підрозділи: охорони, режиму, по роботі з кадрами, інженерно-технічного захисту, розвідки і контррозвідки (детективна група), інформаційно-аналітичної діяльності, оперативного реагування, кризову групу і ін. При цьому забезпечується пожежна безпека, збереження майна, запобігання несанкціонованому доступу до об'єкту, здійснюється контроль і ін. За допомогою організаційних заходів створюються спеціальні підрозділи, пости, патрулі, зони безпеки тощо.

Фінансові кошти необхідні для придбання технічних пристроїв безпеки, змісту служби безпеки, підготовки кадрів, стимулювання праці і ін. Аналогічним чином по прямому призначенню повинні використовуватися і інші сили і засоби.

Сформована система безпеки підприємства зможе вирішувати завдання, що стоять перед нею, тільки тоді, коли діятиме, тобто її невід'ємним складовим елементом є практичні дії по забезпеченню безпеки бізнесу.

Таким чином, в результаті розгляду системи безпеки підприємства можна зробити наступний висновок: служба безпеки підприємства покликана на основі ефективного використовування корпоративних ресурсів створити умови для досягнення цілей бізнесу, своєчасно знайти і максимально послабити дію різного роду небезпек і загроз в умовах конкуренції й господарського ризику.

Тема 9. СОЦІАЛЬНО-ЕКОНОМІЧНІ ПЕРЕДУМОВИ ВИНИКНЕННЯ МАЙНОВИХ СУПЕРЕЧОК, КОРПОРАТИВНИХ КОНФЛІКТІВ ТА НЕОБХІДНІСТЬ ФОРМУВАННЯ ЕФЕКТИВНОЇ СИСТЕМИ БЕЗПЕКИ БІЗНЕСУ

1. ЗАКОНОДАВЧІ ПРОТИРІЧЧЯ ЯК ФАКТОР ЕКОНОМІЧНОЇ НЕВИЗНАЧЕНОСТІ ТА НЕСТАБІЛЬНОСТІ ВИРОБНИЧИХ ВІДНОСИН ТА ПОРОДЖЕННЯ МАЙНОВИХ СУПЕРЕЧОК В ПІДПРИЄМНИЦЬКІЙ ДІЯЛЬНОСТІ

Неузгодженість окремих статей наприклад Цивільного і Господарського кодексів та їх негативний вплив на діяльність суб'єктів господарювання виявила доцент кафедри менеджменту Тернопільського національного економічного університету Світлана Черничинець.

1 січня 2004 року в українському цивільному законодавстві відбулися фундаментальні перетворення. Прийняття нового Цивільного і Господарського кодексів ознаменувало собою новітню епоху для національної системи права. Зазначені законодавчі акти стали новою основою для розвитку її ключових галузей. Проте факт прийняття кодексів мав й протилежну сторону: будь-які дефекти таких основоположних документів набували вирішального значення, оскільки всі підзаконні акти повинні будуватися на їх основі. Саме з цієї причини Цивільний і Господарський кодекси повинні бути однозначними, зрозумілими і позбавленими дефектів.

Аналіз Кодексів показує, що вони дійсно містять серйозні проблеми. Існує значний ризик виникнення конфліктів, спричинених як внутрішніми недоліками Кодексів, так і протиріччями між Кодексами та іншими законодавчими актами.

Господарський кодекс України встановлює відповідно до Конституції України правову основу господарської діяльності (господарювання), яка базується на різноманітності суб'єктів господарювання різних форм власності.

Господарський кодекс України має на меті забезпечити зростання ділової активності суб'єктів господарювання, розвиток підприємництва і на цій основі підвищення ефективності суспільного виробництва, його соціальну спрямованість відповідно до вимог Конституції України, утвердити суспільний господарський порядок в економічній системі України, сприяти гармонізації її з іншими економічними системами.

Цивільним законодавством регулюються цивільні відносини, засновані на юридичній рівності, вільному волевиявленні, майновій самостійності їх учасників.

В результаті цього виникли такі основі проблеми:

- кожен кодекс містить положення, які суперечать іншим

положенням цього самого кодексу.

- існують істотні протиріччя між багатьма положеннями Цивільного і Господарського кодексів, які регулюють одні й ті самі питання.
- існують протиріччя між положеннями кодексів і відповідних законодавчих актів.
- деякі позитивні ідеї кодексів не можуть бути практично здійснені внаслідок прогалин у відповідному законодавстві.

Вище згадані проблеми перешкоджають нормальному веденню підприємницької діяльності у більшості сфер економіки, унеможливлюють правове регулювання деяких правовідносин і здійснення правового захисту інтересів учасників економічного сектору. Крім того, велика кількість прогалин в українському цивільному законодавстві не залишає державним органам та судам іншого виходу крім самостійного тлумачення змісту законів, і сприяє поширенню корупції серед державних органів та недобросовісної конкуренції серед суб'єктів господарювання. У цьому відношенні, Господарський кодекс являє собою найбільшу загрозу для розвитку вільного ринку в Україні, оскільки його природа і методи регулювання є більш притаманними колишній командно-адміністративній економіці, аніж спрямованими на підтримку нової ринкової економіки України.

До 1 січня 2004 року старий радянський Цивільний кодекс, прийнятий у 1963 році, був основним актом цивільного законодавства в Україні. Треба визнати, що за роки після отримання Україною незалежності у 1991 році, Парламент України робив спроби переглянути окремі положення старого радянського Цивільного кодексу. Однак ці локальні зусилля загалом не змогли достатньою мірою змінити природи документа в тій мірі, яка необхідна для безперешкодного функціонування ринкової економіки в країні, яка до набуття незалежності знала лише командну економіку. Спроби вирішити проблеми, які виникли у результаті намагань встановити систему права ринкової економіки на підвалинах основоположного законодавчого акту командно-адміністративної системи шляхом прийняття підзаконних актів у ході знову ж таки непослідовного процесу, також виявилися невдалими.

Україна нарешті зрозуміла, що для побудови правової інфраструктури, потрібної для підтримки ринкової економіки, необхідно змінити основи цієї правової інфраструктури. Саме з цієї причини було прийнято два нових кодекси (Господарський кодекс і новий Цивільний кодекс) і введено їх у дію в 2004 році.

Незважаючи на різні назви документів, вони обидва регулюють багато питань підприємництва. Обсяг Цивільного кодексу є, звичайно, ширшим, ніж обсяг Господарського кодексу. Крім того, Цивільний кодекс регулює набагато ширше коло питань (від правового визначення фізичної особи до права власності і господарських правовідносин). З іншого боку, Господарський кодекс орієнтований конкретно на господарські правовідносини.

До 1991 року законодавство України підтримувало концепцію права власності, визначену як "колективна власність", за якою майнові права мала група фізичних або юридичних осіб і жодна фізична чи юридична особа не мали

виключних прав на майно. Частина 10 Господарського кодексу приймає цю форму власності на майно, яке будь-який учасник, але лише підприємства колективної форми власності, вносить до статутного фонду такого виду підприємства в обмін на частку участі у такому підприємстві. Після внесення таке майно стає колективним майном усіх учасників підприємства колективної форми власності, проте, у той же час воно залишається "окремим" і визначається як колишнє майно учасника, який його вніс. Однак, при виході учасника з підприємства колективної форми власності внесене ним майно повертається йому, воно втрачає свій статус колективної власності і знову стає приватною власністю.

У розділі 1 книги 3 Цивільного кодексу пропонується інший підхід. Майно, внесене до будь-якого підприємства, стає приватною власністю самого підприємства. Після внесення, воно не залишається окремим і не ототожнюється з конкретним учасником. І після виходу учасника з підприємства майже немає гарантій, що конкретне майно, яке вніс такий учасник, буде йому повернуте. Підприємство виплачує учаснику, який виходить, вартість його внеску за власною оцінкою самого підприємства.

Це створює певний ризик для будь-якого учасника підприємства: при виході з підприємства, такий учасник змушений покладатися лише на сумлінність його ділових партнерів у питанні справедливої оцінки його внеску і виплати йому вартості останнього після виходу. Існує також проблема, яка може спричинити конфлікти між діловими партнерами щодо того, який з варіантів - повернення майна в натурі чи виплата його грошової вартості - повинен застосовуватися до учасника, який виходить. У цьому питанні положення Цивільного кодексу більше відповідають "західній" юридичній практиці. Проте, можливо, варто розглянути шляхи вирішення питань, щодо непорядних партнерів, які здійснюють несправедливу виплату або взагалі не відшкодовують вартість майна учасника, який виходить зі складу учасників підприємства. Наприклад, Цивільний кодекс можна було б доповнити положеннями, які б забезпечували права учасника на незалежну і справедливу оцінку його майнових прав після виходу з підприємства і/або гарантію права учасника на повернення його внесків після виходу в натурі, а не грошовими коштами.

З огляду на те, що сфери регулювання Цивільного і Господарського кодексів частково співпадають і що ці два законодавчі акти регулюють багато однакових питань, необхідно, щоб їх визначення суб'єктів регулювання були ідентичними. Як видно з розбіжностей положень кодексів, про визначення видів юридичних осіб, які вони дозволяють створювати в Україні, на сьогодні ситуація інша:

- Стаття 79 Господарського кодексу визначає господарські товариства, які він дозволяє створювати в Україні, так само, як і стаття 113 Цивільного кодексу, проте, визначення, надані у цих двох статтях, не є тотожними.
- Господарський Кодекс містить терміни "суб'єкт господарювання" та "господарська організація". Цивільний кодекс таких термінів не містить. Відтак правомірність зазначених термінів можна оскаржувати.
- Стаття 115 Господарського кодексу визначає юридичну особу у формі

"орендного підприємства". Цивільний кодекс не містить згадки про таку форму організації юридичної особи.

- Кілька положень Господарського кодексу, наприклад, статті 63.1, 113 і 128.3 містять посилання на юридичну особу у формі "приватного підприємства". Цивільний кодекс не дозволяє існування юридичної особи у такій організаційній формі.
- Коли один кодекс вказує, що юридична особа у певній організаційній формі може існувати, а інший кодекс не визнає такої форми організації, то правомірність існування організаційно-правової форми такої юридичної особи може бути оскаржена. Найбільш прийнятним для бізнесу вирішенням цієї проблеми було б редагування Господарського кодексу з одночасним включенням до Цивільного кодексу всіх тих організаційно-правових форм юридичної особи, які дозволяються Господарським кодексом, але не згадуються в Цивільному кодексі. Внаслідок цього вибір відповідної організаційно-правової форми стане більш безпечним для учасників ринку завдяки вирішенню конфлікту між кодексами, а також буде розширений шляхом збільшення вибору форм організації юридичної особи, які дозволяються Цивільним кодексом.

Метою прийняття будь-якого кодексу є прагнення забезпечити комплексне регулювання його предметної сфери. На сьогодні Україна має два кодекси, сфери застосування яких частково перетинаються: Цивільний кодекс охоплює нормативне регулювання підприємницької діяльності, але не обмежується ним; а Господарський кодекс орієнтований на правовідносини у сфері здійснення господарської діяльності. Це призводить до того, що питання підприємництва підлягають подвійному регулюванню. Проте жоден з кодексів не здійснює комплексного регулювання. Тому, щоб відповісти на численні питання, які виникають в процесі повсякденного ведення підприємницької діяльності, необхідно одночасно звертатися до обох кодексів. Хоча ця схема і є нелогічною, вона все ж могла б бути працездатною, якби кодекси у деяких випадках не заперечували один одного, в інших випадках не залишали законодавчих прогалин і загалом не містили нечітких і двозначних положень, як це, на жаль, є у дійсності. Наприклад:

- Стаття 291.3 Господарського кодексу дозволяє дострокове розірвання договорів оренди на підставах, передбачених Цивільним кодексом, але у відповідності з порядком, який встановлюється статтею 188 Господарського кодексу. Відповідно до статті 291.4 Господарського кодексу, наслідки такого припинення дії вказуються у Цивільному кодексі.
- Стаття 265.6 Господарського кодексу визначає, що відносини суб'єкти господарювання, не знають, чого вимагає закон, але й нерідко і державні органи, які забезпечують його виконання. Важко уявити більш несприятливе середовище для діяльності суб'єктів господарювання і розвитку підприємництва.

- Глава 14 Цивільного кодексу описує типи цінних паперів, які можуть бути в обігу в Україні, і процедури проведення операцій з цими цінними паперами. Зазначена глава класифікує фінансові інструменти як цінні папери на пред'явника, іменні цінні папери або ордерні цінні папери. Стаття 197.5 Цивільного кодексу встановлює, що лише ордерний цінний папір може передаватися шляхом індосаменту.
- Стаття 163.3 Господарського кодексу прямо суперечить Цивільному кодексу, визнаючи лише два типи цінних паперів: іменні і на пред'явника. Крім того, зазначена стаття встановлює, що лише іменні цінні папери можуть передаватися шляхом індосаменту.

Тут конфлікт між двома кодексами є очевидним. У цьому випадку слід залишити ці положення Цивільного кодексу без змін і редагувати Господарський кодекс.

Численні протиріччя між Господарським і Цивільним кодексами, однак, не є найвагомішим аргументом на користь редагування деяких статей Господарського кодексу. Скоріше, основною проблемою Господарського кодексу є те, що він дозволяє державі та її органам втручатися у сферу бізнесу, що зашкоджує розвиткові приватного підприємництва в Україні. У той час, як Цивільний кодекс встановлює правову основу підтримки вільної ринкової економіки і обмежує втручання держави у підприємницьку діяльність, Господарський кодекс часто займає протилежний позицію, спрямовану на санкціонування і сприяння втручанню держави в економіку.

Для ілюстрації вищенаведеного твердження варто прискіпливіше розглянути главу 8 розділу II Господарського кодексу, яка регулює діяльність державних підприємств на українському ринку. Проблема з главою 8 полягає в тому, що нерідко важко зрозуміти, коли кодекс говорить про державні органи, уповноважені виконувати функції державного управління, і коли — про державні підприємства, які є незалежними учасниками ринку. Ці два поняття мають тенденцію до злиття, що призводить до того, що Господарський кодекс фактично дозволяє безпосередньо державі діяти на ринку через довірене державне підприємство: наприклад, держава має право наймати і звільняти керівників державних підприємств і спрямовувати діяльність цих підприємств у якості їх власника.

В результаті цього Господарський кодекс пропонує оновлену версію старої концепції "соціалістичного підприємства", де державні органи займаються і державним управлінням і участю на ринку. Ця ситуація могла вважатися нормальною до 1991 року, коли більшість підприємств були у державній власності. Проте сьогодні основними учасниками на ринку є недержавні суб'єкти господарювання, які конкурують на задекларованому вільному ринку. Такий стан справ уряд, теоретично, мав би підтримувати і заохочувати. Проте Господарський кодекс дотримується протилежної позиції. Коли державні відомства стають бізнес-конкурентами недержавних підприємств, то майже із стовідсотковою впевненістю можна вгадати, хто залишиться у виграші. Адже держава не

обмежується, наприклад, лише лобіюванням прийняття вигідних їй нормативно-правових актів, вона фактично сама може приймати і створювати необхідні їй нормативи. Держава може надати собі (тобто, державним підприємствам) кредити, гранти, податкові пільги і будь-яку кількість інших матеріальних і нематеріальних переваг. В результаті державні і недержавні суб'єкти господарювання конкурують не за справедливих можливостей, що є проблемою ситуації, яка склалася в економіці нашої держави на сьогоднішній день.

Структура діяльності державних підприємств, яку встановлює Господарський кодекс, є доволі непрозорою. Наприклад, стаття 142.3 Господарського кодексу встановлює, що порядок використання прибутку державних підприємств встановлюється відповідно до закону. Проте це визначення є настільки неконкретним, що втрачає будь-який сенс, оскільки кодекс не дає жодного посилання на згаданий "закон". Неважко спрогнозувати, що результатом цього стане можливість використання прибутків державних підприємств без жодного контролю, з огляду на те, що не існує дієвого механізму моніторингу, і, навіть, якби він був, то все одно немає реального закону щодо використання таких прибутків, виконання якого можна було б контролювати.

Ця ситуація, за якої сама держава, через свої державні підприємства, змагається за прибутки з недержавними суб'єктами господарювання, також створює конфлікт інтересів для самих державних службовців. Як тільки держава ставить перед собою за мету отримання прибутків, її службовці можуть піддатися спокусі "поповнити" свою бюджетну зарплатню і самим отримати якийсь "прибуток" також за рахунок недержавних підприємств. Як варіант, послуги державних підприємств можуть надаватися за завищеними тарифами. Урядові відомства, які володіють державними підприємствами, можуть попросити натиснути на недержавних суб'єктів господарської діяльності, щоб ті платили такі завищені ціни, загрожуючи їм адміністративними перевірками, санкціями та іншими заходами тиску для того, щоб змусити виконувати свої вимоги.

З огляду на зазначене, досить показовою є стаття 43.4 Господарського кодексу. Вона дозволяє державним службовцям і посадовим особам органів державної влади займатися підприємницькою діяльністю лише з одним винятком: їх можуть попросити призупинити свою підприємницьку діяльність на час оголошення надзвичайного стану або війни. Очевидно, що це положення порушує імперативне правило, закріплене у другому параграфі статті 42 Конституції України, яке встановлює, що підприємницька діяльність посадових і службових осіб органів державної влади та органів місцевого самоврядування "обмежується законом".

На жаль, вищезазначена проблема не є прикрим виключенням у Господарському кодексі. Він містить багато інших положень, які є більш характерними для планової, а не ринкової економіки, про яку йде мова у статті 6 Господарського кодексу. Наприклад, стаття 11 Господарського кодексу передбачає прийняття державою законів про прогнозування економічної ситуації і підготовку урядових програм для управління розвитком української економіки.

Стаття 11.5 Господарського кодексу дозволяє державі позбавляти підприємства, які не дотримуються державних планів щодо економіки, певних встановлених пільг та переваг. А стаття 13.4 Господарського кодексу уповноважує Кабінет Міністрів України і урядові відомства встановлювати державні завдання, які є обов'язковими для суб'єктів господарювання. Все зазначене має ознаки планової економіки.

Перелічені у попередньому абзаці положення є несприятливими для розвитку підприємництва у ринковій економіці. Вони практично беруть в ланцюги підприємства недержавної форми власності, змушуючи її рухатися лише так, як забажає держава. Якщо такі та аналогічні їм положення залишатимуться в силі, недержавні суб'єкти господарської діяльності будуть позбавлені можливості обирати шляхи для вдалого розміщення їх капіталу.

Рештки сумнівів щодо справжньої природи Господарського кодексу остаточно зникають після ознайомлення зі статтею 142.4 Господарського кодексу. Ця стаття дозволяє державі застосовувати нормативи, податки, податкові пільги та господарські санкції саме для того, щоб впливати на вибір суб'єктами господарювання шляхів використання їх власного прибутку. Хоча таке "стимулювання" і не є чимось абсолютно новим (наприклад, у західних країнах з ринковою економікою), але варто мати на увазі те, що в контексті України, з її історією планової економіки, "важелі" можуть виявитися далеко не невинними у порівнянні з їхніми західними аналогами. Наприклад, ніщо у формулюванні статті 142.4 не зможе перешкодити державі впливати на поведінку суб'єкта господарювання шляхом впровадження надвисоких ставок податків на прибуток, отриманий від небажаних для неї видів господарської діяльності. Господарський кодекс фактично дає державі повну свободу у використанні економічних важелів таким чином, який вона вважатиме за потрібний для примушення приватних підприємств діяти так, як сама держава вважає за доцільне.

Наведені приклади вже достатньо ілюструють характер Господарського кодексу і дають переконливі аргументи на користь його повного редагування. Коли документ, гіпотетично створений для сприяння вільному ринку (знову див. статтю 6 Господарського кодексу) містить цілі глави, присвячені фактично впровадженню планової економіки, такий документ явно потребує перегляду. Замість того, щоб повторювати помилки Парламенту України, коли він робив безсистемні спроби вдосконалити старий радянський Цивільний кодекс для того, щоб перетворити його на прогресивний "капіталістичний" нормативний документ доцільним було б термінове ухвалення Парламентом найбільш прийнятного рішення, а саме - про редагування Господарського кодексу повністю і початок всієї роботи з чистого аркуша.

Крім розглянутих вище питань Господарський кодекс як документ, який регулює господарську діяльність в Україні, має багато інших проблем.

Господарський кодекс займає дві суперечливі позиції щодо законності одностороннього припинення дії господарського договору. З одного боку, стаття 188.1 дозволяє одностороннє розірвання договору, якщо інше не передбачено

договором. З іншого боку, стаття 207.2 встановлює, що, коли договір містить положення, яке дозволяє одностороннє припинення його дії, то така дія є незаконною.

Прийняття нового Цивільного кодексу стало суттєвим кроком уперед у процесі розвитку правової системи України. Засади цього документу сприяють поступу країни на шляху до створення справжньої вільної ринкової економіки. Основне призначення Цивільного кодексу полягає у тому, щоб закласти міцні підвалини для регулювання основних галузей цивільного законодавства. На основі цих підвалин має бути прийматися підзаконні нормативні акти. Оскільки Цивільний кодекс служить основою для більшої частини законодавства України, необхідно, щоб його положення були недвозначними, чіткими і позбавленими недоліків, бездоганними - інакше, ефективність виконання законодавства, яке ґрунтується на Цивільному кодексі, ставиться під питання.

Проте практичне застосування Цивільного кодексу показало, що і він далекий від досконалості. Крім наявності в ньому конфліктів з Господарським кодексом, Цивільний кодекс також містить численні двозначні і суперечливі положення, які призводять до виникнення перешкод розвитку та функціонування підприємництва в Україні.

Стаття 191 Цивільного кодексу визначає підприємство як єдиний майновий комплекс і встановлює, що підприємство може бути об'єктом купівлі і продажу, застави, оренди та інших дій. Проте глава 7 Цивільного кодексу, яка регулює правовий статус юридичних осіб, навіть не згадує про "підприємство". Відтак, не існує окремого виду юридичної особи або організаційно-правової форми, які б можна було назвати "підприємством", терміном , який так часто використовується в українському праві. Отже, неможливо точно визначити, чим же насправді є "підприємство".

Цивільний кодекс також не дає жодного прикладу використання визначення підприємства, наведеного у статті 191. Розділ перший третьої книги Цивільного кодексу, який регулює питання права власності, не згадує підприємство в якості незалежного об'єкту, який можна мати у власності. Це не узгоджується зі статтею 191.4 і ускладнює розуміння того, яким саме чином можна відчужувати підприємство, що дозволяється статтею 191.4. Тому до розділу першого третьої книги Цивільного кодексу повинні бути внесені поправки, які б чітко вказували на те, що підприємством можна володіти, права власності на підприємство можна передавати тощо. Відповідно і глава 7 Цивільного кодексу теж повинна бути змінена з метою включення до неї визначення підприємства як окремої організаційної форми.

Через зазначені вище причини українське цивільне законодавство потребує вдосконалення, що має здійснюватися у таких напрямках:

- ґрунтовний перегляд найсуттєвіших конфліктів між положеннями кодексів з метою впорядкування правового регулювання цивільних правовідносин. У більшості випадків конфлікти між Цивільним кодексом, Господарським кодексом та іншими нормативними актами повинні

вирішуватися на користь Цивільного кодексу. Проте у деяких випадках, Цивільний кодекс також потребує внесення змін;

- прийняття усіх поки не існуючих законодавчих актів, посилання на які містяться в Цивільному кодексі. Найважливішими з них є законопроект про міжнародне приватне право та законопроект про акціонерні товариства.

Цивільне законодавство України формує собою основу її системи права в цілому. Що ж стосується ділового життя країни, то цивільне законодавство закладає основні правові принципи, необхідні для функціонування ринкової економіки, наприклад: принципи організації договірних правовідносин, права власності і майнових прав, а також правового статусу юридичних і фізичних осіб. Саме на цій основі ґрунтується решта законів країни, і від неї залежить їх правильне функціонування.

2. УЧАСНИКИ КОРПОРАТИВНОГО ПІДПРИЄМНИЦТВА ТА ПРАВОВІДНОСИНИ МІЖ НИМИ

Як правило, учасники господарського товариства – потенційні супротивники самого товариства. Відповідно до ст. 114 Цивільного кодексу України (далі ЦК України), учасниками господарських товариств можуть виступати фізичні або юридичні особи, які є громадянами України, або іноземцями. Обмеження участі в господарських товариствах може бути встановлено законом. Для прикладу можна привести Закон України «Про цінні папери і фондову біржу», де вказано, що фондова біржа може бути створена не менше ніж 20 засновниками – торговцями цінними паперами. Вказані засновники повинні мати дозвіл на здійснення комерційної і комісійної діяльності цінними паперами. Тобто, обмеження участі в господарських товариствах можуть передбачатися шляхом спеціальних вимог, що мають як кількісні, так і якісні обмеження до складу засновників господарського товариства. Створення господарського товариства, окрім повного і командитного, можливе однією особою, яка стає його єдиним учасником. Право власності на майно виходить з ознак юридичної особи і має самостійну майнову відповідальністю, характеризується наявністю відособленого майна. Закріплене за господарським товариством майно створює необхідну базу для його нормальної, прибуткової діяльності. Відповідно до ст. 115 ГК України, господарське товариство може бути власником:

- майна, переданого йому учасниками (засновниками) товариства у власність, як внесок в статутний капітал;
- продукції, що випущена товариством в результаті господарської діяльності;
- отриманих доходів;
- іншого майна, придбаного на підставах, не заборонених законом.

Внеском в статутний (об'єднаний) капітал господарського товариства можуть бути гроші, цінні папери, інші речі або майно, або інші відчужені права, що мають грошову оцінку, якщо інше не встановлене законом. Грошова оцінка внеску учасника господарського товариства здійснюється за відома інших учасників товариства, а в деяких інших випадках, підлягає незалежній експертній оцінці. Передаючи товариству майнові внески, тобто будівлі, споруди, гроші або внески у формі певних майнових прав у вигляді права користування майном або інтелектуальної власності, учасник одержує свого роду компенсації – відповідні корпоративні права. Для прикладу, в акціонерних товариствах ці корпоративні права оформляються акціями, в товариствах з обмеженою відповідальністю – свідоцтвом про право на частку (її частини) в статутному фонді. Оцінка внеску учасника (засновника) господарського товариства проводиться в національній валюті України – гривні.

Розглянемо більш детально дане питання. З однієї сторони майно, внесене учасником товариства в статутний капітал господарського суб'єкта є власністю юридичної особи і учасник товариства має корпоративні права управління та участі у прибутку товариства. На наш погляд, тут не треба ототожнювати майно учасника (засновника) з майном господарського суб'єкта, в якому цей громадянин є учасником. Коли трапляється питання про звернення стягнення на майно боржника – учасника юридичної особи, то ця різниця є суттєвою. Стаття 166 ЦК України дає чітку регламентацію такої можливості звернення стягнення на пай члена виробничого кооперативу. Закон України «Про господарські товариства» дає таку можливість на частку засновника товариства з обмеженою відповідальністю (ст. 57), повного товариства (ст. 73), а ось, що стосується акціонерних товариств, то справи тут складаються дещо інакше. Належні боржнику акції акціонерного товариства не є часткою в статутному фонді товариства, а є лише цінними паперами з визначеною номінальною вартістю, які можуть бути реалізовані, в тому числі і за ринковою вартістю.

Учасники господарського товариства мають право у встановленому засновницькими документами і чинним законодавством порядку:

- брати участь в управлінні товариством;
- брати участь в розподілі прибутку товариства і одержувати його частину (дивіденди);
- вийти в установленому порядку з товариства;
- здійснити відчуження часток в статутному (об'єднаному) капіталі товариства, цінних паперів, що засвідчують участь у товаристві, в порядку, встановленому законом;
- одержувати інформацію про діяльність товариства в порядку, встановленому засновницькими документами.

З наведеного зрозуміло, що учасники товариства є власниками корпоративних прав, тобто мають право власності на статутний фонд (капітал) юридичної особи, або його частину (пай), включаючи права на управління, отримання відповідної частини прибутку, а також активів у разі ліквідації

юридичної особи. Вищий Господарський суд України в своїй касаційній ухвалі від 15 червня 2005 року підтвердив положення про те, що право власності на майно товариства, можливе тільки у разі ліквідації господарського товариства, а до цього моменту його учасники є власниками своїх акцій, тобто корпоративних прав, а не майна товариства. Саме така категорія питань цікавить тримачів акцій, які вважають, що у разі виходу з числа учасників товариства, вони мають право обміняти свої акції на відособлені будівлі і споруди оскільки володіють достатньою їх кількістю.

Розглядаючи це питання в правовому полі, слід відмітити, що судовій практиці відомі випадки, коли задовольняються позови учасників товариства про виділення частини в спільному майні товариства, мотивуючи це правом власності на певну кількість акцій. Але у Судової палати по Цивільних справах Верховного Суду України із цього приводу своя думка, оскільки при ухваленні таких рішень порушуються норми матеріального права, оскільки чинне законодавство передбачає врегулювання питань оплати вартості майна при виході учасника з товариства. Таке положення закріплено в статті 54 Закону України «Про господарські товариства», що у свою чергу свідчить про пайову участь акціонера в статутному фонді товариства, підтверджує його членство і право на участь в управлінні товариством.

Учасник товариства має право на отримання інформації про його діяльність. Інформацією є документовані або публічно оголошені відомості про події і явища, що мали місце в господарському товаристві, або державі. Ця інформація розміщується у фінансовій звітності, кошторисі і інших документах товариства. Крім цього, учасник має право звернутися безпосередньо за отриманням інформації до товариства. Такий порядок встановлюється в засновницьких документах. Рішенням Державної комісії з цінних паперів і фондового ринку від 26 січня 2005 року № 27, затверджені методичні рекомендації щодо доступу акціонерів і інших зацікавлених осіб до інформації про акціонерне товариство. Мета цих рекомендацій полягає в сприянні ухвалення акціонерними товариства відповідних внутрішніх документів, направлених на забезпечення потреб акціонерів, потенційних інвесторів і інших зацікавлених осіб щодо доступу до достовірної інформації про акціонерне товариство та його діяльність. В цих рекомендаціях проголошуються принципи прозорості, регулярності, оперативності і доступності в отриманні тієї або іншої інформації вище перерахованим суб'єктам корпоративних відносин.

3. МАЙНОВІ ІНТЕРЕСИ ТА ПРАВА УЧАСНИКІВ КОРПОРАТИВНОГО ПІДПРИЄМНИЦТВА ЯК ДЖЕРЕЛО ВИНИКНЕННЯ СУПЕРЕЧОК ТА КОНФЛІКТІВ

Інтереси господарського товариства захищаються в суді не окремим акціонером, особисті інтереси якого можуть суперечити інтересам товариства в

цілому. Акціонер може захищати свої права або законні інтереси, шляхом звернення до суду, у випадках їх порушення. Розмежування майнових інтересів окремих акціонерів від майнових інтересів господарського товариства, як юридичної особи, сприяє більш детальному розгляду корпоративних суперечок, що виникають на цьому ґрунті. І одним з основних питань, які підіймаються міноритарними акціонерами, це участь в розподілі прибутку і отримання дивідендів за підсумками роботи господарського товариства. Як правило, власники великих пакетів акцій, не є зацікавленими особами виплати дивідендів міноритарним акціонерам, що у свою чергу є грубим порушенням у сфері корпоративних правовідносин і суперечить самому поняттю корпоративного права. Проте реалії сьогоднішнього дня дозволяють провести паралель між задекларованими в законодавчому порядку правами, і фактичним застосуванням чинного законодавства. Невиплата дивідендів носить масовий характер і завуальована штучною збитковістю підприємства. Існує і другий варіант, пов'язаний з істотною необхідністю збільшення капіталовкладень. І як наслідок виплата дивідендів представляється як недоцільною і є нічим іншим, як вилученням оборотних коштів. Виплата дивідендів за своєю суттю є обов'язком товариства щодо своїх акціонерів або засновників. Відповідно до рекомендацій Державної комісії з цінних паперів і фондового ринку, рішення про виплату дивідендів повинно оформлятися протоколом із наступним змістом вимог:

- розмір дивідендів, що припадає на одну акцію;
- терміни виплати дивідендів;
- терміни прийому заяв акціонерів у разі їх згоди на внесення нарахованих сум на збільшення статутного фонду;
- спосіб виплати дивідендів;
- порядок виплати дивідендів.

Підводячи підсумок вище викладеному, можна з повною упевненістю констатувати, що численні випадки невиплати дивідендів згідно рішень, за якими стоять власники великих пакетів акцій, служать інтересам мажоритарних акціонерів, і в деякій мірі, стають предметом зловживань з їх сторони. Адже господарські товариства, зокрема акціонерні, створюються з метою отримання прибутку на користь усіх акціонерів товариства. Також, однією з головних цілей створення суб'єкту господарювання, є підвищення добробуту акціонерів у вигляді збільшення ринкової вартості акцій створеного ними товариства. Але, як ми бачимо, теорія часто розходиться з практикою, і права міноритарних акціонерів стають не захищеними, тому на цій основі виникає чимало майнових суперечок та конфліктів.

4. КОРПОРАТИВНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ НОРМ ЧИННОГО ЗАКОНОДАВСТВА

Законодавче регулювання відносин між членами товариств передбачає

моделювання в нормативних актах бажаної поведінки суб'єктів правовідносин і встановлення санкцій, що передбачають відповідальність, за порушення цих правовідносин. По своїй суті, певна кількість цих санкцій має характер юридичної відповідальності, яка реалізується за допомогою заходів державного примусу і полягає в покладанні на правопорушника додаткових обов'язків, яких до цього у нього не було. Ці ж санкції полягають в позбавленні його певних прав.

Комплексний характер корпоративних правовідносин, де пов'язані як публічні, так і приватні інтереси, що вимагають правового захисту, обумовлений тим, що за здійснення правопорушень у сфері корпоративних правовідносин особа може бути притягнута до різних видів відповідальності – починаючи від адміністративної, і закінчуючи кримінальною.

Яскравим прикладом може послужити стаття 223 Кримінального кодексу України, в якій передбачається відповідальність за порушення порядку випуску (емісії) і обігу цінних паперів. Предметом даного злочину є:

- цінні папери, випуск яких може здійснюватися у формі відкритого розміщення за умови реєстрації випуску уповноваженими державними органами;
- документи, представлені для реєстрації емісії цінних паперів.

Суб'єктом злочину згідно чинного законодавства може бути громадянин або посадовець суб'єкта господарювання. Співучасниками, окрім посадовців, виступають відповідні працівники юридичних осіб, що здійснюють комерційні операції з цінними паперами, а також працівники юридичної особи, яка веде реєстр власників цінних паперів. Це у тому випадку, якщо вони внесли в реєстр дані про власників цінних паперів, розуміючи, що ці цінні папери випущені без належної реєстрації.

Таким чином, громадянин може бути суб'єктом цього злочину, якщо він, зокрема, є засновником або акціонером господарського товариства.

Кодексом України про адміністративні правопорушення, передбачена відповідальність за порушення вимог законодавства з емісії цінних паперів (ст.163). Залучення до відповідальності посадовців товариства, які знаходяться з ним в трудових відносинах, можливе у формі дисциплінарної або матеріальної відповідальності, а також відшкодування збитків, заподіяних учаснику неправомірними рішеннями органів товариства, здійснюється через притягнення до цивільної відповідальності. Весь масив санкцій, які застосовуються за порушення правових норм, що регламентують порядок створення, діяльності, ліквідацію юридичних осіб, їх взаємостосунки з учасниками (членами) і учасників (членів) між собою, поєднані в межах одного загального поняття – відповідальність за правопорушення у сфері корпоративних правовідносин. Підставою корпоративної відповідальності є порушення норм права, які можуть бути встановлені як в загальних, так і в корпоративних правових актах. Також корпоративна відповідальність полягає в позбавленні правопорушника певного права або покладанні на нього додаткових обов'язків.

Отже, корпоративна відповідальність є санкцією, що вживається в межах

корпоративних правовідносин юридичної особи до її учасників або учасниками до юридичної особи за порушення корпоративних обов'язків. Майнова і дисциплінарна відповідальність працівників (у тому числі посадовців товариства) застосовується виключно в межах трудових правовідносин, єдиною підставою виникнення яких є трудові правовідносини. Не можна притягати до дисциплінарної або матеріальної відповідальності учасника товариства, якщо він не знаходиться з останнім в трудових відносинах. Так само не можна притягнути до корпоративної відповідальності найманого працівника товариства, якщо він не є його учасником.

Підсумовуючи вище викладене, слід також зазначити, що основи корпоративних правовідносин, що регламентують відносини між учасниками товариства і самим товариством, в чинному законодавстві зосереджені в ЦК України. Норми, що стосуються корпоративної відповідальності, закріплені також в ньому. Таким чином, корпоративна відповідальність, є різновидом цивільної відповідальності. І спірні питання, в основній масі, повинні розглядатися цивільними судами.

Тема 10. ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ РОБОТИ СЛУЖБИ БЕЗПЕКИ ФІРМИ (ПІДПРИЄМСТВА, ОРГАНІЗАЦІЇ, УСТАНОВИ) ТА ДІЛОВА (КОРПОРАТИВНА) РОЗВІДКА

1. СЛУЖБА БЕЗПЕКИ ЯК ПІДСИСТЕМА ПІДПРИЄМСТВА (ОРГАНІЗАЦІЇ): СТРУКТУРА, ОСОБЛИВОСТІ УПРАВЛІННЯ ЇЇ ДІЯЛЬНІСТЮ ТА ЗАБЕЗПЕЧЕННЯ ПРАЦІВНИКАМИ.

Завдання гарантування безпеки підприємства є одним із основних, пріоритетних завдань, що стоять перед усіма структурними ланками і всіма працівниками підприємства, так само як і завдання збільшення прибутку, підвищення власного добробуту. Ефективний захист економічних інтересів фірми може бути забезпечений лише у разі об'єднання зусиль її персоналу: адміністрації, інженерно-технічних працівників, службовців, робітників.

Служба безпеки (СБ) фірми - це самостійний структурний підрозділ. Вона вирішує завдання безпосереднього забезпечення захисту життєво важливих інтересів фірми в умовах комерційного і підприємницького ризику, конкурентної боротьби. На всіх великих і середніх підприємствах (в організаціях) звичайно створюються автономні служби безпеки, а безпеку функціонування невеликих фірм можуть гарантувати територіальні (районні або міські) служби за договорами найму одного чи кількох охоронців. Такі служби охорони зазвичай створюються при місцевих органах внутрішніх справ або при державній службі безпеки.

Підприємство як система має певні структурні ланки:

- дирекцію - керівництво підприємства;
- бухгалтерію;
- відділи - функціональні ланки підприємства;
- допоміжні служби;
- службу безпеки (СБ).

Система діяльності підприємства організаційно складається з таких частин, як:

- організаційно-управлінська діяльність;
- фінансова;
- комерційна або інша основна діяльність підприємства;
- кадрова;
- із гарантування власної безпеки.

Кожна структурна ланка має свої функціональні обов'язки і вирішує своє конкретне завдання. Водночас кожна структурна ланка і кожен співробітник працюють для досягнення загальної мети: підвищення добробуту підприємства, збільшення його прибутку. Від того, як буде реалізована ця мета, залежатиме їх

особисте благополуччя, їх особистий прибуток.

Служба безпеки як відділ підприємства вирішує завдання:

- організації захисту економічних інтересів на підприємстві;
- гарантування безпеки спеціальними засобами і методами. Виконуючи організаційну функцію, служба безпеки працює у взаємодії з дирекцією і відділами (функціональними ланками) підприємства.

Служба безпеки спільно з дирекцією забезпечує:

- ухвалення правильних управлінських рішень (забезпечує керівництво інформацією, веде аналітичну роботу);
- управління системою безпеки (консультує керівництво з питань захисту економічних інтересів);
- створення режиму збереження комерційної таємниці (розробляє правила, що забезпечують його дотримання);
- надання допомоги і здійснення контролю за діяльністю всіх функціональних ланок підприємства.

Служба безпеки спільно з відділами забезпечує:

- здійснення комерційних операцій (бере участь у підготовці контрактів, перевіряє надійність партнерів, відстежує виконання взятих ними зобов'язань);
- підбір, перевірку і підготовку персоналу;
- навчання персоналу прийомів поведінки і правил спілкування, формування загальної і особистої зацікавленості, створення на підприємстві обстановки пильності.

Служба безпеки самостійно працює спеціальними засобами і методами:

- у середовищі працівників підприємства;
- у середовищі партнерів і конкурентів підприємства.

Отже, в підприємницькій діяльності гарантування безпеки - цілісне явище, що має свою чітку структуру й систему. Перед нею стоїть конкретна мета, якої досягають вирішенням управлінських і специфічних завдань.

Діяльність із гарантування безпеки на підприємстві спрямована на конкретні об'єкти і здійснюється особливими засобами і методами. Вона тісно пов'язана з діяльністю всіх функціональних ланок підприємства і має здійснюватися комплексно. Будучи підсистемою організації, ця діяльність має здійснюватися з позицій сучасного менеджменту - науки, практики і мистецтва управління виробництвом, послугами, збутом, персоналом відповідно до умов ринкової економіки, демократичних і економічних свобод.

Організація як самокерована система, з одного боку, є елементом загального ринкового організму, з другого - самостійною спільністю із специфічним внутрішнім середовищем, здатним в умовах конкуренції до ефективної діяльності і розвитку. Тому системний підхід тут особливо важливий. Саме система здатна швидко реагувати на зміни, їх відпрацювання, аналіз, вибір альтернативних рішень щодо виниклих нестандартних ситуативних проблем або завдань.

Основною метою підсистеми безпеки фірми є запобігання: збитку в її

діяльності за рахунок розголошення, просочування інформації та несанкціонованого доступу до джерел конфіденційної інформації; розкраданню фінансових і матеріально-технічних коштів, знищенню майна і цінностей; порушенню роботи технічних засобів забезпечення виробничої діяльності, зокрема засобів інформатизації, а також запобігання збитку персоналу організації. Завданнями підсистеми безпеки фірми є:

- своєчасне виявлення й усунення загроз персоналу і ресурсам; причин і умов виникнення фінансового, матеріального і морального збитку інтересам фірми, порушення її нормального функціонування і розвитку;
- віднесення інформації до категорії обмеженого доступу (службової і комерційної таємниць, іншої конфіденційної інформації, належного захисту від неправомірного використання), а інших ресурсів - до різних рівнів уразливості (небезпеки) і до категорії тих, що підлягають збереженню;
- створення механізму і умов оперативного реагування на загрози безпеки і прояви негативних тенденцій у функціонуванні фірми;
- ефективне припинення посягань на ресурси і загроз персоналу на основі комплексного підходу до безпеки;
- створення умов для максимально можливого відшкодування й локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб, для ослаблення негативного впливу наслідків порушення безпеки на досягнення стратегічної мети.

Організаційна структура підсистеми безпеки організації може бути різною залежно від виду підприємства (банк, фірма), його розмірів, форм власності тощо. Створювати її слід усвідомлено й раціонально, максимально використовуючи досвід фахівців у сфері безпеки бізнесу.

Структура, чисельність і склад служби безпеки визначаються реальними потребами фірми і ступенем конфіденційності її інформації. Залежно від розмірів і потужності організації її безпека і захист інформації можуть бути гарантовані по-різному: від абонементного обслуговування силами приватних охоронних і детективних структур до розгортання повномасштабної власної служби і системи безпеки з розвиненою структурою і штатною чисельністю

У своїй діяльності служба безпеки керується:

- інструкцією з організації режиму і охорони;
- інструкцією щодо захисту комерційної таємниці;
- переліком відомостей, що становлять комерційну таємницю;
- інструкцією щодо роботи з конфіденційною інформацією для керівників, фахівців і технічного персоналу;
- інструкцією щодо організації зберігання справ, що містять конфіденційну інформацію, в архіві;
- інструкцією щодо інженерно-технічного захисту інформації;
- інструкцією про порядок роботи з іноземними представниками і представництвами та ін.

Служба безпеки фірми завжди має бути готовою до подолання критичної (кризової) ситуації, що може виникнути через зіткнення інтересів бізнесу та злочинного світу. Для управління безпекою багато які фірми створюють так звані кризові групи, у складі яких працюють керівник фірми, юрист, фінансист і керівник служби безпеки. Головна мета діяльності кризової групи - протидіяти зовнішнім загрозам для безпеки фірми.

Служба безпеки будь-якої фірми постійно виконує певний комплекс завдань. Головними з них для будь-якої фірми є такі:

1) гарантування безпеки виробничо-господарської діяльності та захисту відомостей, що вважаються комерційною таємницею фірми (підприємства, організації);

2) організація роботи з правового та інженерно-технічного захисту комерційної таємниці фірми;

3) запобігання необґрунтованому допуску й доступу до відомостей та робіт, які становлять комерційну таємницю;

4) організація спеціального діловодства, яке унеможливлює несанкціоноване одержання відомостей, віднесених до комерційної таємниці відповідної фірми;

5) виявлення і локалізація можливих каналів витоку конфіденційної інформації в процесі звичайної діяльності та в екстремальних ситуаціях;

6) забезпечення режиму безпеки за здійснення всіх видів діяльності, зокрема зустрічі, переговори й наради у рамках ділової співпраці фірми з іншими партнерами;

7) забезпечення охорони приміщень, устаткування, офісів, продукції і технічних засобів, необхідних для виробничої або іншої діяльності;

8) забезпечення особистої безпеки керівництва та провідних менеджерів і спеціалістів фірми;

9) оцінка маркетингових ситуацій та неправомірних дій конкурентів і зловмисників.

Зрозуміло, що перелік конкретних завдань щодо гарантування безпеки фірми залежно від специфіки її діяльності може бути більшим або меншим, але завжди достатнім та обґрунтованим.

На великих і середніх підприємствах, як правило, створюються автономні служби безпеки, а безпека функціонування невеликих фірм може забезпечуватися територіальними (районними або міськими) службами, що в них фірма наймає одного чи кількох охоронців. Такі служби охорони, як правило, створюються при місцевих органах внутрішніх справ або при державній службі безпеки.

Роль окремих служб та відділів у процесі забезпечення економічної безпеки підприємства наведено в таблиці 10.1.

Таблиця 10.1

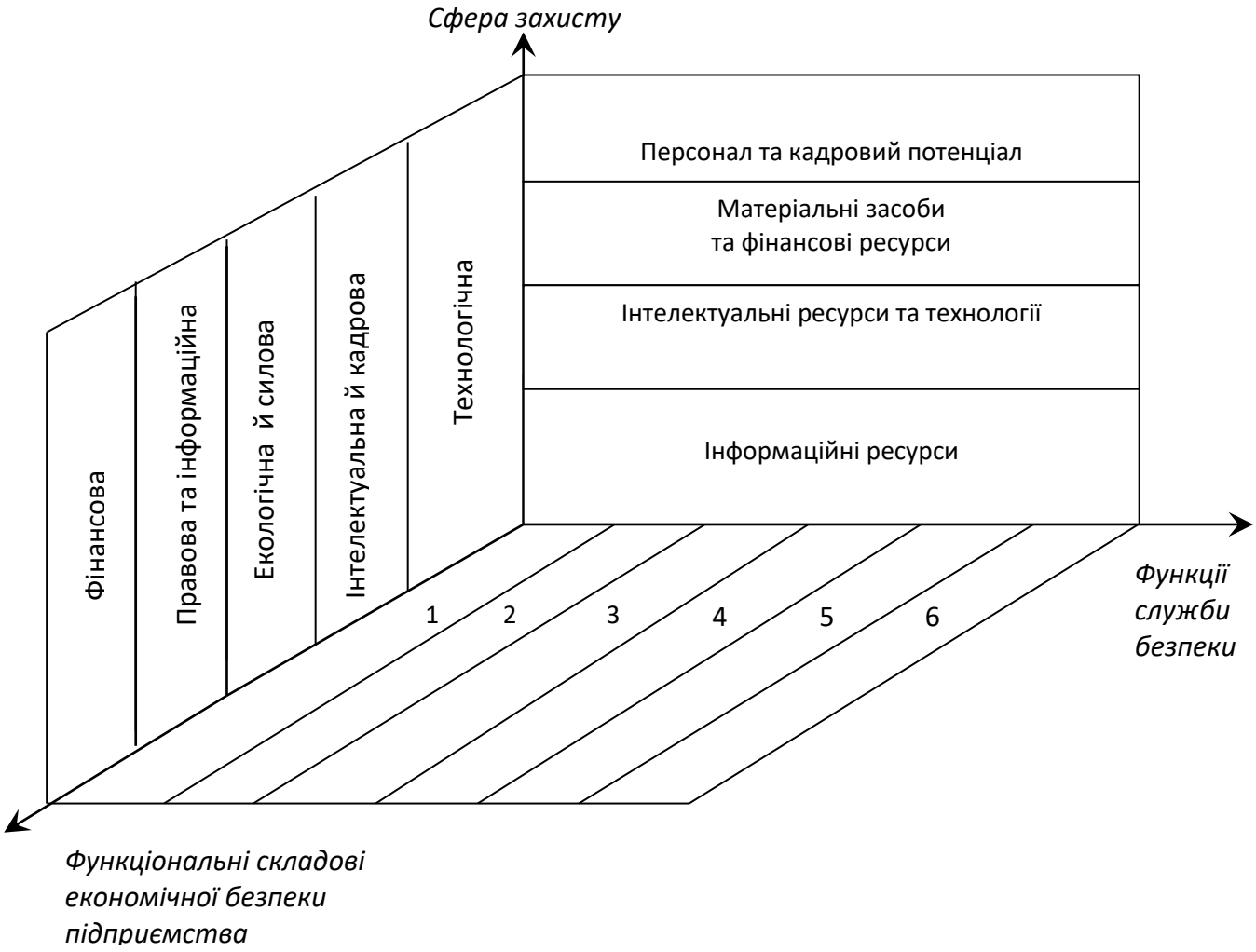
Роль окремих служб та відділів у процесі забезпечення економічної безпеки підприємства

Вид діяльності	Напрям діяльності	Підрозділ фірми
Забезпечення фізичної і моральної безпеки співробітників підприємства	✓ Охорона співробітників ✓ Збирання інформації та превентивні дії для запобігання загрози їхньої безпеки ✓ Розробка заходів щодо усунення можливих загроз	• Служба безпеки • Інформаційно-аналітичний підрозділ • Конкурентна розвідка
Гарантування безпеки майна та капіталу підприємства	✓ Охорона майна (будівель, споруд, устаткування, транспорту) ✓ Охорона перевезень ✓ Страхування майна та ризиків ✓ Організація безпеки інвестиційних процесів	• Служба безпеки • Фінансова служба • Економічний підрозділ
Безпека інформаційного середовища	✓ Захист від промислового шпіонажу ✓ Збирання інформації про зовнішнє середовище бізнесу ✓ Збирання інформації про діяльність конкурентів	• Служба безпеки • Інформаційно-аналітичні підрозділи • Служба конкурентної розвідки
Забезпечення сприятливого зовнішнього середовища	✓ Превентивні дії для запобіганням загрозам ✓ Робота з громадськістю та пресою ✓ Політика лобіювання інтересів підприємства в урядових колах	• Вище керівництво фірми • Служба зв'язків з громадськістю • Служба безпеки

Пріоритетним принципом організації та функціонування системи безпеки підприємства є її комплексність, яку можна зобразити у вигляді тривимірної моделі (рис. 10.1).

Ключові завдання системи безпеки підприємства наведено на рис. 10.2.

Загальні функції служби безпеки підприємства відображено на рис. 10.3.



1 – Охорона майна підприємства та його фінансових ресурсів; 2 – Контроль дотримання режиму; 3 – Охорона кадрових ресурсів; 4 – Охорона важливих документів та процесу документообігу; 5 – Інженерно-технічний захист; 6 – Інформаційно-аналітична діяльність.

Рис. 10.1 – Тривимірна модель комплексної системи безпеки фірми (підприємства, організації)

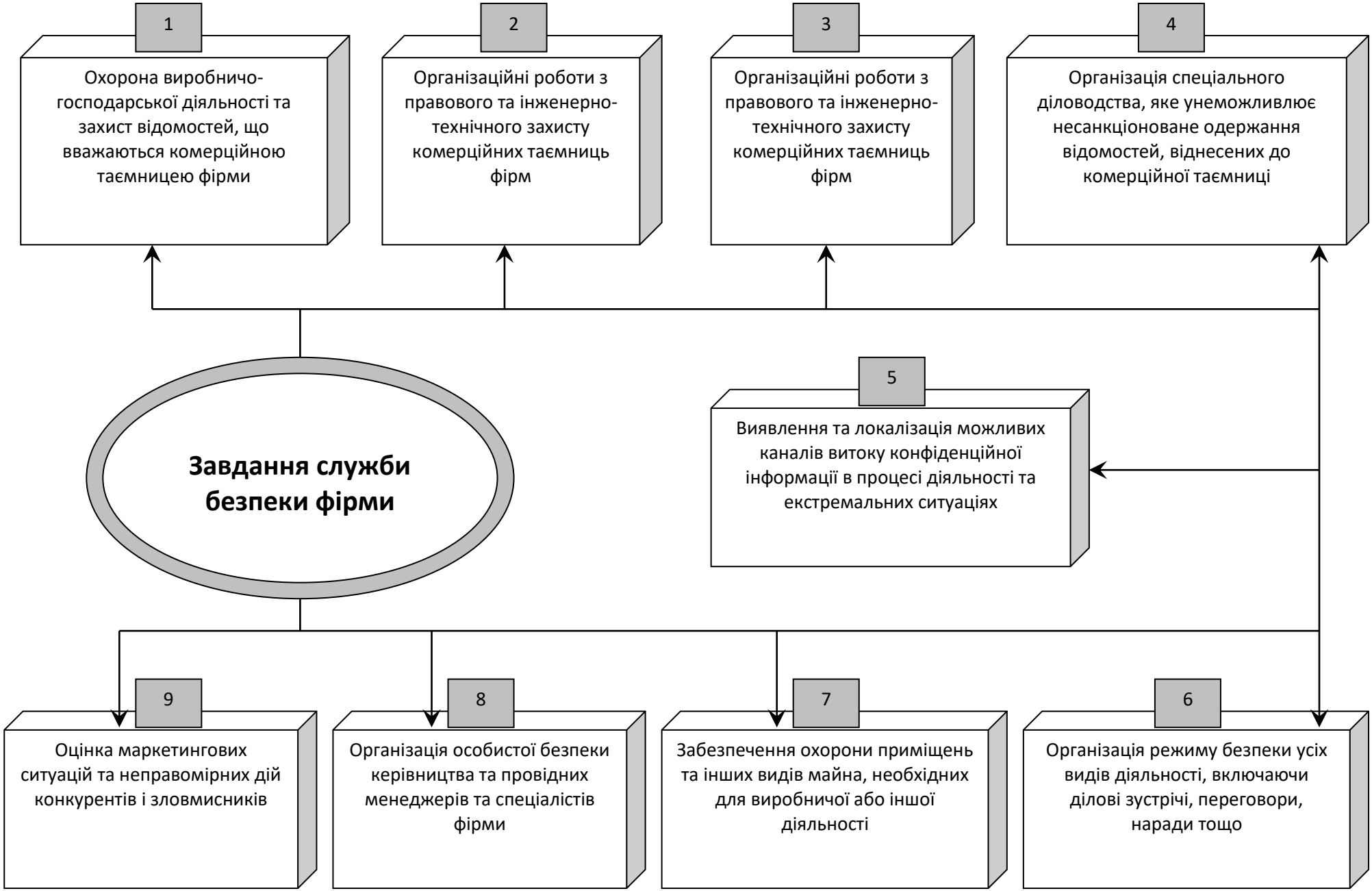


Рисунок 10.2 – Основні завдання служби безпеки фірми (підприємства, організації)

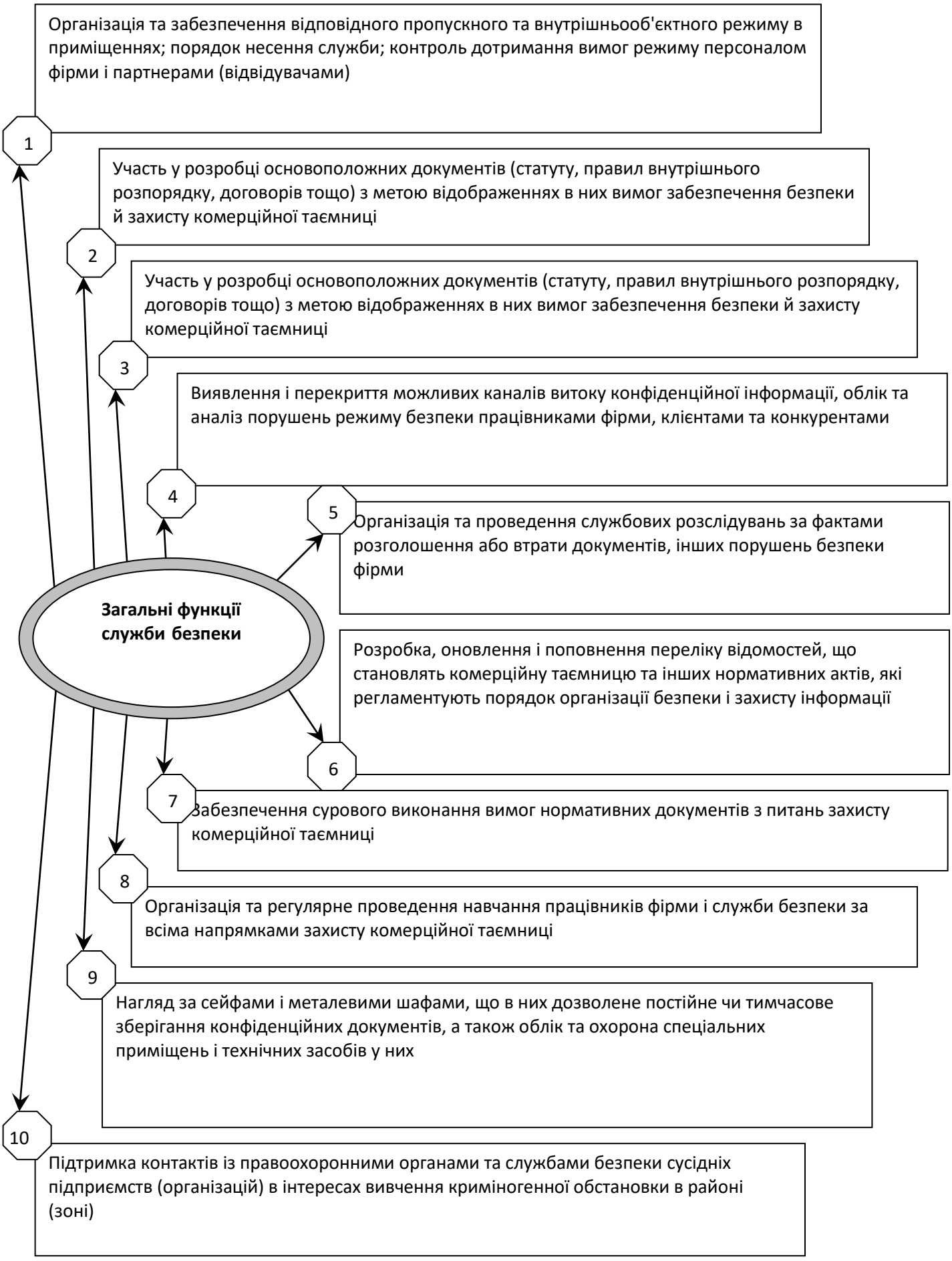


Рис. 10.3 – Типові функції служби безпеки підприємства

Управління безпекою підприємства

Очолює службу безпеки начальник служби на посаді заступника керівника фірми з безпеки.

Органами управління безпекою великого підприємства є:

- дирекція фірми - вищий орган управління;
- правління служби безпеки - виконавчий орган.

До складу правління зазвичай входять начальник служби безпеки, заступник начальника служби безпеки, секретар-інспектор.

Начальник служби безпеки є безпосереднім керівником персоналу служби безпеки. Він підпорядковується директорові підприємства або одному із його заступників відповідно до штатного розпису. Начальник служби безпеки здійснює керівництво діяльністю служби безпеки, вирішує всі організаційні питання, пов'язані з діяльністю служби безпеки, крім тих, що стосуються виключної компетенції дирекції підприємства.

Начальника служби безпеки призначає дирекція підприємства з осіб, що мають вищу освіту. Директор фірми укладає з ним трудовий договір, у якому обумовлено всі посадові обов'язки та умови праці.

Начальник служби безпеки без додаткового доручення діє від імені служби безпеки у всій своїй діяльності, має право підпису всіх правових і бухгалтерських документів служби безпеки, визначає посадові оклади її працівників, вирішує питання щодо надання чи позбавлення премій, інших видів заохочення та мотивування, укладає трудові договори із працівниками служби безпеки тощо.

На час відпустки чи відрядження начальник служби безпеки делегує свої права заступникові.

Начальник служби безпеки відповідає за:

- надання охоронних і пошукових послуг з метою безпеки фірми і суворого дотримання чинного законодавства України;
- забезпечення збереженості спеціальних засобів, зброї, боєприпасів, що придбані підприємством;
- якість професійної підготовки осіб зі складу служби безпеки.

Начальнику служби безпеки не дозволяється суміщати охоронну діяльність із державною службою чи виборною оплачуваною посадою в громадських об'єднаннях, а також надавати послуги особисто чи через своїх підлеглих, що пов'язані із забезпеченням безпеки інших підприємств.

Підбираючи начальника служби безпеки, ставлять насамперед два питання, що стосуються його професіоналізму і лояльності. Відповідно до виконуваних ним функцій він має знати не просто дані про підприємство, а всі проблемні аспекти його роботи, весь негатив, а деколи й дуже багато про особисте життя керівництва фірми. Тому підбір особи на таку посаду має бути дуже чітким і обдуманим.

Поширеним є твердження, що необхідну кандидатуру треба шукати тільки серед своїх і тільки серед колишніх працівників органів. Це значно звужує і так вузьке коло претендентів. Щодо пошуку "серед своїх" можна

погодитися з тим, що особа з рекомендаціями хорошого знайомого матиме набагато більшу довіру, ніж стороння кандидатура. Проте свої, а тим більше родичі, через дружні стосунки з керівником впевнені в тому, що в них не виникне проблем, тому до роботи серйозно не ставляться, і впливати на них складніше через те, що вони "свої"'.

Те, що потрібно шукати кандидатуру серед колишніх працівників силових структур, також потребує уточнення. Як правило, такі фахівці, що пропрацювали в органах тривалий час, є професіоналами, але тільки у вузькій спеціальності. А керівник служби безпеки має знати набагато більше. Крім того, професіоналів органи не відпускають - за ними стежать, їх можуть у будь-який момент залучити до співпраці. Ще один аспект - тривала робота у відповідних структурах накладає відбиток на стиль життя і поведінки цієї особи, що не завжди є позитивним.

При підборі кандидата на посаду начальника служби безпеки слід чітко визначити пріоритети його роботи. Такими пріоритетами можуть бути загрози з боку конкурентів, боротьба з шахрайством персоналу, протидія кримінальним угрупованням чи нейтралізація дії силових структур. Залежно від цього і потрібно шукати спеціаліста. Якщо головна проблема - силові структури, кращим буде працівник з керівної посади в цих структурах з відповідними налагодженими зв'язками. Якщо кримінал, то працівник має досвід роботи з ним і досвід створення відповідних систем безпеки. Якщо конкуренти, важливим є досвід збору інформації та аналізу економіки підприємства.

Процес управління

У найзагальнішому вигляді цей процес складається з трьох стадій, кожна з яких охоплює послідовно здійснювані етапи або операції:

I стадія: збирання, оброблення, узагальнення та аналіз інформації;

II стадія: вироблення і ухвалення управлінського рішення;

III стадія: організація виконання управлінського рішення.

Зрозуміло, що така структура процесу управління не є загальноприйнятою, яку слід копіювати в управлінні діяльністю служби безпеки.

Відповідно до специфіки діяльності служби безпеки та її зовнішнього оточення слід (у межах зазначеної структури) виробляти свій підхід до процесу управління. Наведемо варіант структури процесу управління:

I. Оцінка обстановки.

1. Преамбула.

2. Формулювання обмежень і критеріїв ухвалення рішення.

3. Формування набору альтернативних вирішень проблеми.

4. Оцінка альтернатив.

II. Оцінка конкуруючих сил на ринку послуг (виробництві) - злочинних елементів (груп) у регіоні (зоні) дислокації фірми.

III. Оцінка своїх сил.

5. Технічне забезпечення захисту фірми.

6. Фізичне забезпечення захисту.

7. Якісна характеристика працівників служби безпеки.

IV. Оцінка фірм, що співпрацюють і взаємодіють на ринку послуг.

V. Організація взаємодії постів і порядок їх посилення за різних режимів діяльності.

VI. Організація зв'язку між постами для забезпечення взаємодії.

VII. Організація взаємодії з органами МВС.

VIII. Дія сил і засобів служби безпеки при порушенні режимів захисту.

IX. Забезпечення охорони провідних фахівців фірми, їх сімей і власності.

Таким чином, раціональне впровадження в практику основних елементів системи, механізму і процесу управління дає змогу керівництву служби безпеки значно підвищити ефективність управлінської дії на результати її діяльності.

Багатогранність сфери гарантування безпеки фірми, зокрема захист її комерційної таємниці, вимагає створення спеціальної служби для реалізації всіх захисних заходів.

Структура, чисельність і склад служби безпеки фірми визначаються реальними фінансовими можливостями, масштабом комерційної діяльності, ступенем конфіденційності інформації. Залежно від цих чинників служба безпеки може налічувати від 2-3 осіб, що працюють за сумісництвом, до чисельності працівників повномасштабної служби з розвиненою структурою.

Принциповим питанням, яке доводиться вирішувати кожній фірмі, є питання комплектування служби охорони висококваліфікованими і надійними кадрами. Зарубіжний і вітчизняний досвід гарантування безпеки підприємницької діяльності підтверджують, що переважним є варіант створення банком, фірмою, організацією свого відділення, що забезпечує його безпеку.

Одні фірми категорично відмовляються наймати охоронців за контрактом. Інші такого ж розміру і з такою ж чисельністю персоналу, навпаки, використовують тільки охоронців-контрактників. На практиці проблема забезпечення корпоративної безпеки вирішується за однією з таких схем:

- зведення завдань служби безпеки тільки до охоронних функцій із залученням для їх виконання приватних охоронних структур;
- доручення виконувати охоронні функції приватним охоронним підприємствам, а вирішувати внутрішні питання - власним експертам під керівництвом менеджера з безпеки;
- покладання виконання всіх функцій на власну службу.

При використанні першого варіанта перед укладанням угоди з приватними охоронними структурами слід вивчити імідж таких фірм з огляду на час діяльності, коло клієнтів, професійний рівень, надійність, кадровий склад, фінансове становище та ін.

Другий варіант більш привабливий, але при його використанні ускладнюється контроль надійності охоронців і використання їх для вирішення оперативних завдань.

Третій варіант найбільш дорогий і потребує багато зусиль, оскільки вимагає обов'язкового ліцензування охоронців, створення власної збройової

кімнати, придбання зброї тощо.

Основними якостями і властивостями професійного менеджера, на думку іноземних фахівців, є здатність:

- керувати собою в будь-яких умовах і ситуаціях;
- постійно працювати над своїм професійним зростанням, загальною інтелігентністю і культурою;
- розвивати навички прогнозування, аналізу, запобігання проблемам і труднощам або вирішення їх;
- розвивати здатність впливати на людей залежно від їх становища, віку та інших факторів;
- постійно освоювати сучасні підходи і методи технології менеджменту, знаходити і розробляти нові відповідно до умов України і того середовища, в якому діє фірма;
- розвивати здатність ефективно використовувати на демократичному рівні та за існуючого права владні повноваження, прагнути від формального до неформального лідерства;
- уміти переконувати і навчати людей, мотивувати їх ефективну творчу діяльність та ініціативу;
- уміти формувати й ефективно працювати з групами і колективами на рівні як формального, так і неформального лідера;
- постійно прагнути до творчості і нововведень, вчити цього своїх підлеглих і колег по роботі.

Режим робочого часу у менеджера безпеки напружений і, як правило, не обмежений. Тому і винагорода (зарплата, премії та ін.) у нього зазвичай вищі, ніж в інших фахівців компанії.

Експерти погоджуються з тим, що навіть один охоронець здатен уберегти клієнта від безлічі неприємностей, якщо він професіонал. Правда, у випадках, коли за бізнесменом починають планомірно полювати інші професіонали, його шанси залишитися живим різко знижуються. Проте надійно "закрити" від убивць можна в принципі будь-якого клієнта. Але для цього потрібна ціла команда добре підготовлених фахівців, систематична оперативна робота, першокласні технічні засоби, тобто великі гроші. Мало кому по кишені мати "особисту гвардію" з 10-20 осіб. Більшість підприємців у країнах СНД і Східної Європи утримують не більше двох-трьох охоронців.

2. *ПРОЦЕДУРА СТВОРЕННЯ І ЛІКВІДАЦІЇ СЛУЖБИ БЕЗПЕКИ ПІДПРИЄМСТВА.*

Для створення служби безпеки керівництво і менеджери насамперед розпочати створення її системи безпеки, визначити структурні варіанти ii перспективи її розвитку. Але передусім треба визначити можливості:

- використання служб охорони за контрактом;
- створення власної служби безпеки;

- залучення допомоги державних служб охорони;
- протидії загрозам з боку терористів;
- протидії загрозам вибухів, комп'ютерним злочинам;
- протидії "білокомірцевій" злочинності;
- використання спецтехніки (відео - та інших оперативних систем охорони різних суб'єктів і об'єктів, спеціальних технічних засобів охорони периметра об'єкта, систем охоронного устаткування і центрального управління і т.ін.)

Вирішити створити власну службу безпеки, підприємець передусім повинен звернутися до експертів у галузі організації сучасної системи безпеки недержавного підприємства з проханням провести дослідження цієї проблеми і підготувати пакет документів, що визначають програму і функціонування системи безпеки підприємства. Краще за все це можуть зробити професійно підготовлені менеджери безпеки.

Чому потрібно створювати систему безпеки навіть у малому й середньому бізнесі, зрозуміли вже багато підприємців. В умовах сучасної України для господарюючого суб'єкта існують такі основні джерела загроз, небезпек, втрат, конфліктів і ризиків:

- розкрадання (крадіжки) фондів, власності, дрібні крадіжки, що здійснюються співробітниками;
- "білокомірцева" злочинність, корупція;
- комп'ютерна злочинність, загрози технічного проникнення і просочування електронної інформації;
- вандалізм, вибухи, пожежі, підпали;
- викрадення, захоплення заручників, рекет, загрози шантажу;
- загрози природного походження (катаклізми);
- масові безпорядки.

У процесі організації комплексної системи безпеки господарюючого об'єкта особливу увагу слід звертати на такі елементи:

- здатність розробити програму, адекватну специфічним потребам захисту об'єкта;
- ступінь надійності працівників підприємства;
- вартість програми захисту об'єкта;
- ступінь надійності захисту об'єкта;
- достатня ефективність витрат на програму діяльності;
- рівень загальної відповідальності адміністрації;
- здатність програм гарантування безпеки відповідати вимогам;
- страхові премії як результат виконання програми;
- здатність модернізувати систему безпеки відповідно до сучасних вимог;
- здатність прищепити працівниками підприємства відчуття корпоративності;
- надійність виробника спеціального обладнання, яке використовується для захисту об'єкта;

- засоби впливу на громадську думку на користь вирішення проблем безпеки об'єкта.

Для ефективного функціонування служби безпеки потрібно попередньо опрацювати багато питань. Серед них особливе значення має проектування оргструктури служби безпеки та її ресурсного забезпечення, оскільки без вирішення цих питань її діяльність взагалі неможлива.

Серед причин нерівномірні кількості працівників у різних підрозділах служби безпеки можна назвати фінансові можливості підприємства-засновника, наявність або відсутність таємниць, що охороняються, ступінь участі у конкурентній боротьбі і т.ін. Кожен підрозділ служби безпеки має свої специфічні цілі, завдання і функції, реалізація яких (оскільки вони взаємно доповнюють одне одного) дає змогу значно підвищити ефективність служби безпеки в цілому.

В організаційній структурі передбачена також посада керівника служби безпеки, яка на практиці трансформувалася в начальника служби безпеки. Очевидно, що коли персонал служби безпеки за чисельністю великий, неминуче виникає питання щодо заступників начальника служби безпеки. їх також має бути не менше трьох - за кількістю підрозділів служби безпеки.

Будь-яка оргструктура, навіть най оптимальніша, не зможе дати очікуваних результатів, якщо її не доповнити внутрішніми нормативними актами, що регулюють діяльність усіх підрозділів і співробітників служби безпеки. Образно кажучи, "кістка" (оргструктура) має обрости "м'ясом" (нормативними документами). Причому ці нормативні акти умовно можна поділити на дві групи: 1) ті, що безпосередньо стосуються діяльності самої служби безпеки; 2) ті, що регулюють діяльність інших служб (підрозділів, працівників) підприємства. До першої групи належать: статут служби безпеки, положення про відділи і штаб служби безпеки, положення про групи і сектори служби безпеки, посадові інструкції працівників служби безпеки.

Структура посадової інструкції має такі розділи: загальні положення; функції; посадові обов'язки; відповідальність; взаємини і зв'язки за посадою. Розробляють ці нормативні акти послідовно, починаючи із статуту до посадової інструкції, що дає змогу охопити весь комплекс цілей, завдань і функцій, що вирішуються службою безпеки.

До другої групи внутрішніх нормативних актів, що забезпечують діяльність інших працівників і служб підрозділів підприємства-засновника, належать:

- договір підприємства з партнером про забезпечення ним заходів безпеки комерційної інформації;
- інструкція щодо виконавців робіт і документів, що містять комерційну таємницю;
- зобов'язання про нерозголошення комерційної таємниці;
- перелік відомостей, що становлять комерційну таємницю підприємства і основні вимоги до працівників з її захисту;
- перелік відомостей, які не повинні розголошуватися стороннім особам

з метою особистої безпеки працівників підприємства;
- перелік посадових осіб, уповноважених відносити інформацію до комерційної таємниці;
- правила віднесення інформації до комерційної таємниці і зняття з її носіїв грифу конфіденційності;
- правила ведення таємного діловодства;
- пам'ятка працівникові (службовцеві) про збереження комерційної таємниці підприємства;
- правила приймання відвідувачів на підприємстві;
- правила внутрішнього трудового розпорядку і т.ін.

Проте оптимальна оргструктура і повне правове забезпечення служби безпеки самі по собі не забезпечать п ефективного функціонування, якщо вона не матиме відповідних ресурсів. Продовжуючи образні порівняння, можна стверджувати, що після того, як "кістка" (оргструктура) обросла "м'ясом" (внутрішні нормативні документи), слід поклопотатися про "їжу" (ресурси). Серед них першочергове значення мають фінансові ресурси. Без фінансового забезпечення діяльності служби безпеки безглуздо взагалі говорити про її функціонування.

Не менше значення для керівників служби безпеки має кадрове забезпечення її діяльності. Роботу цю умовно можна поділити на два етапи. На першому етапі відбирають кандидатів для роботи в службі безпеки, перевіряють їх, кандидати проходять спеціальну підготовку і стажування на посаді. При їх відборі особливу увагу приділяють освіті (крім юристів, доцільно запрошувати на роботу також економістів, фінансистів). Крім перевірки органами внутрішніх справ, не зашкодить з'ясувати біографічні та інші дані про кандидата. Зрозуміло, це треба робити не завжди (зайвою буде така перевірка, наприклад, кандидата, якого добре і давно знає керівник служби безпеки) і з письмової згоди кандидатів. Проте письмову згоду на таку перевірку після зарахування кандидата на роботу в службі безпеки слід отримати у будь-якому разі.

Якщо в процесі перевірки встановлена придатність кандидата для роботи в служби безпеки, то його направляють на навчання до недержавної освітньої установи (крім осіб, що мають стаж роботи в оперативних або слідчих підрозділах не менше трьох років). При цьому особливу увагу звертають на наявність ліцензії у цієї установи і якість програми навчання. Після проходження спеціальної підготовки і отримання ліцензії охоронці доцільно організувати стажування кандидата на відповідній посаді (від 1 до 6 міс.) і лише після цього вирішувати питання щодо його зарахування на постійну роботу в службі безпеки або звільнення. Зрозуміло, така можливість має бути передбачена в контракті, який підписується після відбору кандидата.

Повне і якісне забезпечення служби безпеки матеріально-технічними ресурсами - не тільки засіб, а й умова підвищення ефективності роботи її працівників. Ці ресурси умовно поділяють на такі групи:
- зброя і боєприпаси;

- спеціальні засоби;
- службові приміщення різного характеру (кабінети, караульні приміщення, збройові кімнати, стрілецькі тири, кімнати огляду);
- допоміжна техніка (автотранспорт, відео -, кіно -, фототехніка, засоби оперативного радіо - і телефонного зв'язку, комп'ютери тощо);
- засоби запобігання й захисту (охоронно-пожежна сигналізація, сторожові собаки, охоронне освітлення, телебачення та ін.);
- засоби забезпечення нормальної діяльності працівників (формене обмундирування, меблі, канцелярське приладдя, медикаменти, бланки документів, юридична і спеціальна література тощо).

Нарешті, останнє за послідовністю, але не за важливістю, забезпеченні діяльності служби безпеки інформаційними ресурсами. Насамперед слід визначити потребу і обсяги мінімуму інформації, без якої функціонування служби безпеки взагалі неможливе. Таку інформацію можна умовно поділити на три блоки ("Середовище функціонування підприємства" "Стан безпеки усередині підприємства" і "Внутрішньо-організаційна діяльність служби безпеки"), після чого в рамках кожного блоку скласти перелік необхідних відомостей. Цей перелік буде довільним, якщо при його складанні керуватися одним принципом: будь-яка інформація реально мас "обслуговувати", "працювати" на реалізацію як мінімум однієї функції служби безпеки. Можна рекомендувати у зв'язку з цим відносити до цих блоків такі дані, які, зрозуміло, не можуть бути вичерпними.

До першого блоку "Середовище функціонування підприємства" за звичай належать відомості про підприємства-конкуренти, правоохоронні й контрольно-наглядові органи, ринкову кон'юнктуру, криміногенну ситуацію в регіоні, місце розташування підприємства, нормативні акти, що регулюють діяльність підприємства-засновника.

Другий блок "Стан безпеки усередині підприємства" містить відомості про:

- стан злочинності серед персоналу;
- наявність або відсутність комерційної таємниці;
- джерела (канали) і суми матеріального збитку, завданого підприємству;
- аналіз насильницьких злочинів, здійснених проти персоналу;
- ефективність роботи юрисконсульта (юридичної служби);
- співробітників підприємства, що мають доступ до конфіденційної інформації і пов'язані зі збереженням товарно-матеріальних цінностей;
- про місцезнаходження документації, що містить комерційну таємницю, і правила роботи з нею;
- місце розташування і зберігання виробів (описи процесів), що становлять таємницю підприємства.

Нарешті, в третьому блоці "Внутрішньо-організаційна діяльність служби безпеки" мають бути відомості про склад і структуру служби безпеки, переміщення її працівників, дисциплінарну практику, результати перевірок, стан законності.

Очевидно, що без належної практичної організації використання такого масиву інформації не обійтися. Ідеальним варіантом у цьому разі було б створення інформаційної системи на базі комп'ютерної техніки, проте її створення потребує певних витрат. Тому на практиці найчастіше трапляється віддзеркалення й систематизація необхідної інформації в письмових документах. До документів, які складають у службі безпеки і прийнятих вищими державними органами управління, належать:

- організаційні (статут, положення, посадові інструкції, штатний розклад, правила внутрішнього трудового розпорядку);
- правові (закони, підзаконні акти, методичні рекомендації щодо проблем безпеки і т.ін.);
- розпорядчі (накази, інструкції, вказівки, графіки роботи персоналу тощо);
- інформаційно-довідкові (наприклад, протоколи, акти, довідки, листи, доповідні й пояснювальні записки, телефонограми, телеграми, досьє);
- договори, трудові угоди;
- документи про особовий склад (накази щодо особового складу, трудові книжки, матеріали перевірок скарг, графіки відпусток і т. ін.).

Правильно організованим документальним відображенням необхідних відомостей досягають ефективного інформаційного забезпечення діяльності служби безпеки.

Ліквідація служби безпеки можлива у разі добровільної відмови її персоналу від виконання своїх обов'язків, за ініціативою підприємства-засновника, при ліквідації підприємства-засновника і при анулюванні органом внутрішніх справ ліцензій усіх охоронців і детективів. Перший і останній варіанти швидше можливі теоретично, проте повністю виключати їх не можна.

3. ІСТОРІЯ ТА ПЕРЕДУМОВИ ВИНИКНЕННЯ ТА АКТУАЛЬНІСТЬ ДІЛОВОЇ (КОРПОРАТИВНОЇ), ЕКОНОМІЧНОЇ РОЗВІДКИ, ЇЇ ВИДИ ТА НАПРЯМИ РОЗВИТКУ

Аналіз політичних та економічних ризиків в Україні дає підстави стверджувати, що ситуація з ними значною мірою поліпшилася. Це відзначають як українські бізнесмени, так і зарубіжні рейтингові агентства і компанії. Вони переконані, що в нашій країні є перспективи дія успішного розвитку бізнесу.

Кожне підприємство прагне стати конкурентоспроможним на ринку виробництва та реалізації продукції (послуг), і для цього йому необхідно постійно вдосконалювати технологічні процеси, використовувати сучасні досягнення науки і техніки, вводити ноу-хау, автоматизувати облік, підвищувати рівень знань персоналу тощо.

Сучасна ринкова економіка ставить завдання щодо забезпечення суверенітету й незалежності України: свобода, справедливість, безпека, розвиток науки і техніки, прогрес, а отже, отримання й захист інформації,

потрібної для маркетингової діяльності та прийняття управлінських і стратегічних рішень щодо розвитку бізнесу.

Економічна реформа в Україні дала поштовх для появи на економічному ринку недержавних суб'єктів господарювання-акціонерних товариств, комерційних банків, приватних і спільних підприємств.

Практична діяльність суб'єктів недержавного бізнесу, їх мобільність і маневрування перевершили державні структури, створили для них умови впливу і регулювання економіки держави, надали можливість впроваджувати сучасні технології, збільшувати податкові надходженні в бюджет, розширювати експорт, освоювати нові ринки збуту товарів, створювати нові робочі місця. Характерно, що навколо них створюються недержавні фінансові й соціальні інфраструктури.

Сучасна ситуація на українському і світовому ринках характеризується ускладненням комерційних схем та умов здійсненні операцій, використанням комплексних продуктів, посиленням конкуренції між компаніями. Фінансові потоки, рух капіталу, управління ресурсами і персоналом стають складним завданням, що пов'язане із зростанням обсягів звітності і документообігу, збільшенням швидкості інформаційних потоків та своєчасності отримання комерційної інформації.

Вітчизняний бізнес упродовж багатьох років працював в екстремальних умовах, і всім учасникам ринку доводилося працювати в них. Тому не дивно, що у бізнесі сформувалися свої, українські, принципи управління. Але з плином часу способи вирішення проблем, на жаль, залишаються незмінними, і забезпеченню економічної розвідки підприємства досі не приділяється належна увага. Питаннями розвитку та організації економічної розвідки займаються як державні, так і недержавні структури. В ринкових умовах саме недержавні структури економічної безпеки через свою мобільність, краще матеріальне забезпечення, маневрування та розосередження на сучасних ринках мають більші можливості для отримання й аналітичного опрацювання інформації, розроблення стратегій і тактичних прийомів розвитку економічної розвідки.

Попри низку переваг основною вадою недержавних суб'єктів економіки є те, що вони більш уразливі до протиправних зазіхань з боку кримінальних структур і окремих суб'єктів господарювання. Як зазначалося в попередніх розділах, гарантування безпеки підприємницької діяльності стає життєво важливою потребою функціонування недержавних суб'єктів економіки.

Тому справедливим є твердження: якщо в бізнесі є уразливі місця, то завжди знайдуться охочі скористатися плодами чужої праці, а це призводить до виникнення цілого синдикату активних структур економічної розвідки організованої злочинності. Якщо до цього ще додати напружену криміногенну обстановку в сучасній економіці, коли все купується і продається, то цілком зрозумілим стає актуальність проблеми забезпечення захисту об'єктів економіки від зазіхань організованої злочинності і промислового шпигунства, збереження комерційної таємниці фірми, а також створення і функціонування недержавних служб безпеки.

Для того щоб зрозуміти призначення та організацію ділової (корпоративної) розвідки, здебільшого розвідки великої компанії, корпорації чи концерну, потрібно визначити види загроз бізнесу, спрогнозувати можливі втрати, а вже потім сформулювати мету створення служби ділової розвідки, її функції та засоби протидії й ліквідації загроз, тобто будь-яких дій, явищ чи процесів, що можуть спричинити негативні наслідки для бізнесу (матеріальні й моральні втрати).

Визначаючи загрози, варто враховувати:

- їх реальність;
- сутність причин, що їх спричинила;
- гостроту цих причин і термін їх впливу;
- сили й кошти, якими користується супротивник, конкурент.

На будь-якому підприємстві (незалежно від його розмірів) потрібно розробити систему виявлення й розпізнавання загроз та конкретні рекомендації щодо їх локалізації.

Важливим у гарантуванні економічної безпеки України є захист її ринкових основ, насамперед економічної конкуренції. Уникнути конкурентної боротьби підприємці не зможуть, бо вона є іманентним явищем ринку. Отже, потрібно вчитися перемагати в конкурентній боротьбі, приймати ефективні і своєчасні рішення щодо конкурентів. Утриматися в світі підприємницького ризику неможливо поза створенням надійної системи збирання й опрацювання інформації про конкурентне середовище, про низку ймовірних ризиків. І ставлення керівництва підприємства до створення такої системи має бути відповідним.

В умовах гострої конкуренції проблема пріоритетів використання досягнень науки й техніки є найважливішою. Інструментом її розв'язання стає промислове шпигунство, а в позитивному аспекті - ділова розвідка. Як іманентна складова сучасної ринкової конкуренції, ділова розвідка виступає складовою економічної розвідки і посідає відповідне місце у правовому полі України, однак має ще недостатньо визначений і досліджений науковцями вплив на економічну безпеку. '

Реалії сучасного ділового світу такі, що більшість підприємців і керівників підприємств розуміють, що без глибокого аналізу інформації, якою нині наповнені ринки, неможливе успішне ведення бізнесу. Потоки інформації, що генеруються учасниками ділової активності, за її кваліфікованого опрацювання, аналізу й синтезу здатні забезпечити підприємство конкурентною перевагою стосовно інших гравців ринку, які не володіють потрібною інформацією в потрібний час.

У ринкових умовах науково-технічний прогрес перетворюється на сферу гострої конкуренції, метою якої стає отримання надприбутку, який мають ті суб'єкти господарської діяльності, які швидше за всіх впроваджують інновацію у виробництво і монополізують її: засекречують, захищають патентом.

У будь-якому бізнесі за будь-яких умов, перш ніж вкладати гроші, розвивати або змінювати сферу діяльності та напрям бізнесу, вибирати

партнерів з бізнесу, потрібно активно збирати інформацію для прийняття управлінських рішень. Підприємці змушені щодня і постійно вирішувати завдання конкурентної розвідки.

Реалізація інновацій знижує індивідуальну собівартість продукції. Виникає різниця між ринковою ціною та індивідуальною собівартістю продукції, що перебільшує середній прибуток.

Час існування цього тимчасового надприбутку перебуває у зворотній залежності від швидкості розповсюдження цих інновацій, тобто від масовості використання їх конкурентами, що призводить до збільшення пропозиції, зменшення попиту і, як результат, до зниження ціни та зникнення надлишку над середнім прибутком. Бажання підприємців отримати й монополізувати цей додатковий прибуток стає стимулом і водночас гальмом науково-технічного прогресу, який набирає суперечливої форми, а саме:

- для загальновиробничого розвитку науково-технічний прогрес дає можливість розширювати виробництво, автоматизувати технологічні процеси, урізноманітнювати асортимент продукції тощо;
- для власного прискорення він повинен постійно долати вузькі індивідуальні економічні інтереси тих, хто монополізує інновацію.

До розв'язання цих питань і суперечливих проблем бізнесу та розвитку добросовісної конкуренції виявляє інтерес ділова розвідка, яку можна трактувати як окремий, більш звужений напрям економічної розвідки.

У публіцистичних творах економічну розвідку часто ототожнюють з промисловим шпигунством, вважаючи, що для організатора - це економічна розвідка, а для суб'єкта протидії-промислове шпигунство. У вивченні й визначенні меж діяльності економічної розвідки, як і в її історії та розвитку, чимало "білих плям", таємниць і недомовок. Етапи економічної розвідки чітко визначають, що вона є складовою історичного розвитку продуктивних сил та науково-технічного прогресу.

Ринок економічної розвідки України тільки формується. Досі для цього не було об'єктивних економічних обставин. Ще кілька років тому жорстка конкуренція замінювалася з'ясовуваннями стосунків та кримінальними "розборками". Нині ринок дедалі більше набуває структурованого, цивілізованого характеру. І тепер навіть малий бізнес, аби відносно спокійно прийняти рішення, має займати певний сектор ринку, йти в той чи інший регіон, виготовляти конкретний вид продукції, вкладати гроші в певний бізнес, першочерговим має бути попереднє інформаційне опрацьовування.

Характер, форми і способи ведення економічної розвідки змінювалися зі зміною суспільно-політичних формацій, з еволюцією виробництва та рівня розвитку науки й техніки. В історичному плані економічну розвідку можна вважати більш давньою, ніж політичну та військову.

Враховуючи, що сьогодні без отримання інформації та її аналізу, проведення маркетингових досліджень і розвідувальної діяльності неможливо успішно вести бізнес, роль і актуальність впровадження ділової (корпоративної) розвідки, як однієї з розгалужень економічної, є беззаперечною і важливою.

Історія виникнення економічної розвідки, її види та напрями розвитку

Історичні витоки економічної розвідки сягають кінця XIV-початку XV ст. Батьківщиною її вважають Китай. Класичним прикладом економічної розвідки є романтична історія, в якій розповідається про китайську принцесу, яка задля коханого перевезла в капелюсі з живих квітів шовкопрядів, передавши за кордон секрет виготовлення китайського шовку, що багато років був об'єктом розвідки іноземних агентів.

Значними секретами на той час володіли й араби. Для отримання інформації багато агентів і шпигунів відвідували арабський Схід. Араби вміло зберігали свою інформацію, однак, на відміну від китайців, в них можна було її купити.

В аграрну епоху поряд із державною економічною розвідкою зародилася і приватна розвідка. Перша розвідувальна служба була створена флорентійськими купцями-банкірами на початку XIV ст.

Формально виникнення промислового шпигунства пов'язане із запровадженням у XVIII ст. системи патентів на винахід, які мали охороняти права винахідника чи дослідника. Власник патенту на винахід отримував право на переслідування викрадачів секретів протягом двадцяти років, після чого секрет ставав власністю суспільства. З одного боку, введення патенту зумовило багато проблем, а з другого - ознаменувало кінець періоду, який називають кустарним періодом економічної розвідки.

У сучасній літературі трапляються різні поняття розвідки у сфері економіки, а саме:

- економічна розвідка;
- економічне шпигунство;
- конкурентна розвідка;
- бізнес-розвідка;
- ділова розвідка;
- комерційна розвідка;
- промислове шпигунство;
- бізнес-шпигунство;
- корпоративна розвідка;
- інформаційна розвідка;
- фінансова розвідка.

Визначимо істотні риси цих понять. Спільною рисою для усіх є діяльність з отримання інформації для прийняття рішення. Особливості полягають ось у чому. Саме поняття "шпигунство" відрізняється від поняття "розвідка" правовим статусом. Шпигунство ґрунтується переважно на незаконних методах отримання інформації, а розвідка - на законних. При цьому етичний аспект проблеми, як правило, до уваги не беруть.

Розвідка, як і шпигунство, може бути державною (політичною), воєнною та економічною. Масштаб цих явищ - інтереси держави.

Економічна розвідка та шпигунство - хвороба усіх країн та великих національних і транснаціональних корпорацій. Ними активно займаються як державні, так і недержавні служби безпеки. За неофіційними оцінками державних служб безпеки, практично кожна велика фірма краде інформацію у конкурентів і водночас страждає від аналогічних дій з їх боку.

У сучасному світі бізнесу афоризмом став вислів, що капітал боїться відсутності прибутку або дуже малого прибутку так само, як і природа боїться порожнечі. Нові досягнення науки і техніки, сучасні методи промислового виробництва змушують економічну розвідку знаходити нові засоби й методи роботи. Щоб устигати за технічним розвитком, потрібно постійно вдосконалювати техніку шпигунства.

Економічна розвідка охоплює дедалі нові й нові галузі. Тобто промислове шпигунство - це неминуче й закономірне явище самої природи бізнесу, що ґрунтується на бажанні отримати надприбуток будь-якими дозволеними й недозволеними методами. Воно має глибокі економічні корені. Кінцева мета економічної розвідки - забезпечити на мікрорівні додатковий прибуток, по-перше, шляхом копіювання і впровадження "чужої"" інновації і, по-друге, за рахунок економії на умовно-постійних витратах - на науково-дослідних та проектно-конструкторських роботах.

Трактування понять "економічна розвідка", "ділова розвідка", "корпоративна розвідка" дають переважно російські практики та науковці, оскільки на український ринок ці служби просуваються надто повільно, однак і в Україні є вже певні напрацювання в цьому напрямку. Так, У Законі України "Про розвідувальні органи" від 22.03.2001 р. № 2331-III дано визначення понять "розвідувальна діяльність" та "розвідувальна інформація", а саме: "розвідувальна діяльність-діяльність спеціальних органів державної влади, спрямована на захист національних інтересів України від зовнішніх загроз, сприяння формуванню і реалізації державної політики у сферах національної безпеки і оборони"; "розвідувальна інформація - добуті відомості про реальні та потенційні можливості, плани, наміри і дії іноземних держав, організацій та окремих осіб, що загрожують національним інтересам України, а також про події і обставини, що стосуються національної безпеки і оборони". Однак поняття "економічна розвідувальна діяльність" у законодавстві не визначено.

У нашій державі не відбуваються процеси взаємодії між приватним бізнесом і роботою спецслужб, що призводить до різних зловживань.

Важливим у проведенні економічних розвідувальних дій є те, що більшість необхідної інформації можна взяти з легальних відкритих джерел. Через те існує тісний взаємозв'язок між економічною розвідкою, захистом інформації, діяльністю служби безпеки та якісним складом персоналу компанії чи фірми.

Час, коли компанії боролися з конкурентами за допомогою кримінального тиску або адміністративного ресурсу, минув, запевняють бізнесмени. Нині перевагу має той, хто веде ділову розвідку і знає таємницю своїх суперників. В умовах, коли учасники ринку пильно стежать один за одним, необережна заява

або навіть проста неакуратність працівників може обернутися для компанії втратою частки на ринку.

Терміном "конкурентна розвідка" (competitive intelligence) близько 20 років тому в США почали позначати збирання інформації, необхідної для компанії, її успішного розвитку. В Європі більш поширеним є визначення business intelligence - бізнес-розвідка. Завдання конкурентної розвідки - збирання інформації про ринок, бенчмаркінг (вивченні товарів, послуг або методів роботи конкурентів для використання у своїй діяльності), захист конфіденційної інформації, пошук і вивчення об'єктів для поглинання тощо. На відміну від промислового шпигунства, конкурентна розвідка вирішує ці завдання легальними, хоча і не завжди етичними методами.

Ділову (корпоративну) розвідку ведуть компанії з різних секторів ринку. Причиною такого зацікавлення є посилення конкуренції і більшої цивілізованості бізнесу. За останні роки змінилися не лише підходи до безпеки бізнесу, ставлення до організації ділової розвідки, а й форми, методи ведення, підбір персоналу та завдання служб розвідки. Однак суть її залишилася незмінною. Якщо 10 років тому розвідники насамперед перевіряли наявність у бізнес-партнерів кримінальних зв'язків, то тепер вони, як і на Заході, переважно добувають комерційну інформацію.

Багатьом достатньо дізнатися про сильні і слабкі сторони свого конкурента (суперника) та його репутації, щоб скоригувати свою поведінку, при цьому спрацьовують інтуїція і досвід розвідників-маркетологів. Це підтверджують і дані дослідження, проведеного Міжнародним центром конференцій OnConference : більшість компаній використовують ділову розвідку для вивчення стану ринку (74% респондентів) і конкурентів (64%).

В Україні ділова розвідка ще не набула належного розвитку, не досліджена і не описана науковцями, тому ми вивчаємо її за джерелами російської науки і практичною діяльністю розвідувальних фірм.

Вибрати фірму, що займається бізнес-розвідкою, в нашій країні не зовсім просто: в Україні поки не складаються рейтинги подібних компаній (при тому, що досить поширені банківські рейтинги, рейтинги аудиторських і консалтингових фірм тощо). Для вивчення цієї послуги можна проаналізувати матеріали газети Financial Times, яка щороку готує спеціальний додаток про різні галузі, пов'язані з корпоративною безпекою. На теренах колишнього СНГ працюють представництва іноземних компаній, які теж фігурують в огляді газети.

Для вибору "розвідувальної"" компанії можна:

- піти найпростішим шляхом - порадитися зі своїми колегами, які мають досвід звернення до подібних фірм;
- влаштувати тендер між кількома компаніями, порівнюючи пропоновані ними послуги;
- скласти рейтингову таблицю за часовим чинником;
- провести класифікацію і групування фірм за ціновими пропозиціями "розвідувальних" послуг.

Загалом термін "виконання розвідувальних замовлень" завжди залежить від їх специфіки та повноти наданих послуг: зазвичай він становить від двох до шести тижнів, хоча деякі проекти інколи ведуть протягом кількох років. Ціна - категорія ще більш індивідуальна: вона може сягати від кількох сотень доларів до суми, яка істотно відрізняється від стартової.

Послуги, що надаються при виході на новий ринок, у разі появи нового конкурента та посилення конкуренції, відомі як конкурентна розвідка (від англ. competitor intelligence). Ідеться не про промислове шпигунство, а про експертну оцінку планів і стратегій конкурента, про принципи його збутової політики, процеси ухвалення рішень; про осіб, що мають вплив на цей процес; про провідних менеджерів, кадрову політику і т.ін.

Припустімо, що торговельна компанія отримала інформацію про те, що її головний конкурент активно набирає нових працівників - маркетологів і менеджерів з продажу. Вивчивши вимоги конкурента до цих працівників (хороше знання польської і болгарської мов, а також специфіку роботи на східноєвропейських ринках), компанія дізналася, що конкурент збирається освоювати нові ринки збуту продукції 6 результаті компанія зуміла випередити головного конкурента у виході на новий ринок саме завдяки тому, що вчасно отримала достовірну "розвідувальну інформацію".

Не слід очікувати від бізнес-розвідників неможливого. Врешті-решт, про все, що відбувається в компанії-конкурента, партнера, позичальника, інколи не знає навіть її власник. Можна мінімізувати можливі ризики, але уникнути їх у повному обсязі неможливо.

За оцінкою експертів компанії Ci Consulting, нині тільки в Москві діє понад 10 потужних компаній, що спеціалізуються на бізнес-розвідці. їх послуги обходяться клієнтові в середньому в $1000 за місяць, а витрати на утримання власного розвідника в штаті спеціалісти оцінюють мінімум в $20000 за рік. Разове ж замовлення послуг розвідки коштує зовсім недорого - $50-200, залежно від обсягу потрібної інформації.

Аналіз свідчить, що українським бізнесменам, котрі щойно виходять на цивілізовані ринки, матеріально досить важко організовувати власну службу ділової розвідки, бо для цього потрібні значні фінансові ресурси. На початкових етапах значно вигідніше скористатися послугами служб безпеки, детективних бюро, маркетингових фірм тощо. Однак такий підхід теж має свої вади і переваги.

4. СПЕЦИФІКА ТРАКТУВАННЯ ДІЛОВОЇ (КОРПОРАТИВНОЇ) РОЗВІДКИ ТА ЇЇ ВІДМІННІСТЬ ВІД ПРОМИСЛОВОГО (КОМЕРЦІЙНОГО) ШПИГУНСТВА.

В умовах конкуренції спостереження за діяльністю профільних підприємств стає обов'язковим. Інформація про плани інших підприємств необхідна маркетологам, рекламістам і виробничникам, щоб оперативно реагувати на

зміни ринку й новаторства конкурентів. Тому конкурентна розвідка у тому чи іншому вигляді існує на будь-якому підприємстві від самого початку його діяльності. Генеральний директор, який щодня переглядає корпоративні новини в ділових виданнях, фінансовий аналітик, який відстежує біржові котирування, маркетолог, який спостерігає за діями інших компаній, роблять приблизно те саме, що й конкурентний розвідник. Різниця лише в тому, що фахівець з конкурентної розвідки цілеспрямовано збирає, аналізує й сортує інформацію, готує рекомендації для керівництва фірми.

На невеликих підприємствах зі збиранням і сортуванням різної інформації цілком може впоратися одна людина. Зовсім не обов'язково, щоб особа займалася виключно конкурентною розвідкою — крім пошуку й аналізу інформації вона цілком може обіймати посаду, приміром, заступника директора з персоналу. Створювати окремий підрозділ конкурентної розвідки потрібно, коли обсяг необхідної інформації настільки зростає, що не можна обійтися без системної обробки даних.

Конкурентна розвідка — не промислове шпигунство, як багато хто помилково вважає, хоча в них є спільні риси. Мета як конкурентної розвідки, так і промислового шпіонажу — одержання відомостей про діяльність конкурентів, і нинішніх, і потенційних. Конкурентною розвідкою, як і шпигунством, зазвичай займаються фахівці. Але на цьому спільне закінчується.

Головна відмінність конкурентної розвідки від шпигунства — методи й способи отримання інформації, все, що використовується розвідником, є законним. Промисловий шпіонаж, навпаки, передбачає нелегальні методи і технології. Служба конкурентної розвідки користується тільки відкритими джерелами, основна робота розвідника — інформаційно-аналітична, тобто збирання і опрацювання різних даних, що впливають або можуть негативно вплинути на розвиток бізнесу. Шпигунство полягає головним чином в оперативній роботі, зокрема й у вербуванні інсайдерів та збиранні конфіденційної інформації для досягнення конкурентних переваг. Крім того, промисловий шпіонаж передбачає лише збирання інформації, як правило, досить чітко вказаної керіництвом. Конкурентна розвідка орієнтована не тільки на збір і аналіз різних даних, а й на вироблення управлінських рекомендацій, а також на прогнозування можливих дій конкурентів або змін ринку.

Служба конкурентної розвідки на підприємстві може створюватись двома шляхами.

Перший — «під керівника». У цьому випадку топ-менеджер запрошує фахівця й надає йому повноваження та кошти на створення розвідслужби. Фактично керівник конкурентної розвідки входить до числа топ-менеджерів і повністю відповідає за ефективність роботи своєї служби.

Інший варіант — поступова еволюція інших підрозділів у службу конкурентної розвідки. Наприклад, на підприємстві тривалий час працював аналітичний відділ або окремий фахівець, який збирав інформацію (можливо, виконував цю роботу навіть не з обов'язку, а за покликом душі). Поступово коло його обов'язків розширювалося, поставлені завдання ускладнювалися,

обсяг виконуваної роботи збільшувався. Зрештою такий відділ або людина починали працювати фактично як конкурентні розвідники, а потім формувався окремий підрозділ зі своєю структурою, функціями й бюджетом. Саме в такий спосіб найчастіше і створюється служба бізнес-розвідки.

У новому підрозділі конкурентної розвідки найчастіше працює одна особа, яка і виконує всю роботу самостійно. Поступово, зі збільшенням кількості необхідної інформації й розширенням кола завдань, служба конкурентної розвідки розростається. Втім, це відбувається не завжди — і в невеликих компаніях працівник конкурентної розвідки може самостійно виконувати всі завдання, пов'язані з пошуком, обробкою та зберіганням формації.

Головним завданням служби конкурентної розвідки є надання компанії конкурентних переваг, насамперед шляхом повного й об'єктивного інформування топ-менджменту про виникнення або зникнення факторів, що впливають на розвиток бізнесу, і вироблення рекомендацій для прийняття управлінських рішень. Тобто служба має бути підзвітною й підконтрольною керівництву компанії, а результати її роботи повинні бути помітними і можуть бути виражені в грошовому еквіваленті.

Приклади використання конкурентної розвідки на вітчизняних підприємствах.

«Дорога редакціє». Якщо у відкритих джерелах необхідну конкурентному розвіднику інформацію не знайдено, існує абсолютно законний, хоча й не зовсім етичний метод її отримання «з перших рук», тобто від керівника досліджуваної компанії. Для цього достатньо зателефонувати до приймальні директора і, представившись журналістом відомого видання, домовитись про коротке інтерв'ю. Саме так і вчинив працівник великої української компанії – виробника хімічної продукції. Отримавши завдання зібрати дані про конкурента – недавно відкрите представництво західної корпорації, він через секретаря домовився про зустріч з одним із найвищих керівників концерну. Топ-менеджер легко пішов на контакт з «представником преси» і під час особистої зустрічі, вміло скеровуваний запитаннями розвідника, сам видав усю цікаву інформацію. Звинуватити конкурента в отриманні конфіденційних даних нелегальним шляхом неможливо – керівник сам передав інформацію «журналістові», тобто малося на увазі, що вона може бути опублікована в засобах масової інформації.

«Кадрові агентства». Витончений спосіб отримання конкурентної інформації винайшла вітчизняна компанія, яка займається продажем предметів розкоші. Для збирання даних про прямих конкурентів, вона розмістила в Інтернеті оголошення від імені щойно створеного підприємства про відбір на посади, аналогічні тим, що були в конкурентів. Однак запропоновані заробітні плати істотно відрізнялися від установлених конкурентами, зрозуміло, в бік збільшення. Розвідники подбали про те, щоб дані про конкурс потрапили до потрібних співробітників або їхніх знайомих. Унаслідок вузького профілю галузі всі заявки на співбесіду надійшли від працівників фірм-конкурентів, і

всім кандидатам було запропоновано прийти на співбесіду. За годину бесіди з претендентами, представник «створюваної фірми». А насправді – працівник служби конкурентної розвідки підприємства, одержав від опитуваних багато відомостей про організаційну структуру конкурентів, технологію прийняття рішень у їхніх компаніях, дані про особисті якості керівників.

«Держава нам допоможе». Іноді корисним для отримання конкурентних переваг може бути використання в комерційних цілях державних органів. Нещодавно працівникам служби конкурентної розвідки великого столичного виробничого підприємства вдалось встановити, що конкурент у своїй діяльності використовує схеми ухилення від сплати податків. Отриману інформацію було передано до податкової адміністрації та відділу боротьби з економічною злочинністю. Проведене правоохоронцями розслідування виявило, що в цій схемі було задіяне також інше велике підприємство формально ніяк не пов’язане з компанією-правопорушником. Таким чином службі конкурентної розвідки вдалося встановити раніше не виявлений зв'язок між двома великими гравцями ринку і розробити відповідні рекомендації для коригування стратегічного плану розвитку. Крім того, завдяки швидкій роботі конкурентної розвідки підприємству вдалося виграти тендер на постачання товару, проведений західною компанією, оскільки заявки головних конкурентів – нечистих на руку підприємств – були відхилені внаслідок їхнього конфлікту з податковою адміністрацією.

Причиною ототожнення понять "промислове шпигунство" та "економічна розвідка" є неправильне розуміння самого терміна "промислове шпигунство ". Вважається, що воно неодмінно пов'язане з промисловістю і виробництвом. А оскільки більшість сучасних бізнесменів пов'язують свій бізнес з перепродажем та наданням послуг, вони сподіваються, що їхні інтереси залишатимуться недоторканими.

Деякі автори поєднують поняття економічної, промислової, комерційної розвідки з промисловим шпигунством і дають визначення поняттю "розвідка". Зокрема, Євген Смолин вибрав прямолінійний підхід до трактування економічної розвідки, обмеживши її діями за межами держави, які свідчать про наявність спеціальної організації, основна діяльність якої опосередковано або безпосередньо спрямована на добування розвідувальних даних і підрив економічної безпеки держави або конкретного суб'єкта. Одночасно автор подає основні засоби здійснення розвідувальної діяльності, а саме:

- крадіжка креслень, зразків, документів чи інших інформаційних носіїв;
- переманювання в свою фірму службовців конкурента;
- фіктивні переговори з метою заволодіння важкодоступною інформацією;
- вербування агентів;
- впровадження своїх людей у "потрібні організації".

Г. Г. Агафонов, С. А. Буришев, СЯ. Прохоров у тритомнику "Концепція безпеки" також ототожнюють економічну розвідку з промисловим або комерційним шпигунством, зазначаючи, що термін економічна, промислова,

комерційна, науково-технічна розвідка (шпигунство) означає активні дії, спрямовані на збирання, крадіжку, накопичення та оброблення цінної інформації, закритої для доступу сторонніх осіб, які ведуться недержавними організаціями і приватними особами. Ці автори стверджують, що промислове шпигунство стало невід'ємною складовою економічної розвідки і має на меті заволодіння ринками збуту, підроблення товарів, дискредитацію або усунення конкурентів, зрив переговорів за контрактами, перепродаж бізнес-таємниць фірм, шантаж посадових осіб, створення умов для підготовки терористичних і диверсійних актів.

Забезпечення успішної комерційної діяльності підприємців, розвиток цивілізованої конкуренції, створення безпечних умов ведення бізнесу примушують власників підприємств використовувати розвідувальні можливості, а розвідка розглядається як діяльність, призначена для отримання стратегічної (тактичної або конкурентної) переваги над супротивником, виявлення можливих ризиків і управління ними.

Зрозуміло, інформація, яку використовують бізнес-розвідники. надходить від сторонніх джерел, а не від самої компанії - об'єкта дослідження (як це часто відбувається у роботі рейтингових агентств). Крім того, інформацію потрібно перевіряти за кількома джерелами, адже вона є основою для ухвалення найважливіших стратегічних рішень .

Якщо різні джерела дають приблизно однакову інформацію, то це гарантує високий ступінь її достовірності. А коли отримана з різних джерел інформація не збігається, її потрібно аналізувати з урахуванням цього факту. (До речі, це хороший спосіб перевірити професіоналізм "розвідувальної"" компанії, до якої ви звернулися: вона завжди повинна оцінювати частку достовірності тої або іншої інформації (50,80 або 100%). Тому якщо вам говорять, що вся зібрана інформація достовірна на 100%, то, швидше за все, вас обдурюють.

Зарубіжні детективні та "competitive" агентства проводять діяльність, в основі якої лежить легітимність розвідки, а саме: добування інформації законними та етичними методами. В нашій державі розвідка практично використовується лише в службах безпеки акціонерних товариств, корпорацій, банків та в спеціалізованих агентствах. Тому актуальним є трактування Г. Лемке, що розвідка є діяльністю, що спрямована на забезпечення стратегії та комерційного успіху підприємства і здійснюється з метою придбання стратегічної (тактичної або конкурентної) переваги над супротивником (конкурентом), виявлення можливих ризиків і нових можливостей для підприємства та управління ними.

Економічним підґрунтям розвідки є економія коштів, засобів та часу, бо інакше така розвідка не має майбутнього і нікому не буде потрібною. Враховуючи, що поняття "дешево" і "дорого" дуже суб'єктивні, розвідка - це завжди дешево, не в абсолютних показниках, а порівняно з отриманим результатом.

Основою інформаційної війни є заволодіння інформацією, яка повинна

відповідати таким вимогам: бути достовірною, повною, своєчасною і мати обмежений доступ. Недаремно інформаційний ресурс країни вже сьогодні визначається ступенем захищеності власної інформації та повнотою володіння чужою.

Незважаючи на низку прийнятих законів, їх повноту і справедливість, завжди існує спокуса обійти їх. Таку ситуацію характеризують вислови, що вже стали афоризмами: "спецслужби прикриваються гаслами "ми захищаємо демократію від демократії", а бізнес-шпигуни - словами "переможців не судять"".

Перш ніж розглядати ділову корпоративну розвідку, з'ясуємо суть ринкової складової корпоративної безпеки та основні фактори впливу на неї.

Ринкова складова корпоративної безпеки - це механізм захисту від неефективно обраної моделі поведінки підприємства на ринку, можливих помилок у веденні постачально-збутової і цінової політики та стратегії, виготовлення неконкурентоспроможної продукції чи надання послуг.

Ця складова відображує рівень відповідності внутрішніх виробничих можливостей підприємства зовнішнім, які формуються в ринковому середовищі, тобто наскільки виробнича, науково-дослідна робота, маркетингова діяльність відповідають запитам ринку й конкретним потребам споживачів. Важливість цієї складової економічної безпеки полягає в тому, що вона відповідає за процес доведення виготовленої продукції до конкретного споживача. Відомо, що всі зусилля з виробництва будуть зведені нанівець, якщо продукція не буде реалізована.

Неузгоджена робота маркетологів, дизайнерів, конструкторів, економістів, фінансистів, низька якість виготовленої продукції, невчасне реагування на зміну кон'юнктури ринку, неефективна збутова мережа, низький рівень культури підприємства - чинники внутрішнього середовища, які створюють загрозу ринковій безпеці підприємства.

Зовнішнє середовище непідконтрольне підприємству, в ньому в певних відносинах перебувають покупці, продавці, посередники, партнери, конкуренти, фінансові установи, рекламні агентства, митні й податкові організації.

На рівень ринкової безпеки впливають: нечесні дії конкурентів, платоспроможність покупців, часті зміни податків, курсу валют, політична ситуація у країні та світі. Поняття "корпоративна безпека" є складним і багаторівневим, взаємопов'язаним і взаємозалежним, характерним для будь-якого суб'єкта господарювання.

Чим більше уваги приділяють суб'єкти корпоративного сектора вивченню навколишнього середовища, реагують на зміни в ньому, аналізують їх, тим швидше можна передбачити небезпеку, вигідніше використовувати внутрішні можливості, прибутковіше вести бізнес. Саме службою, призначеною "тримати руку на пульсі" цих змін і контролювати маркетингову діяльність корпоративного сектора, є ділова розвідка, або Д(К)Р. За своєю формою, змістом і методами вона істотно відрізняється від промислового і комерційного

шпигунства. Для неї характерне насамперед дотримання законів та чинних нормативних актів, тоді як для промислового і комерційного шпигунства - порушення чинного законодавства.

Вважають, що коли конкурентна розвідка - це фактичне й досконале вивчення конкурента, збирання інформації про маркетингові дослідження неосвоєного ринку з метою забезпечення безперебійного та процвітаючого бізнесу, то ділова розвідка, яка також стосується структур безпеки бізнесу, є значно ширшою. Вона спрямована на розроблення нових технологій, отримання нових знань, прийняття управлінських рішень, досягнення значних переваг, поліпшення фінансових результатів, отримання максимальних прибутків за мінімальних витрат та розроблення стратегічних планів розвитку бізнесу.

В. Кишеня підкреслює, що конкурентна розвідка (competitive intelligence) - це вузький напрям ділової розвідки, який відповідає основній меті: побудові системи взаємовідносин з конкурентами, тобто розроблення комплексу заходів щодо отримання та обробки даних про конкурента: майнових, фінансових та управлінських ресурсах, можливостях і слабких місцях, а також про оперативні та стратегічні плани.

Ділова (корпоративна) розвідка - аналітичний процес, який перетворює розрізнені дані про бізнес (виробництво, збут, комерція чи надання послуг) на потрібну, точну й придатну інформацію про стан фінансово-господарської діяльності:

- підприємств-конкурентів;
- міжнаціональних корпорацій;
- підприємств-партнерів;
- іноземних корпорацій;
- зад і я них ними виробничих сил;
- використовуваних можливостей і намірів.

Тобто дотичними є три основних фактори - споживачі, конкуренти та зміни умов на ринках.

Отже, ділова розвідка, як і конкурентна, є різновидом економічної розвідки, яка має на меті не тільки формування бази даних про конкурентів, їх досягнення чи недоліки, а й прогнозування конкурентоспроможності власної продукції й конкурента, послуг і діяльності фірми; передбачення можливих економічних криз у фінансово-господарській діяльності організації; визначення шляхів їх усунення; вироблення рекомендацій щодо виходу на певний сегмент ринку; підбору кадрів та захисту стабільності й економічної безпеки фірми; розроблення стратегічних проектів для прийняття управлінських рішень.

Основними параметрами будь-якого бізнесу є:

- ідея - що потрібно робити, аби отримувати прибутки;
- процес - безпосередня діяльність для отримання прибутку завдяки правильній організації бізнес-процесів;
- ефективне управління ризиками - вишукування таких шляхів і методів, які б забезпечили беззбитковість бізнес-процесів або звели їх до

мінімуму.

Сутність поняття "ідея" полягає в отриманні максимальних доходів від наявних коштів. Ідею бізнесмен може придумати сам за умови, що він має відповідні кошти і час для її втілення в бізнес, а може запозичити в інших, скопіювати, викрасти тощо, економлячи при цьому час і кошти. Адже коли ця ідея перспективна і ввійшла в бізнес" "золота жила", то, напевно, жоден власник не захоче нею поділитися. Звідси висновок: ідею викупляють, збирають по крихтах і копіюють або банально викрадають.

Процес - це така модель організації бізнесу, котра дає змогу за рівних умов з партнерами по бізнесу отримувати значно більші прибутки.

Західні комерційні структури давно використовують таке поняття, як бенчмаркінг, під яким розуміють вивчення досвіду, стратегії, рішень, ділової практики кращих компаній галузі з метою використання в адаптованому вигляді для поліпшення якості роботи своєї компанії.

Існує й інше за змістом трактування поняття "бенчмаркінг": це метод управління, орієнтований на відтворення еталона. Він передбачає збирання інформації про чужі еталони і ключові параметри бізнес-операцій (бенчмарках) та їх відтворення у своїх компаніях. У перекладі з англ. слово benchmark означає геодезичну відмітку висоти - стійкий орієнтир, щодо якого визначають інші висоти й відстані. Бенчмаркінг - це порівняння ефективності системи з якимось установленим, прийнятим значенням. На Заході поняття "бенчмаркінг" почали використовувати наприкінці 1970-х років. У США, Японії та інших країнах програми бенчмаркінгу розвиваються за державної підтримки; діють також індустріальні бюро знайомств, мета яких - пошук партнерів з бенчмаркінгу.

Отже, бенчмаркінг - це система методів і способів вивчення позитивного досвіду партнерів та конкурентів, розроблення взаємозв'язаної системи показників ефективності й рентабельності, вивчення особливостей досягнення кожного з них окремо і в сукупності та індивідуальній"! зиск від показників, в основі чого лежить свідоме відтворення та впровадження у власному бізнесі необхідного комплексу бізнес-рішень.

Сьогодні ділова розвідка є складовою корпоративної культури ведення сучасного бізнесу. Для виживання підприємства в умовах конкурентної боротьби першочергову роль відіграє розвідка намірів конкурентів, вивчення основних тенденцій бізнесу, аналіз можливості ризиків тощо.

На Заході існує навчальна дисципліна business intelligence, яка вивчає ці аспекти бізнесу, а культура конкурентної розвідки настільки поширена і задіяна, що цей процес сприймається як належне.

На жаль, у нашій країні поняття business intelligence і industrial espionage розглядаються у взаємозв'язку, а термін business intelligence використовується з великою засторогою, оскільки через нерозуміння суті процесів розвідки її трактують як шпигунство.

Промислове шпигунство виникає там, де виявляється слабкість ділової розвідки. У практиці трапляються ситуації, коли правові межі не збігаються з

етичними. То ми маємо справу з некомпетентною діловою розвідкою чи із промисловим шпигунством?

Шпигунство припускає передавання, викрадання або збирання відомостей про державну або військову таємницю, тому промисловим шпигунством мають займатися відповідні органи, уповноважені на це державою. Розвідка і шпигунство - схожі поняття тільки у слов'янських мовах, а business intelligence і industrial espionage - абсолютно не збігаються.

Нині успішне ведення ділової (корпоративної) розвідки багато в чому залежить саме від конкурентної розвідки, адже своєчасне отримання достовірної інформації про конкурента, його діяльність є запорукою успіху власного бізнесу. Однак межа між маркетинговими прийомами добування інформації та промисловим шпигунством настільки непомітна, що її визначити проблематично.

Промислове шпигунство - це добування протизаконним шляхом конфіденційних даних про діяльність конкурентів, крадіжка відомостей, що становлять ноу-хау, ведення недобросовісної конкуренції, отримання персональних даних для їх використання у злочинних цілях.

Однак досить часто бізнес-матеріали, що становлять комерційну таємницю, якимось чином потрапляють на шпальти газет, в рекламні буклети, огляди тощо. Якщо для одних підприємств ця інформація неважлива, то для інших стає цінною знахідкою. Є ситуації, коли компанії, прагнучи отримати необхідні дані, нехтують етичними нормами і просто викрадають або купляють цінну для них інформацію, "зламують" комп'ютерні системи тощо.

Отже, визначити межі промислового шпигунства, тобто таємного отримання результатів нових досліджень, технологій, ноу-хау конкурентів із незначними витратами матеріальних і грошових ресурсів дуже складно.

Якщо будь-яка ланка випадає із взаємозв'язаного ланцюга, то промислове шпигунство не досягає своєї мети. Сучасне промислове шпигунство - це свідоме пошкодження промислового обладнання, інформаційних систем, психологічний тиск на працівників з метою дестабілізації діяльності конкурента. В наших умовах це спроба деяких фірм стати абсолютними монополістами в місті чи регіоні. Для цього застосовують, як уже зазначалося, підкуп, погрози, шантаж працівників, переманювання грамотних спеціалістів від конкурентів, крадіжки баз даних і описів технологічних процесів.

Дослідження гострих проблем вітчизняної економіки свідчать, що причиною більшості з них є неуважне ставлення керівників фірми і держави загалом до створення і захисту конкурентного середовища, організації конкурентної розвідки та гарантування економічної безпеки фірм як економічної одиниці, що може призвести не лише до значних фінансових витрат, а й до банкрутства та втрати бізнесу. Однак, незважаючи на існуючий досвід конкурентної політики високорозвинених країн, наша країна не вчиться на чужих помилках, а припускається серйозних прорахунків. Наприклад, змова товаровиробників нафтопродуктів, ринкова влада яких ґрунтується на належності російським кампаніям 90% вітчизняного ринку, призвела до

монополізації цього стратегічно важливого ринку.

Отже, ділова розвідка - явище об'єктивне й закономірне. Правовідносини в діловій розвідці складні, нечітко визначені, адже будь-які способи добування інформації про конкурента вже за своєю суттю с зворотногострою зброєю, яка може бути використана проти вашого бізнесу. Ці складнощі переживав бізнес у всіх країнах світу. Зокрема, в Японії донедавна існувала така філософія: для чого витрачати 10 років та 1 млрд. доларів на дослідження, коли за хабар в 1 млн. доларів інженер фірми-конкурента зможе швидше й ефективніше досягти такого самого результату. І лише в квітні 2003 р. Міністерство економіки та промисловості зробило перші кроки для оголошення промислового шпигунства діянням, що підпадає під кримінальну відповідальність. Аналогічна ситуація і у Франції. Уряд цієї країни визнає, що безпосередньо передає захоплені секрети французьким корпораціям, тут розвідка працює і для приватного сектора.

Ділова розвідка має суспільно-корисний характер, оскільки допомагає бізнесу, як вітчизняному, так і зарубіжному, розвиватися, вдосконалюватися, диверсифікуватися. Водночас у найближчому майбутньому, коли бізнес стане більш професійним, конкурентним і цивілізованим, ділова розвідка буде розглядатися як необхідна умова забезпечення стратегічної стійкості, конкурентоспроможності та економічної безпеки фірми.

На макрорівні всі країни ведуть економічну розвідку: це питання національної безпеки та міжнародного права. Разом із тим урядові розвідувальні структури дедалі частіше діють в інтересах приватних корпорацій. Стосовно мікрорівня йдеться про конкуренційне право, захист економічної конкуренції, авторських і суміжних прав, обмеження монополізму, порушення комерційної таємниці тощо. Що є законним, а що ні, мають вирішувати юристи, а для економістів головне - ефективність. Хоча між економістами та юристами має існувати чітка взаємодія на основі правовідносин цивілізованого ринку.

Нині стерті всі ідеологічні бар'єри, і шпигунство розглядається як звичайний бізнес, такий самий, як торгівля комп'ютерами, автомобілями чи сигаретами. Можна сказати, цей бізнес поставлено на економічну основу, де місце "солдатів холодної війни" зайняли економісти та маркетологи. Серед них існує така думка: "Багатий не той, хто перший винайшов велосипед, а той, хто перший дізнався про це і зробив свій бізнес".

Для досягнення найбільшої ефективності, пов'язаної зі збиранням, опрацюванням та узагальненням інформації" розвідувальна діяльність спирається на принципи й методи, деякі з яких мають закритий характер.

У практиці розвідувальної роботи давно використовується спостереження за конкурентом без проникнення на його об'єкти. Цьому сприяють новітні технічні засоби. За допомогою мініатюрних мікросхем, які вмонтовуються в аудіо - та відеотехніку, можна отримати найнеобхіднішу та широкомасштабну інформацію. Деякі з таких пристроїв можуть передавати інформацію на відстань 1000 км. Останнім часом у розвідувальній техніці використовується лазерний промінь.

Промислове шпигунство поставлено на державну основу і фінансується державою. За словами колишнього директора ЦРУ Гейтса, нині безпека ділової інформації дедалі частіше опиняється під загрозою, а джерел небезпеки стає все більше. Неприємності можуть виникнути не лише з боку організованих злочинних синдикатів і терористів, а й від розвідувальних центрів, що фінансуються урядом.

Уряди фінансують операції, під час яких вивчається діяльність різних компаній, можна отримати відомості про майбутні контракти, узагальнюється інформація про фінансовий стан організацій та банківських операцій, аналізуються події, які можуть позначитися на формуванні цін на світовому ринку.

Відповідні структури прагнуть володіти повною інформацією про стан ринку, а також про технології виробництва. Інколи вони навіть готові поділитися нею з компаніями своєї країни. Для отримання важливих відомостей розвідувальні служби США, Франції та інших країн використовують численні методи, розроблені в період "холодної" війни.

Через економічні правопорушення та корупцію щорічно компанії США втрачають $260 млрд. у межах країни і ще $140 млрд. - у зарубіжних операціях. Ці цифри щороку зростають. За даними Американської спілки промислової безпеки, починаючи з 1985 р. кількість випадків шпигунства щодо промислових галузей США зросло на 260%. За інформацією з інших джерел, США втратили від викрадення комерційних таємниць лише в 2001 р. $250 млрд.

На думку американських оглядачів, промислове шпигунство починає серйозно загрожувати національним інтересам найпотужнішої країни світу. Не дивно, що США, де витрати на технологічні розробки й дослідження сягають астрономічної суми $600 млрд. є основним об'єктом міжнародного корпоративного шпигунства.

ФБР вважає, що в промисловому шпигунстві проти США беруть участь урядові секретні служби багатьох країн, в тому числі й колишніх союзників та партнерів. Під час слухання в конгресі в травні 2002 р. представники цього агентства, на яке покладено функції протидії корпоративному шпигунству ззовні, оголосило список 23 країн, де ця діяльність здійснюється державними розвідувальними службами. В цьому списку Ізраїль, Англія, Німеччина, Франція, Росія та ін.

Американська спілка індустріальної безпеки щорічно відмічає зростання кількості великих американських корпорацій, щодо яких здійснювалися акти шпигунства. Найбільш привабливими виявилися секрети IBM (комп'ютери), Coming Inc. (спеціальне покриття, оптика, напівпровідники), Honeywell Corp. (авіакосмічне обладнання), Eastman - Kodak (фотообладнання, в тому числі і для аерокосмічного знімання), АТТ (зв'язок), General Electric (електротехніка).

Аналітики Агентства національної безпеки США були шоковані коли їм вдалося дешифрувати й перевести перехоплені повідомлення, призначені для Токіо, з вашингтонського офісу корпорації "Міцубісі": вони містили щоденне аналітичне зведення ЦРУ, призначене для президента США і членів Ради

національної безпеки. За кілька років до цього працівники корпорації "Хітаті" змогли проникнути в IBM, передавши викрадену інформацію через японське консульство в Сан-Франциско.

З'ясуємо фактори активного розвитку промислового шпигунства:

1. У передових країнах світу фундаментальна наука дедалі тісніше зростається з великим бізнесом. В результаті виникла цікава ситуація: інвесторам стало економічно вигідніше вкладати кошти не в саму інноваційну діяльність, а в інфраструктуру з добування інформації про неї.

2. Із настанням епохи комп'ютеризації провідне місце у шпигунському бізнесі посіли фахівці з ЕОМ або, як їх інакше називають, агенти-цифровики. Вони належать до нової еліти злочинного світу і е більшою небезпекою, ніж вуличні й залізничні грабіжники, оскільки можуть одним ударом довести до банкрутства фірму, завдати шкоди будь-якій галузі промисловості або навіть цілій країні. Ідеальним полем діяльності для комп'ютерних шахраїв є те, що нині численні фірми об'єднані одною комп'ютерною установкою. Ця установка дає можливість зібрати дані в єдиний центр. Підключитися до такого центру без проблем може будь-який комп'ютерний хакер. Таким чином він може не тільки отримати секретну інформацію, а й вивести з ладу всю систему за допомогою вірусів. Прикладом може слугувати історія із західнонімецькою фірмою "Шмідт унд фольке", яка займалася розробкою корисних родовищ на дні моря. Завдяки роботі хакера було викрадене не тільки точне географічне положення району дослідження, а й найцінніший секрет - метод пошуку цих родовищ. Після оброблення цієї інформації вона була продана конкуруючій фірмі, яка зекономила на цьому великі кошти, а фірма "Шмідт унд фольке" зазнала великих втрат. Або, наприклад, загальна система паспортизації ЄДАПС, яка об'єднує у своєму банку даних паспортні дані всього населення країни, чи система податкової служби з присвоєння ідентифікаційних номерів, матеріали баз даних яких часто з'являються на чорному ринку.

Останнім часом уряди деяких держав прийняли нормативно-правові акти, згідно з якими діяльність комп'ютерних хакерів карається законом. Але незважаючи на це, багато комп'ютерних злочинів так і залишаються нерозкритими.

Економічні ризики ще досить високі. Якщо раніше для шахрайських дій у сфері підприємництва були характерні досить очевидні й примітивні способи обману, то нині вони стали складнішими й витонченішими.

Часто, незважаючи на оптимістичні прогнози, стійкий і динамічний розвиток бізнесу, через кілька років підприємство опиняється перед загрозою банкрутства, виникає потреби в його додатковому фінансуванні. До таких втрат призводить незадовільне керівництво, слабка кадрова політика і брак досвіду в цій сфері діяльності. Проте глибше вивчення ситуації показує, що насправді використовується витончена схема шахрайства, здійснюється розкрадання грошових коштів.

Крім того, незважаючи на збільшення доступу до вітчизняної і зарубіжної преси, дуже важко знайти інформацію, що заслуговує на довіру. Упередження й

помилкова інформація дуже поширені. Тільки наявність достовірної інформації про партнерів дає змогу компаніям уникнути багатьох неприємностей і забезпечити належний рівень своєї економічної безпеки.

Потрібно розмежовувати поняття "розвідка" й "контррозвідка". Розвідка - це добування й забезпечення інформаційних потоків, а контррозвідка - контроль за інформаційними потоками та можливими шляхами витоку інформації. Економічна контррозвідка - системне явище, яке включене в загальну службу безпеки. В її завдання входять збирання, систематизація і захист безпосередньо інсайдерської інформації оперативно-комерційного характеру, оскільки така інформація є важливою і за незначного обсягу, випереджає реальні події і цінна тим, що на її основі можна робити прогнози на майбутнє з високою точністю.

Однак економічна розвідка й контррозвідка підпорядковані службі безпеки, яка діє в обмежених напрямах, не дозволяє називати себе діловою або конкурентною розвідкою. Це по суті інформаційно-аналітичний відділ служби безпеки. А основне завдання ділової розвідки не виконується: не розробляються і не приймаються стратегічно важливі управлінські рішення в компаніях.

Коли йдеться про конкурентну розвідку, то це не лише дослідження ринку, бажання дізнатися про обсяги продажу конкурентів, а й (у цьому відмінність від інформаційно-аналітичної роботи) наскільки швидко керівник конкуруючої фірми здатний приймати рішення, ризикувати. Це вже не просто інформаційно-аналітична робота, а й частково розвідувальна. Тут можуть застосовуватись методи "інформаційної провокації", наприклад публікація статті й "відстежування конкурента".

Організовуючи відділ ділової розвідки, слід враховувати, що його діяльність є легальною, але таємною, тому важливо приховувати від конкурентів і партнерів інформацію про цей вид діяльності, її методи і засоби.

Працівники служби ділової розвідки підприємства спеціальними методами й заходами мають виявляти загрози, розробляти методи запобігання їм та усунення їх, рекомендувати акції щодо їх нейтралізації. Останнім часом посилено розвивається новий напрям діяльності, в основі якого зафіксовано кінцевий результат - "виконану функцію". Він пов'язаний із "психо-інжинірінгом" - управлінням колективною свідомістю.

Не слід зосереджувати увагу на грі слів "конкурентна розвідка", "ділова розвідка". Перша думка, що виникає під час аналізу словосполучення "конкурентна розвідка" стосовно збирання розвідувальних даних про конкурентів - оманлива. Безперечно, йдеться про досягнення переваг у конкурентній боротьбі, що підтверджує вживання поняття "конкурентна", однак заміна цього терміна на вже відомий термін "ділова" знімає всі сумніви. А одночасне вживання терміна "бізнес-розвідка" поряд із синонімом "ділова розвідка" жодних сумнівів не викличе.

Отже, конкурентна розвідка - це вузький напрям ділової розвідки, який відповідає основній меті: побудові системи взаємовідносин з конкурентами, тобто створенню комплексу заходів щодо отримання та опрацювання даних про

конкурента, а також про його оперативні та стратегічні плани. Ділова розвідка - це легальний вид діяльності, який належить до поняття добросовісної конкуренції. Тому такі методи в рамках business intelligence зазвичай не використовуються. Цим ділова розвідка відрізняється від промислового шпигунства.

Зважаючи на це визначення, можна стверджувати:

- ділова (корпоративна) розвідка є таким інструментом менеджменту, який забезпечує менеджерів актуальною, спеціально зорієнтованою на прийняття управлінських рішень інформацією про стан внутрішнього і зовнішнього середовищ компанії;
- конкурентна розвідка - це збирання і обробка інформації легальними методами і способами, при використанні яких явища й тенденції дослідження інформації вивчають з огляду на конкуренцію та конкурентну боротьбу.

Таким чином, ринок, крім внутрішнього опрацювання проблем, вимагає сил і коштів для розвідки, збирання та опрацювання численних джерел зовнішньої інформації. Нині написано багато книг і статей, придумано багато термінів. Спробуємо з'ясувати, що означають і як застосовуються ці терміни.

Діяльність, пов'язана з одержанням інформації будь-якого характеру за використання технічних засобів, методів агентурного втручання, є протизаконним видом добування інформації і застосовується лише відповідними службами за наявності чинних документів.

Зважаючи на базове значення поняття "розвідки", визначимо терміни маркетингова, конкурентна і ділова корпоративна розвідки.

Маркетингова розвідка - поняття широке: "маркетинг" означає не тільки вивчення конкурентів, а й просування продукту з початкової стадії розроблення до продажу, рекламу, ціноутворення.

Конкурентна розвідка (competitive intelligence) - вузький напрям ділової розвідки, який відповідає основній меті: побудові системи взаємин з конкурентами, тобто створенню комплексу заходів щодо отримання й оброблення даних про конкурента: про його майнові, фінансові та управлінські ресурси, можливості, вразливість, а також про оперативні та стратегічні плани. Конкурентна розвідка, на відміну від розвідки на користь держави, проводиться на користь бізнесу і тільки бізнесу.

Під діловою (корпоративною) розвідкою (у перекладі з англ.-business corporate intelligence) розуміють збирання та аналіз відомостей про партнерів і конкурентів. Мета ділової розвідки виявити реальний стан справ у корпораціях, сильні й слабкі сторони їх бізнесу.

Діловою (корпоративною) розвідкою займаються банки, інвестиційні, аудиторські, дослідницькі, консалтингові компанії, рейтингові агентства. Одні роблять це на користь власного бізнесу, інші - за завданням клієнтів. Фактично будь-яке маркетингове дослідження містить елементи ділової розвідки.

Зазначимо, що у сфері інформаційних технологій термін business intelligence був введений в обіг Говардом Дреснером в 1989 р. для позначення

набору концепцій і методик підвищення ефективності ухвалення бізнес-рішень за допомогою фактографічних інформаційних систем, тобто має дещо відмінне значення. У цій сфері ділова розвідка визначається як широка категорія технологій, пов'язаних зі збиранням, зберіганням, аналізом і забезпеченням доступу до інформації з мстою ухвалення оптимальних ділових рішень. У цьому разі таке явище, як ділова розвідка, безпосередньо не стосується забезпечення економічної безпеки.

Порівнюючи та аналізуючи конкурентну і ділову розвідку країн Заходу, можна говорити, що перша - спрямована на дослідження мікрооточення, тобто внутрішнього оточення конкретної організації, та макрооточення крізь призму конкуренції; друга - віддає перевагу макрооточенню. Отже, розуміння необхідності аналізу зовнішнього середовища як єдиного цілого спричинило розмивання меж між цими поняттями.

Для виживання підприємства в умовах конкурентної боротьби першочергову роль відіграє розвідка намірів конкурентів, вивчення основних тенденцій бізнесу, аналіз можливих ризиків.

Методів ділової (корпоративної) розвідки дуже багато. Людина, не ознайомлена з ними, уявляє їх як заборонені. Проте базові методи ґрунтуються на логіці і збиранні легальних даних. А ось методи збирання інформації різняться кардинально: це і діалог із працівниками фірми конкурента, і бесіда по телефону з менеджерами, і резюме працівників, і Інтернет. Частина методів ґрунтується на спостереженні, яке широко використовують у дослідженні конкурентів.

Використання методів і технологій розвідки дає змогу успішно здійснювати прогноз кризових явищ у бізнесі, тобто реалізовувати функцію превентивного запобігання кризі. Така ситуація дає змогу вжити запобіжних ходів і знизити вірогідність настання кризи, локалізувати або зменшити можливі збитки. Крім того, поінформованість щодо майбутньої кризи може бути використана для зміцнення свого становища або послаблення конкурента.

Нині роль ефективно організованої ділової розвідки посилюється. Труднощі полягають у правильному усвідомленні не тільки зовнішніх обставин, а й внутрішнього середовища компанії. Не є таємницею, що доволі часто менеджери, бажаючи показати свою діяльність у кращому світлі перед вищим керівництвом або власниками підприємства, а інколи й просто прикриваючи свої помилки, спотворюють або фальсифікують інформацію, яка надходить в управлінські структури. Це призводить до ухвалення неоптимальних рішень, які можуть завдати збитків бізнесу. Завданням ділової розвідки є перевірка інформації і запобігання подібним ситуаціям.

Збирання й опрацювання актуальної та достовірної інформації обновлює інформаційні ресурси, а отже, виникає потреба в сучасних технічних засобах і наявності програмного забезпечення, яке дасть змогу не лише збирати і зберігати дані з різних джерел, а й вести пошук по інформаційних масивах, використовуючи різні критерії. Для адекватного опрацювання отриманих даних і формування обґрунтованих висновків та прогнозів потрібні

висококваліфіковані фахівці-аналітики.

Оскільки найважливішим у діяльності служб економічної безпеки стає прогнозування, то основну роль відіграє аналітична робота. Більшість бізнесменів вважають, що інформаційно-аналітична робота - дороге задоволення. Однак аналіз інформації здійснюють, навіть якщо він не входить у бізнес-процеси. Адже важко знайти ділову людину, яка б не цікавилася новинами і не перечитувала пресу, не стежила за новинами. А от це заняття, що проводиться сист

5. ОСОБЛИВОСТІ ДІЛОВОЇ (КОРПОРАТИВНОЇ) РОЗВІДКИ ЇЇ РОЛЬ У БІЗНЕСІ.

Поняття "ділова (корпоративна) розвідка" (Д(К)Р) увійшло до українського лексикону порівняно недавно. У період боротьби із "загниваючим" імперіалізмом за кордоном цей процес називали негативно забарвленим словосполученням "промислове шпигунство". Однак це не заважало нашій державі давати завдання звичайній розвідці і за тими крихтами інформації, яку вона здобувала, ставити перед інститутами й окремими ученими завдання, які сьогодні вирішує ділова (корпоративна) розвідка.

Фактично Д(К)Р забезпечує керівництво підприємства інформацією, необхідною для превентивного ухвалення рішень. Це збирання інформації, її класифікація (за вагомістю, рівнем вірогідності, напрямком застосування і т.д.), аналіз, прогноз розвитку ситуації, підготовка рекомендацій керівництву. Розрізняють стратегічну Д(К)Р і оперативну .

Служба Д(К)Р залежно від масштабу підприємства може складатися з одного штатного працівника, а може бути великим і розгалуженим підрозділом. У практичній діяльності до процесу Д(К)Р залучається багато працівників підприємства, що не мають прямого адміністративного зв'язку з цим підрозділом.

Завдання стратегічної Д(К)Р за змістом близькі до завдань стратегічного планування і маркетингу і зводяться до визначення структури й динаміки тієї сфери господарсько-економічної діяльності, в якій працює (або збирається працювати) підприємство, з виявленням і аналізом усіх конкурентів і контрагентів у цій сфері діяльності.

Оперативна Д(К)Р вирішує гострі завдання негативної взаємодії з конкретним конкурентом і часто діє на межі етично та юридично установлених норм і засобів. Оскільки йдеться про цільову функцію створення труднощів або перешкод конкурентові, то всі ці завдання ставляться з явним акцентом на пошук слабких місць у діяльності конкурента.

Джерела інформації, цінної для вирішення завдань Д(К)Р, численні й різноманітні. Навіть поверхневий огляд дає змогу виявити, що для оперативної Д(К)Р, де потрібна інформація (зокрема, негативна), ретельно приховується й не афішується ні в ЗМІ, ні в ділових чи інших друкованих матеріалах. Основними джерелами інформації здебільшого є люди, а саме міжособистісне

спілкування, переважно неофіційне, працівниками конкурента.

Водночас для стратегічної Д(К)Р плідна і цікава інформація є в загальнодоступних джерелах. Вона не тільки не приховується, а навпаки, рекламується, організовується і подається у вигляді різних баз даних, довідників, оглядів, наукових статей, публіцистики тощо. Моніторинг згадок про підприємство чи про конкурентів у ЗМІ дає низку можливостей для ділової (корпоративної) розвідки.

Якщо вам потрібно оцінити доцільність нового бізнес-проекту, надійність партнерів, серйозність намірів конкурентів, інформація має бути максимально повною. Як відомо, хто володіє інформацією, той править світом. Проте самостійно і швидко знайти потрібні відомості не так просто. Тому і з'явилися фірми, що спеціалізуються на пошуку бізнес-інформації.

Коли варто звертатися до послуг бізнес-розвідників? Нині в Україні, за прикладом "старшого брата", почали досить активно працювати компанії, що займаються бізнес-розвідкою. Тому важливо зрозуміти, в яких випадках і які послуги цих фірм можуть знадобитися саме вам.

У компанії з'являються нові стратегічні завдання, які потрібно оцінити. Це може бути купівля контрольного пакету акцій або значної його частки незнайомою для інвестора компанією із стратегічною метою, поява нових партнерів або сумісне ведення бізнесу.

Отже, вирішення конкретного завдання Д(К)Р можна подати як тристадійний процес, зображений у табл. 10.2.

Таблиця 10.2.

Процес вирішення конкретного завдання Д(К)Р

Етап	Завдання	Дія
1	1.1. Визначення потреби в інформації	Систематизація запитань
	1.2. Організація ресурсів для збирання інформації	Систематизація джерел інформації
		Збирання інформації
2	2.1. Опрацювання й оцінювання інформації	Класифікація інформації
		Систематизація інформації
	2.2. Аналіз інформації і складання висновків	Генерація вторинної (узагальнюючої) інформації
3	3.1. Передавання інформації особам, що ухвалюють рішення	Забезпечення оперативного зворотного зв'язку із замовником
	3.2. Адресний розподіл інформації між підрозділами	Систематизація адресатів. Забезпечення конфіденційності

Великі розвідники типу Ріхарда Зорге свого часу вирішували всі питання перших двох етапів Д(К)Р поодинці, причому в умовах, які навіть віддалено не нагадують те, що ми маємо нині, ні за кількістю джерел інформації, ні за засобами пошуку цієї інформації, ні за засобами її опрацювання та аналізу, ні за умовами власної роботи. У 1980-і роки робочі групи, створювані ВПК, при ЦК

КПРС працювали в інших умовах, але методи "ручного" опрацювання інформації на той час ще не зазнали практично ніяких змін. А ці методи в умовах не дуже конспіративної діяльності кожної такої групи і достатньо серйозних прав, делегованих групі владою, зводилися до добровільно-примусового залучення до роботи провідних фахівців і керівників, директивної організації закритих або напівзакритих нарад, семінарів, експериментальних програм аж до колективного вироблення думок і рекомендацій кворумом провідних фахівців країни з виокремленої проблеми.

Якщо розглядати не загальнодержавний рівень, а звичайне ЗАТ із сотнею працівників, то за правильної організації роботи служба Д(К)Р є міні-копією описаної вище ситуації: завдання від групи Д(К)Р може отримати будь-який працівник, аж до президента або директора фірми. Адже бувають ситуації, коли потрібна інформація може бути добута з джерела, доступ до якого має тільки президент фірми чи директор.

Досвід останніх років показав, проте, що стратегічні завдання Д(К)Р цілком можна вирішувати, не залучаючи до розвідувальної діяльності багато працівників і не користуючись ніякими закритими джерелами інформації.

О. Солженіцин написав вибухонебезпечний на той час "Архіпелаг ГУЛАГ" за матеріалами загальнодоступних джерел, якщо не враховувати численні особисті листи колишніх в'язнів. У відомих усім книгах Віктора Суворова (Резуна) як докази використано низку фактів, масу відкритих документів і матеріалів, які й донині не спростовані.

Тому й не дивно, що не в такі вже й далекі часи газету "Правда" не видавали в бібліотеках читачам без спеціального дозволу відповідних органів. Або згадаймо скандальні судові справи Пасько, Нікітіна та інших, коли з десяти нібито кримінальних шпигунських епізодів дев'ять "лопалися" в суді через те, що інформація, використана підсудними, була взята із загальнодоступних джерел. Тому слід чітко знати, на що націлювати розвідку.

Отже, в умовах інформаційного простору приховати щось державі чи окремій фірмі стає дедалі важче, як би ретельно не приховувалися певні факти, особливо коли вони стосуються фінансово-господарської діяльності. Сліди їх або супутніх з ними подій настільки численні й різноманітні, що навіть за відкритими джерелами інформації можна виявити ці факти.

Інформації про супутні події так багато, що перед службою Д(К)Р постає проблема її надміру, тобто високого відсотка інформаційного "непотребу", особливо завдяки розвитку Інтернет. Навіть те, що Україна більше за Росію (не враховуючи західних сусідів) відстає в "інтернетизації" своєї фінансово-господарської діяльності, економічного та політичного життя, обсяги інформації на сайтах "Українська ПРАВДА", "УРА-Информ", УНІАН, Forum, "І нтерфакс-Україна", "Українські новини" та в російському "Рунеті" є безмежними. І не використовувати ці канали інформації є серйозним упущенням служби Д(К)Р будь-якого підприємства.

Аналіз свідчить, що у відкритому Інтернеті доступні всі програмні продукти, необхідні для створення повного життєвого циклу комп'ютерної

підтримки служби Д(К)Р.

Враховуючи комп'ютеризацію технологічних процесів щодо отримання, опрацювання та використання необхідної для бізнесу інформації, спробуємо конкретизувати етапи процесу вирішення завдань (табл. 10.2), поставлених перед Д(К)Р з метою визначення частини роботи служби Д(К)Р, яку можна автоматизувати.

Етап 1.1. "Визначення потреби у відомостях"

Систематизація питань - це відповідальне завдання, оскільки визначає вектор, напрям пошуку. Таку важливу роботу мають виконувати відповідальні експерти - працівники, що володіють системним підходом, мають аналітичний склад розуму та професійно знають всі подальші дії служби Д(К)Р .

У результаті формується ієрархічна структура класифікатора тем або питань з попередньою розміткою їх порівняльної значущості. І вже на цьому етапі закладаються основи етапу 2.1. "Систематизація інформації"", тобто система питань будується з урахуванням майбутньої системи відповідей і висновків.

Етап 1.2. "Організація ресурсів для збирання відомостей ", на якому розрізняють кабінетну Д(К)Р й агентурну

Слово "агентурна" не слід розуміти як "шпигунська": агентом у цьому контексті може бути будь-яка людина, що є джерелом усної інформації (сусід в автобусі чи в потягу, учасник застілля чи конференції), будь-який співробітник своєї або чужої фірми, що має у своєму розпорядженні відкрите джерело письмової інформації. На цьому етапі не наголошують на незаконних способах добування інформації, оскільки ці дії виходять за межі компетенції Д(К)Р і підпадають під кримінальну відповідальність та контролюються службами економічної контррозвідки конкурентів.

Кабінетна Д(К)Р за правильної організації вивільняє значну кількість працівників і цим істотно полегшує вирішення завдань третього етапу (пункт 3.1. "Про збереження конфіденційності"). Властивим і характерним для служби Д(К)Р господарюючих суб'єктів є те, що ділова розвідка 95% інформації черпає з відкритих джерел. 4% - із напівофіційних і лише 1% - із секретних джерел. А з урахуванням "інтернетизації" суспільства виявляється і такий чинник: чим більші завдання ставляться перед Д(К)Р, тим більша частина необхідної інформації доступна через Інтернет.

Ці серйозні завдання і є переходом від ручного пошуку необхідної інформації до комп'ютерного. Комп'ютер читає тексти в сотні мільйонів разів швидше за людину, проте, аби він не тільки читав, а й аналізував суть прочитаного і відбирав тільки те, що людині потрібне, людина має пояснити комп'ютеру, що вона хоче і що потрібно шукати. Це пояснення має бути мовою, зрозумілою для комп'ютера. Тобто має бути створена не лише програма, а ціла експертна система, яка як експерт має проаналізувати отриману інформацію. Експертна система - це програма, що поводиться подібно до експерта в деякій, звичайно вузькій прикладній сфері. Типові застосування експертних систем передбачають такі завдання, як медична діагностика, інформаційний пошук та

аналіз, локалізація несправностей в устаткуванні й інтерпретація результатів вимірювань.

Експертні системи (ЕС) мають вирішувати завдання, що потребують експертних знань у певній сфері. У тій чи іншій формі експертні системи повинні мати ці знання. Тому їх також називають системами, заснованими на знаннях. Проте не кожну систему, засновану на знаннях, можна розглядати як експертну. Експертна система повинна також уміти певним чином пояснювати свою поведінку і свої рішення користувачеві, так само, як це робить експерт-людина. Це особливо важливо у сферах, для яких характерна невизначеність, неточність інформації (наприклад, у діловій розвідці, медицині). У цих випадках здатність до пояснення потрібна для того, щоб підвищити ступінь довіри користувача до порад системи, а також для того, щоб дати можливість користувачеві знайти можливий дефект у міркуваннях системи. У зв'язку з цим в експертних системах варто передбачати дружню взаємодію з користувачем, що робить для користувача процес міркування системи "прозорим". Часто до експертних систем ставлять додаткову вимогу - здатність мати справу з невизначеністю і повнотою. Інформація про поставлене завдання може бути неповною чи ненадійною; стосунки між об'єктами предметної сфери можуть бути наближеними. Тоді в усіх цих випадках потрібні міркування з використанням імовірнісного підходу. У найзагальнішому випадку для побудови експертної системи має бути розроблений механізм виконання таких функцій системи:

- вирішення завдань з використанням знань про конкретну предметну сферу, при цьому виникне необхідність мати справу з невизначеністю;
- взаємодія з користувачем, у тому числі пояснення намірів і рішень системи під час і після закінчення процесу вирішення завдання.

Кожна із цих функцій може виявитися дуже складною і залежатиме від прикладної сфери, а також від різних практичних вимог. У процесі розроблення і реалізації можуть виникати різні важкі проблеми, тому у складі Д(К)Р має бути спеціаліст із комп'ютерної техніки.

Мета досліджень з ЕС полягає в розробленні програм, які під час вирішення завдань, важких для експерта-людини, отримують результати, що не поступаються за якістю та ефективністю рішенням, що подані експертом.

Експертна система - це програмний засіб, який використовує знання експертів для високоефективного наочного розв'язання завдань, що цікавлять користувача. Вона називається системою, а не просто програмою, оскільки містить основи знань, "вирішування" проблеми і компонент підтримки. Останній допомагає користувачеві взаємодіяти з основною програмою.

Експерт - це людина, що здатна чітко виражати свої думки і користується репутацією фахівця, вміє знаходити правильні рішення проблем у конкретній предметній сфері. Експерт використовує свої прийоми і знання, щоб зробити пошук рішення ефективнішим, і ЕС моделює всі його стратегії.

Інженер знань - людина, що має знання з інформатики і штучного інтелекту, знає, як треба будувати ЕС. Інженер знань опитує експертів, групує

знання, вирішує, як вони повинні бути подані в ЕС, і може допомогти програмістові у написанні програм.

Засіб побудови ЕС - це програмний засіб, який використовує інженер знань або програміст для побудови ЕС. Цей інструмент відрізняється від звичайних мов програмування тим, що забезпечує зручні способи подання складних високорівневих понять.

Користувач - людина, яка використовує вже побудовану ЕС. Так, користувачем може бути юрист, що використовує її для кваліфікації конкретного випадку; студент, якому ЕС допомагає вивчати інформатику; начальник служби ділової розвідки, який на основі проаналізованого матеріалу складає прогнозовані перспективні плани чи визначає можливі напрями усунення ризиків та їх причин тощо. Термін "користувач" дещо неоднозначний. Зазвичай він позначає кінцевого користувача. Проте користувачем може бути:

- творець інструменту, що відлагоджує засіб побудови ЕС;
- інженер знань, що уточнює, чи є в ЕС знання;
- експерт, що додає системі нових знань;
- клерк, котрий заносить у систему поточну інформацію;
- власник бізнесу;
- керівник служби безпеки компанії;
- менеджер з безпеки;
- начальник служби ділової розвідки.

Важливо розрізняти інструмент, який використовують для побудови ЕС, і саму ЕС. Інструмент побудови ЕС охоплює як мову, використовувану для доступу до знань, що містяться в системі, так і їх подання, а також підтримують засоби - програми, які допомагають користувачам взаємодіяти з компонентами експертної системи, вирішуючи проблему.

Процедура "спілкування з комп'ютером" - це "складання пошукового залиту". Існує багато баз даних, які є і так званими "пошуковими машинами" зі своєю унікальною "мовою запитів". За обсягом українсько - та російськомовного матеріалу, що зберігається в базі, лідерами є три російські ("Індекс", "Рамблер", "Апорт") та одна світова ("AltaVista та Google") пошукові машини, що розуміють українську та російську мови. Щодо англомовних текстів, то для їх розшуку в Інтернеті функціонують десятки загальносвітових пошукових машин і багато регіональних та локальних систем.

Зі світових пошукових машин Google має, мабуть, найбільший обсяг даних і найрозвиненішу мову запитів, що припускає побудову складних запитів із використанням усіх основних логічних операторів. Насправді граматика й синтаксис будь-якої мови запитів набагато примітивніші від будь-якої із живих мов, тому навчитися писати запити, дотримуючи тих 7-10 правил, якими описується ця мова, зовсім нескладно.

Якщо запит написаний і справді адекватно відображує потребу в інформації, то подальшу роботу з її збирання вже можна спокійно доручити так званому "пошуковому роботові" - комп'ютерній програмі, яка із заданим ступенем регулярності опитує сервер пошукової машини щодо наявності свіжої

інформації за вказаним запитом, отримує цю свіжу інформацію і (один з варіантів) накопичує її у вашій електронній поштовій скриньці.

Отже, між етапами 1.1 і 2.1 є найбільш трудомісткий етап збирання інформації, і саме цей етап можна майже повністю покласти на безлюдну технологію комп'ютерного пошуку, причому одночасно з етапом 2.2 "Опрацювання та оцінювання інформації".

Оглядаючи сотні мільйонів текстів, "пошукові роботи" можуть завалити групу аналізу служби Д(К)Р (адже комп'ютер - це інструмент для аналітика, а не замість аналітика) сотнями й тисячами текстів. Щоб цього не сталося, доцільно заздалегідь провести досить тонку роботу зі складання, зіставлення та стикування трьох класифікаторів:

- класифікатора запитань (етап 1.1);
- класифікатора тем відібраної інформації;
- класифікатора персоналу, для якого працює служба Д(К)Р.

Поки що складається враження, що ця робота схожа на мистецтво, алгоритмізації не піддається і для кожного завдання виконується вручну методом послідовних наближень. Головна складність в тому, що результат її має бути зрозумілим не тільки людині, а й комп'ютеру, тобто має бути закладеним в експертну систему. Лише тоді розширений потік відібраної інформації автоматично розділятиметься на безліч спеціалізованих потоків і осередків класифікаторів так. що на наступних етапах робота значно полегшиться.

Результати роботи агентурної Д(К)Р вводяться в базу даних окремо. Тому неважко ввести цей маленький, але унікальний потік інформації у вигляді текстів в основний потік, а аналіз та автоматична розкладка цих текстових блоків у класифікатор нічим не відрізняються від того, що вже описано для інформації з Інтернет.

Етап 2.2. "Аналіз інформації і складання висновків "

За визначенням не можна повністю довіряти комп'ютеру хоч би тому, що відповідальність за неправильний висновок на нього не покладеш. Тим більше, керуючись правилами захисту інформації; ні рекомендації, ні висновки, ні заходи краще в комп'ютерну систему не вводити. Розрахунок достовірності того чи іншого факту можна певною мірою автоматизувати, якщо заздалегідь кожне джерело інформації (або хоч би частина цих джерел) забезпечити якимось коефіцієнтом довіри, а оцінюючи достовірність факту, посилання на який є в кількох документах, автоматично розраховувати підсумковий коефіцієнт довіри.

Етап 3.1 і частина етапу 3.2 автоматизуються так само, як і **етап 2.1.** Якщо кожна тема буде зіставлена з відповідними підрозділами або працівниками, то можна автоматично реалізувати принцип, яким керуються спецслужби: кожен повинен знати ту й лише ту інформацію, яка потрібна йому для його роботи.

Інша частина етапу 3.2 "Збереження конфіденційності відомостей" дотична із завданнями симетричної служби - служби економічної

контррозвідки.

Для полегшення завдань служби Д(К)Р в сучасних умовах можна використовувати:

- класифікатор цілей (запитів, тем, напрямів пошуку);
- групу пошукових роботів (в Інтернеті - основними європейськими мовами);
- програму автоматичного розкладання інформації в класифікатори;
- класифікатор працівників і підрозділів;
- програму автоматичного розподілу інформації за користувачами;
- інтерактивний довідник з тем, що ґрунтується на зібраній за весь час інформації.

Можна зробити висновок, що всі конкретні банкрутства (крім викликаних стихійним лихом: буревієм, повінню, виверженням вулкана або землетрусом) пов'язані з незнанням зовнішнього середовища і поганою роботою служби Д(К)Р.

Роль ділової (корпоративної) розвідки у бізнесі

Реалії сучасного ділового світу такі, що багато бізнесменів розуміють, що без глибокого аналізу інформації, яка нині заполонила весь світовий ринок, неможливе успішне ведення бізнесу. Потоки інформації, що генеруються учасниками ділової активності, за її кваліфікованого опрацювання, аналізу та синтезу висновків здатні озброїти компанію конкурентними перевагами стосовно інших гравців ринку, які своєчасно не володіють потрібною інформацією.

Ділова (корпоративна) розвідка не пов'язана з великими витратами, але при цьому надає переваги, які не може забезпечити будь-який інший структурний підрозділ компанії. Ділова розвідка не повторює роботи інших структур із меншою собівартістю, а дає можливість отримувати дані, які в принципі неможливо отримати інакше.

У будь-якому бізнесі та за різних умов кожен власник перш ніж робити грошові заощадження у створення, розвиток чи зміну профілю бізнесу, вибирати партнерів чи співвласників, має активно зібрати інформацію для прийняття рішення і лише після її аналізу робити висновок. Відійшли в минуле часи, коли від вкладення капіталу отримували 200-500% прибутків, адже практично всі сектори ринку освоєно. Через це в умовах прогресуючих ринкових відносин треба шукати ніші через чітко побудовану й випробувану часом структуру ділової (корпоративної) розвідки, отримуючи дані про:

- ринки збуту;
- конкурентів;
- партнерів;
- продукцію і послуги;
- контрагентів;
- нові технології;
- проекти законодавчих актів;

- політичні події в країні і світі.

Ринок ділової розвідки в Україні лише формується, набуває структурованого й цивілізованого характеру. Адже незалежно від капіталів підприємства, його обсягів та перспективності для виходу на ринок конкретного регіону (гірничий Донбас, аграрне Закарпаття) потрібне чітке визначення та інформаційне опрацювання перед вкладанням коштів чи матеріальних активів.

Ділову розвідку підприємства треба порівнювати з іншою діловою розвідкою та за кінцевим результатом - з положенням компанії на ринку, а не з іншими підрозділами.

Звідси часткове, епізодичне заняття діловою чи її складовою - конкурентною розвідкою дає результат, набагато скромніший, ніж якщо займатися нею систематично. Щоденне методичне виконання розвідувальної діяльності дає змогу досягти серйозних переваг над конкурентами.

Саме ці переваги можемо сформулювати, взявши за основу напрацювання Ларрі Каханера (Капапег, 1997), який створив класичний перелік ключових питань, що став головним у цій сфері, та досвід вітчизняного, російського і зарубіжного бізнесу.

Розглянемо конкретно кожну із переваг Д(К)Р.

Основні переваги компанії, що має сильну структуру ділової (корпоративної) розвідки:

1. **Прогнозування змін на ринку.**

Компанія маг постійно проводити моніторинг середовища, в якому вона працює, тоді зрідка виникають непередбачувані несподіванки. Зокрема, в Росії через зміну мінімальних нормативів площ на відкриття аптек на ринку медикаментів склалася ситуація, коли власникам бізнесу, у яких термін ліцензії закінчився в цей період або які не встигли відкрити нову аптеку до зміни нормативів, довелось або докуповувати сусідні з ними приміщення, або йти з бізнесу. Передвісниками подібної ситуації були публічно доступні джерела інформації, що дозволяли прогнозувати появу цієї проблеми, вжити заходів захисту бізнесу, але багато хто їх просто не помітив, що й призвело до значних витрат.

2. Прогнозування дій конкурентів і партнерів.

Установлення цін на побутову хімію на певному секторі ринку компанія за допомогою аналізу попиту на продукцію та цін конкурсні їв.

3. Виявлення нових або потенційних конкурентів.

У практиці бувають факти, що в процесі навчання ділової розвідки початківці, що освоюють технології розвідки, виявляють на ринку компанії, невідомі їм, але такі, котрі в майбутньому можуть загрожувати бізнесу як конкуренти. Велику роль у подібному моніторингу відіграють сучасні засоби стеження за новою інформацією в Інтернеті.

4. Можливість використання досвіду інших компаній.

Відома приказка, що "розумний чоловік завжди виведе сім'ю зі скрутного становища, а мудрий чоловік не допустить, щоб сім'я в такому становищі

опинилася", практично є основним принципом лілової (корпоративної) розвідки.

Можливість вчитися на чужих помилках інтуїтивно зрозуміла всім, а копіювання успішних управлінських рішень - тим більше. Мабуть, не знайдеться жодної людини, яка хоча б раз не списувала в школі чи в інституті. Проте тільки ділова (корпоративна) розвідка здатна безкоштовно організувати збирання думок клієнтів про будь-який продукт або швидко проаналізувати судову практику з погляду маркетолога. а не юриста.

5. Відстежування інформації, пов'язаної з патентами і ліцензіями.

Ділова розвідка здатна допомогти фахівцям з патентного законодавства з'ясувати, які напрями діяльності конкурентів відображені в публікаціях, але не захищені патентами. Це нормальна практика, яка має технології, відшліфовані десятиліттями , і може застосовуватися практично в усіх країнах.

Якщо компанія, що має ноу-хау, не змогла або не захотіла їх захистити відповідно до чинного законодавства, то вона не може притягнути до відповідальності тих, хто відтворив виріб або технологію, подібні до її власних зразків.

Після того як перспективні ідеї і напрями виявлені фахівцями з патентного права, проводять експертизу, в процесі якої з'ясовують, що технологія нічим не захищена, проводяться її патентування на своє ім'я. Особливо часто подібна ситуація спостерігається в компаніях, що виходять на світовий ринок, проте підприємства і компанії, які не мають зовнішньоекономічних зв'язків, також можуть піддаватися таким ризикам.

Для прикладу, згадаймо опубліковані в пресі та Інтернеті матеріали, в яких зазначалося, що після початку перебудови в другій половині 1980-х років в радянські бібліотеки, зокрема провінційні, попрямувала велика кількість представників іноземних компаній, іноземних студентів і стажерів. Були перериті підшивки відомих за радянських часів науково-популярних видань для дорослих і молоді, а також місцевих газет, які вважалися "закритими" для іноземців протягом кількох десятиліть. Чимало опублікованих у них ідей радянських учених і креслень пристроїв, схем було запозичено і на законних підставах запатентовано за межами СРСР, Росії, України.

6. Оцінювання доцільності придбання нового бізнесу.

Здебільшого власники бізнесу штучно підвищують вартість компанії для отримання максимального прибутку. Наприклад, фірма з виготовлення керамзито-цементних виробів відкриває кілька цехів в орендованому приміщенні для виготовлення тротуарної плитки, черепиці, керамзитоблоків, водовідведень тощо, покриваючи видатки за рахунок іншого бізнесу компанії. Тобто створюється імідж перспективної компанії. І лише придбавши бізнес, не маючи умов для прогресивного випуску продукції через слабку автоматизацію процесів, відсутність ринків збуту, зростання цін на оренду, новий власник скорочує виробництво, а часом і покидає придбану сферу бізнесу.

Зрозуміло, що перед купівлею бізнесу треба перевірити всі ці дані. Зазвичай із таким завданням міг впоратися і сам власник без ділової розвідки,

проте ділова розвідка може дати відповіді на потрібні запитання значно простіше, ніж хтось інший, оскільки володіє всіма необхідними для цього інструментами.

7. Відкриття чи створення нового бізнесу.

Ця стадія діяльності компанії співзвучна з попереднім етапом і якоюсь мірою подібна до етапу "Можливість використання досвіду інших компаній", однак ширша, оскільки дає змогу не лише визначити досвід окремих компаній, а й стан ринку загалом, зробити аналіз конкурентоспроможності секторів ринку.

Інколи для створення нового бізнесу достатньо вивчити особливості діяльності своїх колег, розпочати справу під їхнім чітким керівництвом і бізнес запрацює на вас. А інколи бізнес просто не йде. Наприклад, фізична особа здає власний автомобіль в оренду під таксі іншій людині, на яку оформляє ліцензію, купує рацію, таксолічильник, оплачує страхування автотранспорту та його технічний огляд, сплачує податок, тобто вкладає значну суму власних заощаджень. Однак через низку непередбачених чинників (недобросовісність партнера, постійна експлуатація транспортного засобу без профілактичних ремонтів, несвоєчасність розрахунків з орендарем тощо) бізнес не виправдовує намірів і стає збитковим. Як результат - фактично "добитий" транспортний засіб, витрати на капітальний ремонт, непотрібна власникові амуніція такс і,тобто матеріальні й моральні збитки.

Не менш важливим є виявлення "підводних каменів", які є практично в кожному бізнесі. Краще вчасно відмовитися від відкриття бізнесу, ніж вкласти в нього кошти і потім "мінімізувати збитки". Якщо при започаткуванні нового бізнесу ви не бачите конкурентів, то це означає, що ви - майже Білл Гейтс або просто чогось недооцінили, не прорахували чи занадто самовпевнені.

Саме ділова (корпоративна) розвідка здатна допомогти у виявленні "підводних каменів" та організації прибуткового бізнесу.

Здебільшого успіх будь-якого бізнесу залежить від:

- якості матеріалів і сировини, які використовують у виробництві;
- вміло підібраного кваліфікованого складу компанії;
- стилю керівництва та сформованого інформаційно-аналітичного кістяка колективу;
- автоматизації технологічних процесів та сильної маркетингової і розвідувальної систем.

8. Вивчений політичних, законодавчих або регуляторних змін, які можуть вплинути на бізнес.

Згадаймо період, коли в Україні було прийнято законодавчі документи, що забороняли ввезення м'яса і курей з-за кордону. Фірми, які знали про прийняття цих нормативних документів про заборону, цілими фурами завозили м'ясні продукти в холодильні сховища, підвищили ціни та витіснили з ринку не лише дрібних конкурентів, а й виробників вітчизняного продукту.

Пріоритетом стратегічної розвідки є моніторинг політики, оскільки політика, без сумніву, важливіша для ділової (корпоративної) розвідки, ніж

економіка. Політичні рішення впроваджувалися і будуть впроваджуватися в життя незалежно від їх рентабельності, ефективності і витрат грошових коштів на їх впровадження. Тому, щоб не втратити бізнес, потрібно враховувати політичні зміни, тенденції і напрями, прогнозувати і передбачати наслідки політичних подій та інтриг. На основі викладеного вище можна виокремити такі головні завдання ділової (корпоративної) розвідки за політичними аспектами:

- відстежувати законодавчі та адміністративні тенденції в діях влади щодо бізнесу загалом;
- відстежувати лобіюючі зміни в законодавстві, які можуть вплинути на власний бізнес на користь інших бізнес-груп або ваших прямих (непрямих) конкурентів;
- у період передвиборчих кампаній аналізувати позиції реальних претендентів у владні структури в контексті інтересів свого бізнесу. Однак в умовах вітчизняного бізнесу за постійної зміни влади, безкомпромісних дій політиків, постійного лобіювання всіх рівнів не можуть залишатися на рівноцінних позиціях сили, що пробивають собі дорогу до влади. На думку більшості експертів, оптимальною у виборі є та сила, котра давно позитивно зарекомендувала себе, чия ідея реалізована на Заході. Або потрібно робимо ставку на всіх, хто реально претендує на успіх політичних конкурентів (без непотрібної публічної заангажованості) за принципом "хай переможе сильніший";
- збирати й аналізувати інформацію та інформувати керівництво про випадки, коли діяльність компанії чи окремі її напрями починають зачіпати чиїсь політичні інтереси;
- відстежувати дрейф політичних інтересів впливових структур та інформувати керівництво структур про ці факти, особливо якщо підприємство вносило зміни у свою діяльність, а ситуація складається так, що вона починає зачіпати інтереси новосформованих політичних владних структур.

9. Вивчення нових технологій, продуктів і процесів, які можуть вплинути на бізнес.

Це один із пріоритетних напрямів роботи стратегічної ділової розвідки, що потребує розуміння, компетентності та знання специфіки продукту компанії. Моніторинг спеціальних періодичних видань і збірок, наукових доповідей та праць лаг змогу в науковомістких галузях (зокрема, в медицині, електроніці) заощадити значні кошти і час за рахунок використання чужих напрацювань.

Моніторинг останніх розробок у сфері комп'ютерної техніки показує, що плазмові монітори витиснули з виробництва своїх попередників; пристрої USB-флешки витіснили гнучкі дискети, які панували на ринку знімних носіїв інформації більш як десять років.

10. Погляд на свій бізнес очима сторонньої особи.

Люди люблять тиражувати власні успіхи і прогнозувати майбутнє па

власному досвіді. Це нормально для окремої особи чи групи людей в побутовому аспекті, проте для компанії може бути неприйнятним або взагалі згубним.

Часто самовпевнені керівники найбільших компаній, які справді досягли високих результатів, починають вважати себе всесильними й за підтримки своїх підлеглих вважають усі свої рішення єдино правильними. Якщо таким керівникам не вдається оточити себе творчо мислячими працівниками, які є досить сміливими, щоб висловлювати власну думку, то компанія може зазнати краху. Прикладом може слугувати історія втрати компанією Levi Strauss ринку джинсів, на якому вона домінувала тривалий час.

Звідси висновок, що найкрихкішою є саме жорстка структура підприємства. І в структурі будь-якої фірми, і в її підходах до бізнесу і життя загалом має бути закладена гнучкість, що поєднується із спрямованістю на виконання загальних завдань та потреби розвитку бізнесу.

Ділова розвідка за характером своєї роботи має справу з кращими прогресивними рішеннями і відстежує всі новинки як у виробничій сфері, так і у технології управління. Тому вона не має аналогів для оцінки відповідності методів ведення бізнесу реальним вимогам ринкової конкуренції.

11. Перетворення слабких сторін бізнесу на конкурентні переваги.

Прикладом таких перетворень можна вважати відомий трюк компанії з виробництва спортивного одягу, склади якої виявилися затовареними напередодні виходу потужної реклами конкурента, який пропонував аналогічний товар. Через брак коштів для просування своєї продукції компанія почала пропонувати свої вироби на спеціалізованому сайті в Інтернет. Ноу-хау полягало в тому, що фірма зосередилась на термінології, яку конкурент використовував у рекламі своєї продукції.

Споживачі, що користувалися Інтернетом, виявляли інформацію про розрекламовану продукцію аутсайдера, що мала прийнятну ціну, і здійснювали покупки. Отже, за рахунок знання специфіки покупців, а також використовуючи прогалини в роботі конкурента, підприємство фактично за чужий рахунок продало свою продукцію з мінімальними витратами на її просування.

Для довідки: вивчивши ринок і споживачів певного регіону, можна виділити сектори ринку, в яких споживачі користуються Інтернетом чи використовують Інтернет конкуренти, слабкі сторони та прогалини в маркетинговій діяльності конкурента.

12. Виявлення змін і реагування на них раніше за виникнення кризових ситуацій.

Практична ситуація: Компанія-видавець, яка має Інтернет-магазини з продажу літератури, за рахунок моніторингу згадок та публіцистичних статей про себе в Інтернеті, виявила початок інформаційної війни проти себе. На сайтах і форумах почали з'являтися окремі, але пов'язані загальною ідеєю, публікації, що формують негативну суспільну думку про компанію. Якби компанія не мала структури ділової розвідки, котра, відстеживши інформацію,

підготувала звіт керівництву, на основі якого було вжито відповідних заходів, то невідомо, як би розвивався бізнес.

13. Виявлення слабких місці конкурента і недомовок у його рекламі.

Ділова розвідка здатна проаналізувати скарги споживачів на продукт конкурента і на підставі виявлення приховуваних ним недоліків дати рекомендації стосовно своєї реклами, щоб вона підкреслювала саме ті переваги власного продукту, яких продукція конкурента не має.

Практична ситуація: В одного виробника будильників сигнал їх дзвінка здебільшого дуже тихий, але виробник ніколи не зазначає це в рекламі, про це говорять користувачі. Крім того, користувачі стверджують, що ці будильники дорожчі, ніж в інших виробників. Будильники конкурента не вирізняються технічними досягненнями, однак сигнал їх гнучкий і чистий, і ціпа більш доступна. І це спрацьовує.

14. Виявлення потенційних джерел просочування конфіденційної інформації через працівників компанії.

Здебільшого функція захисту не належить до компетенції ділової розвідки, і отримана інформація зазвичай передається службі безпеки.

Практична ситуація: Навіть початківець у діловій розвідці підприємства, який проводить аудит присутності своєї компанії в Інтернеті, виявляє в мережі повідомлення, що містять адреси корпоративної електронної пошти. Там, де служба безпеки не приділяє належної уваги використанню корпоративної пошти в особистих цілях, обсяги присутності співробітників підприємства можна порівняти із присутністю всієї фірми-виготовлювача. Практика свідчить, що ця проблема актуальна навіть для деяких компаній державного рівня. Здебільшого такі повідомленні працівників містять запрошення до знайомства або розповідають про їх хобі, або пропонують купити товари, надати послуги.

Інколи трапляються резюме працівників підприємства нинішніх, або колишніх, що хочуть знайти нове місце роботи. Саме ці резюме є стабільним джерелом інформації, оскільки за їхніми даними можна спланувати і здійснити незаконне залучення цих осіб до співробітництва.

15. Збирання інформації про партнерів і клієнтів.

Крім інформації про наявність кримінальних зв'язків і методи вирішення проблем, прийняті вашими контрагентами, дуже важливо знати, звідки у партнерів гроші. Якщо не зауважити цей факт, то можна випадково стати співучасником відмивання кримінальних грошових коштів або жертвою краху вашого банку. Мабуть, мало приємного для власника бізнесу в тому, що в самий пік укладання угод чи відвантаження товару грошові кошти на рахунках банку з вини вашого партнера або банку потрапляють під арешт.

З викладеного вище можна зробити такий висновок: в епоху науково-технічного прогресу та науково-технічної революції економічно-розвідувальна діяльність є одним із найсучасніших засобів конкурентної боротьби. Ставши невід'ємною частиною бізнесу, вона встановлює диктатуру меншості над більшістю, створює всі умови для функціонування системи загальнонаціонального контролю над економікою, наукою, людьми.

Активне й ефективне ведення економічної інформаційно-аналітичної діяльності має особливе значення для держав, у яких з тих чи інших причин на певний час загальмувався економічний та науково-технічний прогрес. Тому в інтересах зміцнення всіх сфер національної безпеки України було б доцільно мати потужну розгалужену розвідувальну структуру та відповідне правове поле її діяльності.

Тема 11. КОМЕРЦІЙНА ТАЄМНИЦЯ ТА ЇЇ ЗАХИСТ ВІД НЕДОБРОСОВІСНОЇ КОНКУРЕНЦІЇ

1. СУТНІСТЬ І ЗНАЧЕННЯ КОМЕРЦІЙНОЇ ІНФОРМАЦІЇ. КОМЕРЦІЙНА ТАЄМНИЦЯ ПІДПРИЄМСТВА.

На думку західних теоретиків-економістів, успішний розвиток підприємництва значною мірою залежить від політико-економічного середовища (командно-адміністративного або ринково-конкурентного), в якому відбувається ринкова діяльність. Проте не менш важливим чинником, що формує економічне середовище, є криміногенна ситуація, яка утруднює або зводить нанівець дії підприємця. Наявність умов, за яких виникає реальна загроза завдання шкоди (збитків) суб'єкту господарювання, визначає першочерговим оперативне рішення проблеми гарантування економічної безпеки.

У ринкових умовах підприємницька діяльність у нашій країні здійснюється в ситуації наростаючої невизначеності і мінливості економічного середовища. Отже, виникає неясність і невпевненість в отриманні очікуваного кінцевого результату, тому зростає ризик, тобто небезпека невдачі, непередбачених втрат. Особливо це спостерігається на початку освоєння підприємництва.

В умовах командно-адміністративної економіки всі звикли до того, що економічна обстановка формується "зверху", в наказовому порядку, у вигляді набору правил і норм. Плани, програми, ухвали, інструкції, державні ціни, фонди, ліміти, наряди, тарифи формували ту економічну систему і те господарське середовище, в яких змушені були діяти підприємства і люди.

Звичайно, жорстка система централізованих настанов і розпоряджень сковувала ініціативу, пригнічувала зацікавленість і творчий пошук. Але вона забезпечувала явну або удавану чіткість, нав'язаний "порядок".

Для посилення контролю на ненаціоналізованих підприємствах в 1917 р. був прийнятий декрет "Про робочий контроль", що відміняє право власності трудових колективів на виробничу інформацію (тобто відміняє поняття "комерційна таємниця"). Проте в ринковій економіці інформація стає товаром і має підпадати законам товарно-грошових відносин. Кожен власник має право відстоювати свої інтереси, узгоджені з інтересами інших власників і суспільства.

Багато питань підприємницької діяльності регулюються і забезпечуються цивільним, адміністративним, трудовим, авторським, кримінальним та іншими видами законодавства. Говорити нині про те, що за допомогою тільки правового регулювання і охорони можна вирішити всі проблеми, пов'язані із гарантуванням безпеки підприємництва, не тільки передчасно, а й, як свідчить практика, нереально в найближчому майбутньому.

Ринок - це передусім економічна свобода. Над підприємцем можуть стояти тільки закон і встановлювані ним обмеження. Державне регулювання в умовах ринку полягає переважно у встановленні норм здійснення підприємницької діяльності і податкової системи. Решта визначається виробником і споживачем, а деякою мірою складається випадково.

За економічну свободу доводиться платити. Адже свобода одного підприємця водночас супроводжується і свободою інших підприємців, які вільні купувати чи не купувати його продукцію, пропонувати за неї свої ціни, продавати йому свою продукцію за певними цінами, диктувати свої умови операцій. При цьому природно, що ті, з ким доводиться вступати в господарські відносини, насамперед добиваються своєї вигоди, а вигода одних може стати збитком для інших. До того ж, підприємець-конкурент взагалі схильний витісняти свого опонента з ринку.

У нових ринково-конкурентних умовах виникає багато проблем, пов'язаних із гарантуванням безпеки не тільки фізичних і юридичних осіб, їх майнової власності, а й підприємницької (комерційної) інформації як виду інтелектуальної власності. Для захисту підприємницьких інформаційних потоків від різних посягань застосовують як правові, так і спеціальні заходи, а за потреби комплекс їх.

Сукупність відомостей, які використовують у підприємницькій діяльності, можна умовно згрупувати за такими напрямами:

а) підприємницька (комерційна) інформаційна система (відомості про стан економічної системи; чинники, які позитивно чи негативно впливають на сферу господарювання і комерції, в якій діє підприємець);

б) правова інформаційна система (відомості про чинне законодавство, що регулює й охороняє діяльність підприємницьких (комерційних) структур);

в) спеціально-оперативна інформаційна система (відомості про способи, сили і засоби гарантування безпеки підприємницької інформації від доступу третіх осіб).

Підприємницька діяльність у всіх сферах нерозривно пов'язана з отриманням і використанням різних видів інформації. Причому нині інформація є особливим товаром, що має конкурентну вартість. Для підприємця часто найбільш цінною є інформація, яку він використовує для досягнення цілей фірми і розголошування якої може позбавити його можливості вирішувати ці завдання, тобто створює загрозу безпеці підприємницької діяльності. Звичайно, не вся інформація може, в разі її розголошування, створювати таку загрозу, проте існує певна інформація, яка потребує захисту.

Інформація, яку використовують у підприємницькій діяльності, вельми різноманітна. її можна поділити на два види: промислова і комерційна. До промислової належать: інформація про технологію і спосіб виробництва, технічні відкриття і винаходи; "ноу-хау"; конструкторська документація, програмне забезпечення тощо.

Комерційна інформація - це відомості про фінансово-економічне становище підприємства (бухгалтерська звітність), кредити і банківські

операції, про укладені договори, контрагентів, структуру капіталів і плани інвестицій, стратегічні плани маркетингу, аналіз конкурентоспроможності власної продукції, клієнтів, плани виробничого розвитку, ділове листування та ін.

Відповідно до Закону України "Про інформацію", громадяни, юридичні особи, що володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, отриманою власним коштом або такою, котра є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, і встановлюють для неї систему (способи) захисту. Для цього, крім наказу про комерційну таємницю, підприємства можуть складати посадові інструкції із зазначенням порядку і системи обміну інформацією між працівниками підприємства і зовнішніми користувачами, деталізований графік документообігу із призначенням осіб, відповідальних за витік інформації, вносити спеціальні розділи в трудові угоди та контракти і т.ін.

Типові відомості, що становлять комерційну таємницю. У наведеному нижче переліку відомості, що становлять комерційну таємницю, згруповано за тематичним принципом. Пропонований поділ на групи має рекомендаційний характер і може бути змінений залежно від специфіки відомостей, що становлять комерційну таємницю конкретного підприємства (організації). Відомості, введені в цей перелік, є комерційною таємницею тільки з урахуванням особливостей конкретного підприємства.

1. Відомості про фінансову діяльність:
- прибуток, кредити, товарообіг;
- фінансові звіти і прогнози;
- комерційні задуми;
- фонд заробітної плати;
- вартість основних і оборотних фондів;
- кредитні умови платежу;
- банківські рахунки;
- планові звітні калькуляції.

2. Інформація про ринок:
- ціни, знижки, умови договорів, специфікація продукції;
- обсяг, історія, тенденції виробництва і прогноз для конкретного продукту;
- ринкова політика і плани;
- маркетинг і стратегія цін;
- відносини зі споживачами і репутація;
- чисельність і розміщення торгових агентів;
- канали і методи збуту;
- політика збуту;
- програма реклами.

3. Відомості про виробництво і продукцію:
- технічний рівень, техніко-економічні характеристики проектованих виробів;
- плановані терміни створення проектованих виробів;
- застосовування і перспективні технології, технологічні процеси, прийоми і устаткування;
- дані про модифікацію і модернізацію раніше відомих технологій, процесів, устаткування;
- виробничі потужності;
- стан основних і оборотних фондів;
- організація виробництва;
- розміщення і розмір виробничих приміщень і складів;
- перспективні плани розвитку виробництва;
- технічні специфікації існуючої і перспективної продукції;
- схеми і креслення окремих вузлів, готових виробів, нових розробок;
- стан програмного і комп'ютерного забезпечення;
- оцінка якості та ефективності;
- номенклатура виробів;
- спосіб упаковування;
- доставка.

4. Відомості про наукові розробки:
- нові технологічні методи, нові технічні, технологічні і фізичні принципи, заплановані для використання в продукції підприємства;
- програми НДР;
- нові алгоритми;
- оригінальні програми.

5. Відомості про систему матеріально-технічного забезпечення:
- склад торгових клієнтів, представників і посередників;
- потреби в сировині, матеріалах, комплектувальних вузлах і деталях, джерела задоволення цих потреб;
- транспортні й енергетичні потреби.

6. Відомості про персонал підприємства:
- чисельність персоналу підприємства;
- визначення осіб, що приймають рішення, та їхня філософія.

7. Відомості про принципи керівництва підприємством:
- застосовувані і перспективні методи керівництва виробництвом;
- факти ведення переговорів, предмет і цілі нарад і засідань органів керування;
- плани підприємства щодо розширення виробництва;
- умови продажу і злиття фірм.

8. Інші відомості:
- важливі елементи систем безпеки, кодів і процедур доступу до інформаційних мереж і центрів;
- принципи організації захисту комерційної таємниці.

Інформація фірми, що становить комерційну таємницю, за важливістю може належати до чотирьох рівнів:

1. Життєво важлива - незамінна інформація, наявність якої стратегічно необхідна для функціонування підприємства. Витік цієї інформації ставить під загрозу самофункціонування організації (підприємства).

2. Важлива - інформація, процес ліквідації наслідків витоку якої складний або пов'язаний з великими витратами.

3. Корисна - інформація, витік якої завдає матеріальної шкоди підприємству, однак воно може ефективно функціонувати й у разі витоку цієї інформації.

4. Неістотна - інформація, витік якої не завдає матеріального збитку підприємству і не впливає на його функціонування.

Інформація, що належить до перших трьох рівнів, є комерційною таємницею. Для збереження відомостей, що становлять комерційну таємницю, наказом по підприємству потрібно ввести такі нові грифи інформації за ступенем важливості:

- для життєво важливої - комерційна таємниця 3 (КТ 3);
- для важливої - комерційна таємниця 2 (КТ 2);
- для корисної - комерційна таємниця 1 (КТ 1).

Уся ця інформація має різну цінність для підприємця, і розголошування її може призвести (або не призвести) до загроз економічній безпеці різного ступеня важкості. Тому інформацію доцільно поділяти на три групи:

а) інформація для відкритого користування будь-яким споживачем у будь-якій формі;

б) інформація обмеженого доступу - тільки для органів, що мають відповідні законодавчо встановлені права (міліція, податкова поліція, прокуратура);

в) інформація тільки для працівників (або керівників) фірми. Інформація, що належить до другої і третьої груп, є конфіденційною і має обмеження у розповсюдженні.

Отже, конфіденційна інформація - це документована (тобто зафіксована на матеріальному носієві і з реквізитами, що дають змогу ідентифікувати її) інформація, доступ до якої обмежується відповідно до законодавства України. Частина цієї комерційної інформації становить особливий блок, і її можна віднести до комерційної таємниці.

Комерційна таємниця підприємства - це інформація, що не є державним секретом і пов'язана з виробництвом, технологічною інформацією, управлінням, фінансами та ін. Розголошування (передача, витік) її може завдати збитку інтересам фірми. Така загальна характеристика категорії "комерційна таємниця" підприємства є законодавчо правильною.

Узагальнення різних поглядів вітчизняних і зарубіжних авторів дає змогу дати розширене трактування цієї складної категорії. У найбільш загальному вигляді вона охоплює інформацію про:

- торговельні відносини фірм;

- організацію і розміри обороту засобів;
- стан ринку збуту;
- банківські операції;
- постачальників і споживачів;
- сутність патентів;
- структуру капіталів;
- плани інвестицій;
- укладені контракти;
- формування ціни на товар;
- розмір прибутку і обсяг виробництва.

До виробничої таємниці належить інформація про:

- способи виробництва і технології;
- організацію праці;
- технічні відкриття і винаходи;
- цілі і характер дослідницьких робіт.

Доцільно також у загальному обсязі комерційної інформації виділити два основні блоки. Такий підхід передбачає, що до категорії науково-технічної і технологічної інформації належать відомості про конструкцію машин і устаткування, використовувані матеріали, методи і способи виробництва, дизайн, програмне забезпечення ЕОМ та ін.

До категорії ділової належить інформація про:

- фінанси підприємства (фінансова звітність, стан розрахунків з клієнтами, заборгованість, кредити, платоспроможність, прибуток, собівартість продукції та ін.);
- стратегічні й тактичні плани розвитку виробництва, зокрема з використанням нових технологій, винаходів, ноу-хау;
- плани та обсяги реалізації продукції (плани маркетингу, характер і обсяг торговельних операцій, рівень цін, складські запаси);
- аналіз конкурентоспроможності своєї продукції, ефективності експорту й імпорту, передбачуваний час виходу на ринок;
- плани рекламної діяльності;
- списки торгових та інших клієнтів, конкурентів, відомості про взаємини з ними, їх фінансове становище, умови контрактів та ін.;
- методи і організацію управління;
- власну оцінку характеру і репутації персоналу та підприємства;
- систему організації праці.

На практиці керівники і підприємці не завжди цілком чітко уявляють собі, що означає поняття "комерційна таємниця", як її слід охороняти і як результати подібної роботи можуть впливати на економічний стан підприємства.

За оцінками експертів, втрата лише чверті інформації, що належить до комерційної таємниці, забезпечує вагомі переваги конкурентам і протягом кількох місяців призводить до банкрутства половини фірм, що припустилися витоку інформації. Є всі підстави вважати, що в процесі розвитку ринкових

відносин із властивими їм конкуренцію і господарським розрахунком підходи до охорони комерційної таємниці радикально зміняться.

У ринковій економіці інформація є товаром і її отримання, зберігання, передача та використання мають відповідати законам товарно-грошових відносин. Кожен власник має право охороняти свої інтереси і захищати необхідну інформацію, отримуючи при цьому певну свободу підприємництва. Право на таємницю означає обмеження державного втручання в економічне життя підприємства і захист його інтересів піл час взаємодії з іншими суб'єктами ринкових відносин. На відміну віл державних і військових таємниць, комерційна таємниця є власністю конкретного підприємства. її головне призначення - забезпечувати підприємству економічні переваги в конкурентній боротьбі.

В економіці України держава в особі своїх численних органів тривалий час посідала монопольне становище в засекречуванні н охороні різної інформації. Це пояснювалося переважною часткою державної власності на засоби виробництва і продукти праці. Часто виникали ситуації, коли країна поступалася пріоритетами в різних галузях науки і виробництва через безгосподарне ставлення до пропозицій раціоналізаторів, винахідників і вчених. Продукти інтелектуальної діяльності йшли за кордон, а через деякий час за значні валютні кошти нам доводилося купувати там продукцію, виготовлену з використанням наших розробок.

Витоку за кордон інтелектуальної продукції (ідей, пропозицій, винаходів, відкриттів) багато в чому сприяла практикована раніше в країні система привласнення вчених ступенів, орієнтована на кількість статей, опублікованих в зарубіжних наукових журналах. Такі "легальні" канали просочування інтелектуальної інформації були надзвичайно широкими. Витрачаючи чималі кошти на її отримання, ми часто "за дякую" віддавали її західним фірмам, які мали від її використання великі доходи.

За нинішніх ринкових конкурентних відносин просочування такої інформації може негативно позначитися на становищі підприємства в боротьбі за споживача. Саме тому тепер доцільно юридично точно визначати категорію і правовий статус комерційної таємниці, розробляти механізм відповідальності за її розголошування. Інтереси окремих підприємств мають бути підпорядковані інтересам країни. Паралельно із розвитком приватизації і становленням підприємництва в нашій країні потрібно створити систему, що забезпечує продаж інформації підприємства за кордон без збитку для держави в цілому. У промислово розвинених країнах аналоги таких систем є. Вони передбачають різні ефективні методи економічної дії на приватних підприємців, котрі на збиток національним інтересам країни дозволяють собі порушувати заборони держави на експорт науково-технічної продукції.

У нашій країні нині немає законодавчого захисту комерційної таємниці, не практикується широке вжиття заходів економічної відповідальності при вирішенні цієї проблеми, не напрацьовано відповідну судову практику. Можливо, саме тому в реальному житті підприємств процвітає явне і таємне

безоплатне запозичення інтелектуальної власності і комерційної інформації конкурентів (кооперативів, малих підприємств і приватних осіб).

Економічна безпека підприємств порушується насамперед тоді, коли його співробітники працюють за сумісництвом в інших місцях, використовуючи при цьому документацію (методики, креслення, програми та ін., створену на основному підприємстві, але юридично не закріплену в його власності. Адже саме ця інтелектуальна продукція (знання й технологія) часто становить найбільш цінний капітал підприємства. Будь-який суб'єкт господарських відносин, що використовує цю інформацію, зобов'язаний укладати з підприємством договір і віддаванні йому частину прибутку, отриманого від використання досягнень. Проте нинішній економічний і правовий стан опрацьовування цього питання не дає змоги підприємству - власникові інформації заявити і реалізувати свої претензії.

Для вирішення цієї проблеми доцільно законодавчо обмежити (а іноді й повністю заборонити) безкоштовне використання досвіду окремих підприємств. Водночас потрібно регламентувати порядок купівлі-продажу пріоритетних розробок з урахуванням їх реальної ринкової вартості. Підприємці мають підготуватися до переходу внутрішнього ринку на патентно-ліцензійну систему охорони промислової власності. На підприємствах доцільно зміцнити відповідні підрозділи патентно-ліцензійних відділів, ввести досвідчених фахівців у маркетингові служби, організувати власними зусиллями ефективну систему захисту інформації.

Фахівці науково-технічних, виробничих, економічних та інших служб підприємства повинні навчитися правильно й конкретно (у вартісній формі) оцінювати передбачувані та реальні втрати фірми внаслідок просочування інформації, віднесеної до категорії комерційної таємниці.

У найбільш загальному вигляді втрати підприємства від недотримання умов конфіденційності призводять до того, що:

- знижуються можливості продажу ліцензій на власні наукові розробки, втрачається пріоритет в освоєних галузях науково-технічного прогресу, зростають витрати на переорієнтацію діяльності дослідницьких підрозділів;
- виникають (створюються конкурентами) труднощі в закупівлі сировини, технології, устаткування та інших компонентів, необхідних для нормальної виробничої діяльності;
- обмежується співпраця підприємства з діловими партнерами, знижується вірогідність укладання вигідних контрактів, виникають проблеми у виконанні договірних зобов'язань;
- зростають витрати підприємства на створення нової ринкової стратегії, зміну структури маркетингових досліджень та ін.; виникає реальна загроза застосування економічних санкцій щодо винних у розголошуванні комерційної таємниці.

Точний вартісний розрахунок сукупного розміру всіх втрат досить складний, трудомісткий, а іноді просто неможливий через брак достовірних

початкових даних. Тому в більшості випадків достатньо укрупненої експертної оцінки втрат підприємства, зумовлених недотриманням вимог захисту інформації.

Компенсація перелічених вище втрат підприємства часто вимагає значних додаткових витрат, що знижує ефективність виробництва загалом і можливість успіху в конкурентній боротьбі. Саме тому питанням захисту комерційної таємниці нині приділяється дедалі більше уваги.

2. *ПРАВОВІ АСПЕКТИ КОМЕРЦІЙНОЇ ТАЄМНИЦІ. МЕХАНІЗМ ВИЗНАЧЕННЯ ПЕРЕЛІКУ ІНФОРМАЦІЇ, ЩО СТАНОВИТЬ КОМЕРЦІЙНУ ТАЄМНИЦЮ*

Комерційна таємниця, як уже зазначалося, - це інформація, яка с секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, і у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію (ст. 505 Цивільного кодексу України).

Ст. 420 ЦКУ визначено, що комерційна таємниця є об'єктом інтелектуальної власності. Відповідно майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визнала інформацію комерційною таємницею, якщо інше не встановлено договором.

Зокрема, до майнових прав інтелектуальної власності на комерційну таємницю належать:

- право на використання комерційної таємниці;
- виключне право дозволяти використання комерційної таємниці;
- виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці;
- інші майнові права інтелектуальної власності, встановлені законом (ст. 506 ЦКУ).

У свою чергу, ст. 162 Господарського кодексу України (ГКУ) визначає, що суб'єкт господарювання, який є власником технічної, організаційної або іншої комерційної інформації, має право на захист від незаконного використання цієї інформації третіми особами за умов, що ця інформація має комерційну цінність у зв'язку з тим, що вона невідома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а власник інформації вживає належних заходів до охорони її конфіденційності. Термін правової охорони комерційної таємниці обмежується в часі.

Отже, можна із впевненістю сказати, що склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються самостійно її власником або керівником підприємства з дотриманням чинного законодавства.

Підприємство має право розпоряджатися такою інформацією на власний розсуд і здійснювати щодо неї будь-які законні дії, не порушуючи при цьому права третіх осіб.

Крім того, підприємство як власник відомостей, які є комерційною таємницею, має право призначати особу (осіб), яка буде володіти, користуватися і розпоряджатися такою інформацією, визначати правила обробки інформації та доступу до неї, а також встановлювати інші умови щодо комерційної таємниці.

Але слід зазначити, що не будь-якій інформації підприємство може надати статус комерційної таємниці, обмеживши таким чином доступ до неї третіх осіб і насамперед контролюючих органів. Про це йдеться у ч. 2 ст. 505 ЦКУ, якою визначено перелік відомостей, що становлять комерційну таємницю. Зокрема, нею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які, відповідно до закону, не можуть бути віднесені до комерційної таємниці.

Зазначені вище відомості можуть бути визнані такими, що становлять його комерційну таємницю, громадянином-підприємцем, який здійснює підприємницьку діяльність без створення юридичної особи.

Склад і обсяг відомостей, які становлять комерційну таємницю підприємства, визначаються його керівником з урахуванням Постанови Кабінету Міністрів України "Про перелік відомостей, що не становлять комерційної таємниці" від 9.08.1993 р. № 61J (далі - Постанова № 611). Усі види інформації, які можуть вважатися комерційною таємницею, умовно можна поділити на дві групи: технічна і комерційна. До першої належать незапатентовані науково-технічні розробки, бази даних та інші комп'ютерні програми, створені підприємством; усі види "ноу-хау", технічні проекти, промислові зразки, незапатентовані товарні знаки тощо. Слід мати на увазі, що об'єкти інтелектуальної власності, щодо яких отримано патенти або авторські свідоцтва, до складу комерційної таємниці зараховувати немає сенсу, оскільки подібні об'єкти охороняються відповідним законодавством. До другої групи віднесено умови контрактів, дані про постачальників і покупців, інформацію про переговори, маркетингові дослідження, дані про розрахунок відпускних цін, розміри знижок тощо.

Механізм визначення переліку інформації, що становить комерційну таємницю

Конфіденційну інформацію поділяють на інформацію обмеженого доступу і на секретну. До першої належать відомості, розголошування яких заподіює збитку тактичним інтересам, таким як зрив конкретного контракту, зниження відсотка прибутків від операції, ускладнення угод, виконання окремої угоди. Розголошування секретної інформації завдає збитку інтересам фірми, може поставити під загрозу саме її існування надалі. її становлять відомості, ознайомлення з якими дає змогу конкурентам підірвати репутацію фірми в очах партнерів, заподіяти їй фінансового збитку, призвести до конфлікту з

державними органами, поставити у залежність від кримінальних структур.

Вітчизняні підприємства переймають практику іноземних підприємств, яка передбачає чотири способи визначення поняття "комерційна таємниця":

1. Тотальний

Суть цього методу дуже проста. Ознайомившись із переліком Закону України "Про комерційну таємницю", в якому зазначено, що не може бути комерційною таємницею, потрібно просто методом виключення все, що залишилося, визнати комерційною таємницею підприємства. Таким чином, таємницею буде вся інформація підприємства. Цей спосіб найбільш простий і найменш ефективний. Справді, дуже легко оголосити всю інформацію, що підлягає захисту, секретом. Ось тільки як її захищати? У свідомості людини зазвичай усе означає нічого. Це дуже абстрактне поняття, що потребує конкретного пояснення. Отже, або доведеться створювати відмінну працюючу систему, яка займеться захистом "всього", або потрібно буде змиритися з тим, що таємниця залишається лише закріпленою на папері.

2. Плагіаторський

Теж вельми легкий спосіб. Треба просто з'ясувати, яку саме інформацію партнери вважають комерційною таємницею, і так само вчинити на підприємстві. Природно, що повного списку ніхто з конкурентів не надасть, але підказати, які саме сфери діяльності підлягають засекречуванню, і дати невелику підказку, напевне, зможуть. У крайньому разі досить просто ознайомитися із спеціальними матеріалами і літературою, що досліджує ці теми. Зазвичай як допоміжну інформацію там подано перелік інформації, яка може бути віднесена до комерційної таємниці.

Проблема тільки в тому, що все, що вдасться дізнатися у такий спосіб, буде швидше рекомендацією, свого роду "сировиною", з якої потрібно створити необхідний продукт. У комерційній таємниці є достатньо універсальних положень, які підходять абсолютно для всіх. V кожній ситуації потрібна індивідуальна робота, що враховує всі нюанси й особливості. Те, що одні вважають таємним, може бути відкритим в інших випадках і навпаки.

3. Аналітичний

Цей спосіб дещо складніший за перелічені вище, але і набагато ефективніший. Спосіб полягає в "рольових іграх", його давно використовують психологи, слідчі, маркетологи та ін. Як же він діє? Уявіть себе на місці іншої людини. Наприклад, подумайте, яка саме інформація про конкурентів була б особливо корисною. Тепер уявіть себе на місці конкурентів і розгляньте ситуацію щодо вашого підприємства. Вельми корисно уявити себе на місці зловмисника (злодія, шантажиста чи іншого недоброзичливця), адже загроза може виходити і від них. Якщо ваша уява працює погано, залучіть родичів, друзів. Зверніться до власного персоналу з таким завданням, вони не тільки допоможуть, а й, можливо, ви виявите в декого з них чудові аналітичні якості, які раніше він не використовував. Отримані таким чином результати після певного опрацювання і слід визнати комерційною таємницею. Природно, що такі "сеанси перевтілення" слід проводити регулярно, адже підприємство

розвивається. Результат такої роботи, якщо вона проведена зі всією серйозністю, може бути дуже ефективним.

4. Експертний

Якщо в описах попередніх способів були ситуації, коли бізнесмен намагається самостійно вирішити свої проблеми, то в цьому разі потрібно звернутися по допомогу до фахівців. Природно, професіонал, що займається захистом комерційної таємниці, здатний зробити це набагато краще за будь-яку непідготовлену особу. Люди, чиєю професією є захист і безпека, мають відмінну підготовку, підкріплену практичним досвідом. І для них не становитиме особливих труднощів виконати свою роботу. Фахівців у цій сфері мало, але вони є. І їх послуги не такі вже й дорогі, як здається, їх вартість набагато менша за той збиток, якому вони допоможуть запобігти.

Доцільно надати захист комусь не з керівного складу як додатковий обов'язок до вже наявних обов'язків. Чи треба говорити, що менеджер чи заступник директора і без цього мають достатньо роботи. Відповідно і займатися нею вони будуть "як-небудь", швидше демонструючи видимість роботи. Тому це рішення є найбільш негативним.

Значно кращим є рішення, коли повноваження із захисту розподіляють серед відповідних працівників наприклад, менеджер, юрист, бухгалтер, працівника служби персоналу, охоронець. Загалом такий спосіб може дати добрі результати. Кожен працівник займатиметься своєю справою, в якій він розбирається, і водночас спільними зусиллями можна досягти потрібної мети. Тільки чи зможе начальство грамотно поставити завдання і, найголовніше, проконтролювати їх виконання? Практика показує, що не завжди може.

Тому якнайкращим рішенням є створення власної служби безпеки, що складається хоча б з кількох працівників, які займаються безпосередньо питаннями захисту. На жаль, мати службу безпеки може не кожне підприємство. (До речі, іноді службою безпеки помилково називають охоронців, що виконують дещо інші завдання). Тоді до вирішення питання залучають фахівця-консультанта. Доцільно не просто одноразово залучати такого спеціаліста для надання послуг, а регулярно звертатися до нього по допомогу.

У будь-якому разі до інформації, що становить комерційну таємницю, належать:

- кредитні договори з банками;
- договори купівлі і продажу, починаючи від певної суми (для дрібної фірми це може бути 1000, для великої - 25 тис. або 100 тис. "зелених" чи їх еквівалент);
- відомості про перспективні ринки збуту, джерела коштів або сировини, товари, вигідних партнерів;
- будь-яка інформація, надана партнерами, якщо за її розголошування передбачені штрафні санкції.

Для безпосереднього визначення переліку відомостей, що становлять комерційну таємницю, на підприємстві можна створити спеціальну комісію, яка

займатиметься групуванням і уточненням інформації з цього переліку. Чисельність членів такої комісії - не більше 4-5 осіб. Створюють її з найбільш кваліфікованих і компетентних фахівців основних підрозділів та представників служби безпеки підприємства, ознайомлених як із діяльністю підприємства в цілому, так і з роботою окремих підрозділів. До складу комісії бажано вводити:

- фахівця, який володіє фінансовими питаннями, кон'юнктурою ринку та інформацією про діяльність конкуруючих фірм (як правило, це фінансовий менеджер);
- фахівця, який досконало знає систему організації роботи підприємства, її особливості;
- фахівця з питань зв'язків з іншими підприємствами, а також з укладення контрактів і договорів;
- фахівця, який володіє всіма відомостями про продукцію, що випускається, її технологічний цикл і виробництво, про проходження усіх видів інформації (усної, документальної, у вигляді зразків, вузлів, блоків, готової продукції).

У разі якщо підприємство є великим або виготовлена ним продукція досить різнорідна, можна створити кілька таких груп: одну - головну для координації та узагальнення результатів роботи, інші - залежно від потреби - по кожній окремій виробничій ділянці.

Проте підприємство може складатися лише з кількох осіб, особливо на початкових етапах розвитку. Тоді такої мети справді здатен досягти один керівник за умови, що він володіє всією необхідною інформацією. Однак, щоб уникнути суб'єктивних помилок, краще розглядати ці питання щонайменше удвох.

Як уже зазначалося, у групі мають бути провідні фахівці, які володіють повним обсягом даних, що можуть бути віднесені до комерційної таємниці. Однак це не означає, що варто обов'язково ознайомлювати всіх залучених експертів з конкретною інформацією, яка може становити комерційну таємницю, якщо раніше вони її не знали. Достатньо, коли хоча б один із них був детально обізнаний з окремим питанням, що розглядається, а інші мали про нього загальне уявлення Такий підхід зробить роботу групи більш раціональною і зможе на першому етапі усунути можливі передумови для необґрунтованого поширення комерційної таємниці.

Отже, перед групою експертів потрібно поставити комплекс завдань у такій послідовності:

а) виділити всі види діяльності підприємства, що приносять прибуток на даний момент;

б) за наявними даними про ринок збуту оцінити, чи перевищує рівень прибутку з певного виду діяльності аналогічні показники на інших підприємствах;

в) визначити ймовірну перспективу рентабельності цієї діяльності.

Якщо з економічного погляду зазначений вид діяльності відповідає цілям підприємства і нині, і в перспективі, а прибуток вищий, ніж у конкуруючих

фірм, то експерти мають визначити, що саме в цьому виді діяльності дає змогу отримувати прибуток. Відповідь на це питання і буде комерційною таємницею підприємства. Так, для відомостей наукового характеру це зазвичай:

- ідеї, винаходи, відкриття;
- окремі формули;
- нові технічні проекти;
- нові методи організації праці та виробництва;
- програмне забезпечення;
- результати наукових досліджень.

Для відомостей технологічного характеру:

- конструкторська документація, креслення, схеми, записи;
- описи технологічних процесів;
- ноу-хау;
- точні знання конструкційних характеристик виробів та оптимальних параметрів розроблюваних технологічних процесів (розміри, обсяги, конфігурація, зміст компонентів у відсотках, температура, тиск, час тощо);
- відомості про матеріали, з яких виготовлені окремі деталі, умови експериментів, обладнання та устаткування, на якому вони проводилися;
- окремі нові або унікальні вимірювальні комплекси, прилади, верстати й устаткування, що використовуються на підприємстві.

Для відомостей ділового характеру:

- дані про укладені або заплановані контракти;
- дані про постачальників і клієнтів;
- огляди ринку, маркетингові дослідження;
- інформація про конфіденційні переговори;
- калькуляція витрат виробництва підприємства, структури цін, рівня прибутку;
- плани розвитку підприємства та його інвестицій.

Якщо у виділенні вузлових відомостей виникають проблеми, то можна розглянути вид діяльності щодо окремих технологічних етапів, логічного алгоритму дій. У будь-якому разі корисними будуть аналогічні приклади організації захисту таємниць західними фірмами.

Для уникнення незаконного та несанкціонованого розповсюдження комерційної таємниці на досліджуваному підприємстві, так само як і на інших підприємствах, потрібно під час приймання на роботу ретельно вивчати обставини індивідуального ставлення людини до потреби збереження комерційної таємниці, обставини минулої роботи людини тощо. Отже, вивчення проблеми правового захисту комерційної таємниці дає змогу зробити висновок про необхідність подальшої законодавчої, науково-дослідної роботи та постійного розроблення практичних рекомендацій щодо вдосконалення системи організації захисту такої інформації.

3. НЕДОБРОСОВІСНА КОНКУРЕНЦІЯ І МЕТОДИ ВИКРАДЕННЯ ТАЄМНИЦЬ ПІДПРИЄМСТВА. ЕКОНОМІЧНЕ ШПИГУНСТВО

Перехід від планового господарювання до ринкового, виникнення численних приватних підприємств, зниження ролі державного регулювання в різних сферах економічного життя - все це призводить до різкого посилення конкуренції між виробниками товарів та послуг. Історичний досвід показує, що загалом конкуренція сприяє розвитку продуктивних сил і прогресу суспільних відносин, проте лише тоді, коли вона має цивілізовані форми. Саме в цьому разі перевагу отримує той суперник, чия стратегія спрямована на підвищення якості пропонованих товарів і послуг, зниження цін на них, надання додаткових пільг споживачам.

Водночас протиборство між конкурентами може відбуватися з використанням нецивілізованих, недобросовісних і навіть незаконних засобів і методів. У такому разі вперед виривається не той, хто краще працює, хто більше піклується про споживача, а зухвалий злочинець. На жаль, нині в Україні, зокрема, великого поширення набули саме нецивілізовані форми конкурентної боротьби. Сприятливі умови для них створюють специфічні умови пострадянського економічного простору: загальна низька культура підприємницької діяльності, незавершеність процесу формування ринкових відносин, відсутність або неефективність багатьох законодавчих і нормативних актів, економічна нестабільність (інфляція, безробіття, неплатежі), відсутність розгалуженої системи державних органів і суспільних організацій для боротьби з нецивілізованою, недобросовісною і незаконною конкуренцією.

Основний принцип конкуренції зі знаком "мінус" полягає в прагненні зміцнити своє становище за рахунок ослаблення позицій конкурентів (аж до їх повного витіснення) або обману споживачів, або поєднанням того й іншого. Нецивілізована конкуренція відбувається у формі економічного шпигунства, корупції, брехливої реклами, компрометації окремих працівників і фірм в цілому, фальсифікації та підробки продукції конкурентів, маніпулювання з діловою звітністю для отримання різних фінансових вигод і, нарешті, за допомогою прямого обману, грабежу, завдання матеріального збитку, психологічного й фізичного придушення (аж до вбивства).

Конфіденційна інформація існує, як правило, в матеріальній формі. Це зразки продукції або товарів, різні документи, креслення, плани, схеми, аналітичні огляди, моделі, каталоги, довідники, фотографії і слайди, магнітні та оптичні носії інформації.

Нерозуміння вітчизняними бізнесменами значення заходів захисту конфіденційної інформації є однією з причин небажання західних партнерів мати з ними справи. Вони приїздять, дивляться на те, як вирішуються проблеми охорони офісів, комерційних таємниць, посміхаються, підписують протоколи про наміри - і не роблять жодного кроку далі. Вони розуміють, що все вкладене ними буде або розграбовано, або використано з мінімальною ефективністю. А

головне - вкрадуть їхні комерційні таємниці. Тим часом у Західній Європі і США втрата 20% конфіденційної інформації призводить до розорення фірми протягом одного місяця.

Письмове опитування 250 московських бізнесменів, проведене у літку 2004 р., засвідчило, що найбільш типовими формами і методами економічного шпигунства вони вважають:

- підкуп або шантаж співробітників фірми - 43% відповідей;
- знімання інформації з ПЕВМ спецтехнікою (проникнення в бази даних, копіювання програм) - 42%;
- копіювання або розкрадання документів, креслень, експериментальних і товарних зразків - 10%; прослуховування телефонних розмов, підслуховування розмов в приміщеннях і автомобілях - 5%.

Цікаво порівняти результати цього опитування з думкою групи експертів країн європейської спільноти (2004 р.) про форми і методи несанкціонованого доступу до комерційних таємниць тих фірм, що конкурують:

- підкуп або шантаж працівників фірми, впровадження туди своїх агентів - 42% відповідей;
- знімання інформації з ПЕВМ спецтехнікою - 35%;
- копіювання або розкрадання документів, креслень, експериментальних і товарних зразків - 13%;
- прослуховування і підслуховування - 5%;
- інші способи - 5%.

Як бачимо, висновки обох груп зацікавлених осіб вражаюче близькі. Щодо умов, які сприяють витоку комерційних таємниць фірм, то опитування 3 тис. респондентів у семи містах Росії, проведене московським центром з вивчення проблем недобросовісної конкуренції у 2002 р., дало такі результати:

- балакучість співробітників, особливо у зв'язку із споживанням алкоголю і в дружніх компаніях, - 32% відповідей;
- прагнення співробітників заробити гроші будь-яким способом, за принципом "гроші не пахнуть" - 24%;
- відсутність служби безпеки на фірмі - 14%;
- "совкова" звичка працівників "ділитися передовим (та іншим) досвідом", давати поради стороннім - 12%;
- безконтрольне використання інформаційних і копіювальних засобів на фірмі - 10%;
- психологічні конфлікти між працівниками, між співробітниками і керівництвом, набір випадкових людей, здатних "продатися" або "помститися", - 8%.

Відповідно до міжнародних правових норм розрізняють три види недобросовісної конкуренції:

1) коли комерційну діяльність однієї фірми прагнуть видати споживачеві за діяльність іншої;

2) дискредитація комерційної діяльності за допомогою розповсюдження помилкової інформації;

3) неправомірне використання в комерційній діяльності позначень, що вводять споживача в оману. Існуючі на Заході законодавчі акти щодо товарних знаків, фірмових найменувань, недобросовісної конкуренції визначають конкретну відповідальність за такі дії:

- підкуп покупців конкурентів;
- з'ясування комерційних таємниць конкурента за допомогою шпигунства або підкупу його службовців;
- установлення дискримінаційних комерційних умов;
- таємна змова на торгах і неофіційне створення таємних картелів;
- бойкот торгівлі іншої фірми для протидії конкуренції або запобігання їй;
- продаж своїх товарів за свідомо заниженою ціною з наміром протидіяти конкуренції або придушити її (демпінг);
- навмисне копіювання товарів, послуг, реклами або інших видів комерційної діяльності конкурента і т.ін.

Відомі три форми недобросовісної конкуренції:

1. Економічне придушення, яке передбачає різні засоби і способи обмеження ділової практики, компрометацію фірм-конкурентів, їх керівників, шантаж персоналу, зрив операцій, паралізацію діяльності фірм шляхом використання ЗМІ і мафіозних зв'язків у державних органах.

2. Промислове або комерційне шпигунство, яке має на меті протиправне заволодіння комерційними засобами конкурента для отримання власних вигод.

Якщо інформація про конкурентів, що надходить легальними каналами, не дає повної і точної відповіді на запитання, яке цікавить адміністрацію підприємства, то, незважаючи на те, що більшість серйозних підприємців вважають, що застосовувати шпигунство неетично, багато компаній все-таки вдаються до послуг комерційних шпигунів. Шпигуни конкуруючих компаній часто використовують такі засоби, як пряму пропозицію (те, що мовою фахівців називається "вербуванням в лоб"), підкуп, крадіжки та інші прийоми. Такі підходи полегшуються тим, що нова техніка підслуховування, яка з'явилася на ринку, робить промислове і комерційне шпигунство набагато ефективнішим.

Зазначимо, що сума, яку зазвичай недобросовісні конкуренти пропонують за видачу цінної інформації, набагато перевищує посадовий оклад працівника фірми. Таким чином, підписка про нерозголошення таємниці зовсім не є гарантією повного її збереження.

3. Пряме фізичне придушення, що є злочинним посяганням на життя і здоров'я персоналу підприємства. Основні методи фізичного придушення конкурента:

- організація пограбувань і розбійних нападів на офіси, виробничі та складські приміщення, розкрадання вантажів тощо;
- знищення матеріальних цінностей і нерухомості конкурента шляхом підпалів, вибухів і т.ін.;
- фізичне усунення керівників, захоплення заручників. Найактивніше в Україні виявляються криміналізація і недобросовісна конкуренція у

фінансовій сфері. Більшість експертів вважають, що це особливо відчутно в національній кредитно-фінансовій системі.

Згідно з оцінками американських експертів, втрати фірм і корпорацій у США, зумовлені розкраданням конфіденційної інформації, у 1999 р. становили близько $40 млрд.!

Дослідники вважають, що існують три загальновизнані в світі форми інтелектуальної власності: авторське право, патентне право та інститут комерційної таємниці. Тобто серед об'єктів промислової власності виділяють такі, що захищаються за допомогою патентного права, а також ті, захист яких здійснюється за режимом комерційної таємниці. Така концепція також має істотні вади, оскільки фактично включає інститут комерційної таємниці до промислової власності. Однак слід зазначити, що, з одного боку, інформація, яка є об'єктом промислової власності, може й не становити комерційної таємниці, а з другого - предметом комерційної таємниці може бути не лише та інформація, яка є об'єктом промислової або інтелектуальної власності взагалі. До речі, останнє положення і зумовлює назву складу злочину (ст.1486 КК України), предметом якого є відомості, що становлять комерційну таємницю - підприємницьке шпигунство, на відміну від традиційного терміну "промислове шпигунство" (рос. "промышленный шпионаж").

Ст. 1486 Кримінального кодексу України передбачає відповідальність за два самостійні склади злочинів:

1) незаконне збирання з метою використання відомостей, що становлять комерційну таємницю;

2) незаконне використання відомостей, що становлять комерційну таємницю, якщо це завдало великої матеріальної шкоди суб'єкту підприємницької діяльності.

Під незаконним збиранням відомостей, що становлять комерційну таємницю, слід розуміти добування протиправним способом відомостей, які, відповідно до законодавства України, становлять комерційну таємницю (ст. 16 Закону України "Про захист від недобросовісної конкуренції"). Здійснення підприємницького шпигунства у формі незаконного збирання відомостей, що становлять комерційну таємницю, спрямоване на організацію витоку інформації. Відповідно до чинного законодавства, для того, щоб визнати діяння "неправомірним збиранням комерційної таємниці", спосіб збирання відомостей обов'язково має бути протиправним.

Поняття "протиправного способу добування" має охоплювати і неправомірне отримання відповідних відомостей у володіння, в тому числі за умов правомірного доступу. Таким чином, протиправність збирання є обов'язковою умовою визначення певного діяння як злочинного. Однак щодо власне злочину, передбаченого ст.1486 ККУ, закон не передбачає якогось певного способу вчинення злочину як обов'язкову ознаку об'єктивної сторони (тут ідеться вже не про "спосіб збирання", а про "спосіб незаконного збирання") або як кваліфікуючу ознаку.

Способи вчинення незаконного добування можуть бути різними, зокрема:

- вилучення, в тому числі викрадення, матеріальних носіїв інформації, яка становить комерційну таємницю (документів, що містять відповідні відомості, або предметів матеріального світу, певні ознаки яких можуть бути досліджені з метою встановлення необхідної інформації);
- незаконне дослідження носіїв опосередкованої інформації (технічних демаскуючих ознак, що містяться у власних або відображених фізичних полях об'єктів, які захищаються, а також у їхніх слідах у навколишньому середовищі);
- незаконне ознайомлення з такими документами або предметами в будь-який спосіб;
- порушення таємниці повідомлень;
- організація витоку мовної інформації;
- одержання інформації від осіб, які нею володіють, за плату (в цьому разі йдеться про осіб, які не мають права розпоряджатися відповідною інформацією);
- шляхом застосування погроз або насильства.

Зазначені дії (як і інші злочинні дії в інформаційній сфері) також можуть бути вчинені фізичним (безпосередні дії людини, що завдають шкоди інтересам, які охороняються законом, та правам суб'єктів інформаційних правовідносин, що спрямовані на організацію витоку інформації) чи технічним (організація витоку інформації технічними каналами) способами.

Під каналами витоку інформації слід розуміти джерела інформації, середовища розповсюдження сигналів та апаратуру зняття і запису інформації.

Фізичний спосіб скоєння в більшості випадків спрямований не на інформацію безпосередньо, а на її матеріальні носії (викрадення), тоді як злочини, що вчинені технічним способом, здебільшого не зачіпають цілісності та належності матеріальних носіїв. У сучасних умовах набуває розповсюдження технічний спосіб незаконного збирання інформації шляхом використання інформаційних мереж як глобальних (наприклад, Internet), так і локальних. Для прикладу таких злочинів наведемо викрадення баз даних з інформацією про клієнтів через підключення до банківських інформаційних мереж.

Досить різноманітними є також засоби вчинення злочину технічними каналами. Для досягнення мети підприємницького шпигунства шляхом отримання інформації за допомогою технічних засобів застосовуються: акустичні засоби (спрямовані або вмонтовані мікрофони, вібродатчики), лазерні засоби отримання мовної інформації, засоби отримання інформації з дротів та комунікацій, засоби перехоплення побічних випромінювань, закладені пристрої, комп'ютерна техніка,в тому числі її інформативні частини. Засоби вчинення підприємницького шпигунства у формі незаконного збирання відомостей, що становлять комерційну таємницю, так само, як і інші ознаки об'єктивної сторони підприємницького шпигунства (місце, час та обставини вчинення), не мають значення для кваліфікації злочину, але можуть бути враховані судом під час призначення покарання винній особі.

Злочин у формі незаконного добування з метою використання інформації,

що становить комерційну таємницю, слід вважати закінченим з моменту вчинення дій, спрямованих на незаконне збирання відомостей, що містять комерційну таємницю, незалежно від їх подальшого використання та настання шкідливих наслідків. Це означає, що склад підприємницького шпигунства у зазначеній формі є формальним.

Наступною формою об'єктивної сторони підприємницького шпигунства є незаконне використання відомостей, що становлять комерційну таємницю.

Це означає впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності без дозволу уповноваженої на те особи неправомірно здобутих відомостей, що становлять комерційну таємницю. Таке поняття незаконного використання, яке міститься в Законі "Про захист від недобросовісної конкуренції, не можна вважати досконалим, оскільки, зазначаючи про використання "неправомірно здобутих відомостей", він не враховує випадків такого протиправного використання, коли інформацію отримують правомірно (слід відрізняти від неправомірного збирання за умов правомірного доступу, про яке йшлося вище з приводу попередньої форми об'єктивної сторони).

Отже, інформація, що містить комерційну таємницю, може бути надана суб'єктові на законній підставі для досягнення певної мети. В такому разі використання зазначеної інформації з іншими цілями означатиме порушення комерційної таємниці, тобто буде неправомірним. Крім того, неможливо не вважати використанням передачу або продаж інформації зацікавленим особам, тобто випадки, коли суб'єкт підприємницького шпигунства власноруч не здійснює впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності відомостей, що становлять відповідно до законодавства України комерційну таємницю (це відбувається найчастіше).

Якщо не вважати платну чи безоплатну передачу здобутої інформації її використанням (передачу неправомірно здобутої інформації), це також позбавить сенсу обов'язкову ознаку суб'єктивної сторони незаконного збирання відомостей, що становлять комерційну таємницю, а саме - мету використання, оскільки, як уже зазначалося, найчастіше інформацію незаконно збирає особа не для власних потреб, а для передачі зацікавленим особам, і така передача буде кінцевою метою злочину. Отже, якщо не вважати платну чи безоплатну передачу інформації її використанням, незаконне збирання інформації з метою передачі, а не з мстою використання для власних потреб, таке незаконне збирання не буде розглядатися як злочинне. Крім того, злочином не буде в такому разі і передача зацікавленим особам інформації суб'єктами користування такою інформацією без згоди уповноваженої на це особи (що, власне, є використанням інформації не з тією метою, для досягнення якої інформація надавалася на законних підставах, про що йшлося вище).

Обов'язковою ознакою об'єктивної сторони незаконного використання відомостей, що містять комерційну таємницю, є наслідки у вигляді заподіяння великої матеріальної шкоди суб'єкту підприємницької діяльності, тобто шкоди, яка в 50 і більше разів перевищує встановлений законом неоподаткований

мінімум доходів громадян за місяць. При визначенні розміру заподіяної шкоди слід враховувати прямі матеріальні збитки, витрати на відвернення шкідливих наслідків використання відомостей іншими суб'єктами підприємницької діяльності, витрати на перепрофілювання напрямів діяльності, збитки від зниження попиту або цін на товари та послуги. Заподіяння внаслідок злочину моральної шкоди суб'єкту підприємницької діяльності (наприклад, підрив ділової репутації) на кваліфікацію не впливає, але має враховуватись при призначенні покарання судом. Склад злочину, таким чином, є в цьому разі матеріальним.

Суб'єктом підприємницького шпигунства як у формі незаконного збирання відомостей, що містять комерційну таємницю, так і у формі їх незаконного використання, може бути фізична осудна особа, яка досягла 16-річного віку. Таким чином, суб'єктом підприємницького шпигунства є загальний суб'єкт. Разом із тим, не виключаються випадки скоєння підприємницького шпигунства спеціальним суб'єктом, наприклад, посадовою особою. В таких випадках за наявності ознак посадового злочину кваліфікацію слід проводити за сукупністю.

Суб'єктом незаконного використання відомостей, що містять комерційну таємницю, є особа, яка, власне, здійснює використання зазначених відомостей, незалежно від того, ким були зібрані використовувані відомості. Якщо збирання інформації було здійснене тією самою особою, яка здійснює незаконне використання такої інформації, необхідно розмежовувати, суб'єктом яких саме дій (якої форми підприємницького шпигунства) є особа.

У випадках, коли йдеться про незаконне використання відомостей, ознайомлення з якими або одержання яких було здійснене на законних підставах (наприклад, особа, якій інформація, що становить комерційну таємницю, була надана для досягнення певної мети, використовує інформацію для інших цілей, не погоджених із суб'єктами розпорядження інформацією), винну особу слід вважати суб'єктом підприємницького шпигунства у формі незаконного використання відомостей, що містять комерційну таємницю, звісно, за умови, якщо таке використання завдало великої матеріальної шкоди суб'єкту підприємницької діяльності

Якщо йдеться про випадки використання зазначеної інформації, яка була зібрана тією ж особою в незаконний спосіб (незаконність використання в цьому випадку зумовлена незаконністю збирання інформації), особу слід визнати суб'єктом підприємницького шпигунства у формі незаконного збирання з метою використання відомостей, що містять комерційну таємницю. Це зумовлено, так би мовити, більшою суворістю підходу законодавця до визнання таких дій злочинними: для визнання підприємницького шпигунства у формі незаконного збирання відомостей злочином не вимагається настання наслідків у вигляді заподіяння шкоди, так само, як і акту використання незаконно зібраних відомостей (за умови, що збирання здійснюється з метою використання). Таким чином, особа, яка використовує інформацію, котру попередньо зібрала незаконним шляхом, має нести відповідальність за самий

факт незаконного збирання з метою використання відомостей, що містять комерційну таємницю, незалежно від настання протиправних наслідків та розміру заподіяної шкоди.

Установлення, суб'єктом якої саме форми підприємницького шпигунства є винна особа, незважаючи на те, що всі вони містяться в одній частині ст. 1486 КК України і за них передбачена однакова відповідальність (навіть якщо визнати особу суб'єктом і збирання, і використання, її дії неможливо буде кваліфікувати за сукупністю), має важливе значення, якщо в діях особи містяться ознаки і збирання, і використання інформації.

Проте можливі випадки, коли дії особи, яка незаконно зібрала, а потім використала відомості, що містять комерційну таємницю, будуть кваліфіковані як незаконне використання. За наявності передбачених законом наслідків у вигляді великої матеріальної шкоди, які необхідні для визнання незаконного використання закінченим злочином, винний не уникне покарання. Однак, якщо така шкода заподіяна не буде, склад злочину у формі незаконного використання не реалізується, і винний не буде покараний, незважаючи на те, що збирав відомості незаконним шляхом.

Таким чином, винна особа є суб'єктом:

- незаконного використання відомостей, якщо вони були отримані нею або іншою особою на законних підставах для іншої мети, або використання мало відбуватися за додержання певних умов, які особа порушила; такі відомості були незаконно здобуті іншою особою;
- незаконного збирання відомостей, якщо вони були в незаконний спосіб зібрані нею з метою використання, незалежно від того, чи відбувся акт використання; такі відомості були в незаконний спосіб зібрані нею та використані, незалежно від того, чи наявні наслідки використання у вигляді великої матеріальної шкоди.

Як уже зазначалося вище, незалежно від форми, в якій здійснюється підприємницьке шпигунство, суб'єкт цього злочину є загальним. На характеристику суб'єкта не впливає особливість об'єкта та предмета злочинних посягань, тобто цінність для здійснення підприємницької діяльності. Це означає, що суб'єктом підприємницького шпигунства не обов'язково має бути суб'єкт підприємницької діяльності. Як правило, суб'єктами підприємницького шпигунства є особи, які (або за допомогою яких) реалізують зовнішні загрози інформаційній безпеці суб'єктів підприємницької діяльності (конкуренти, агенти конкурентів, особи, які не мають безпосереднього завдання конкурентів, злочинні елементи, партнери).

Такі особи можуть мати як корисливу, так і некорисливу зацікавленість у результатах своїх дій. Особливу категорію суб'єктів підприємницького шпигунства становлять працівники фірми (різновид внутрішніх загроз) - вони можуть діяти як за завданням, так і без завдання конкурентів (останнє найбільш характерне для так званих "ображених працівників").

Традиційно вважають, що працівники фірми можуть бути суб'єктами лише розголошення комерційної таємниці - це положення досить справедливе,

однак не виключає і цілеспрямованого збирання ними з метою подальшої платної передачі певної інформації, якщо таке збирання є незаконним (наприклад, працівник за службовими обов'язками не має доступ) до комерційної таємниці, однак незаконно отримує таку інформацію і продає її конкурентам), тобто здійснення ними підприємницького шпигунства. Це є характерним не лише для підприємницького шпигунства, а й для шпигунства взагалі.

В Україні суб'єктом злочину може бути лише фізична особа. Однак світовий досвід переконує в тому, що на підприємницькому шпигунстві спеціалізуються й заробляють чималі гроші навіть окремі юридичні особи, які використовують професійні, проте здебільшого протиправні засоби отримання інформації. Цікавим є, наприклад, факт, що в США з 1986 р. легально існує "Спільнота спеціалістів з добування відомостей про конкурентів" (SCIP), яка спеціалізується на відшукуванні важкодоступної інформації, яка характеризує виробничі можливості та показники фірм, спосіб життя та схильності їхнього керівного складу (тобто відомостей, які належать до комерційної таємниці відповідно до законодавства США), використовуючи як загальнодоступні, так і нелегальні засоби та способи. В умовах впровадження сучасних інформаційних технологій в Україні і поширення підприємницького шпигунства та інших інформаційних злочинів дослідження цієї проблеми є дуже актуальним.

Економічне шпигунство

Форми і методи економічного шпигунства

Підкуп - найпростіший і найефективніший спосіб отримання конфіденційної інформації. Зрозуміло, він потребує деякої попередньої роботи для з'ясування ступеня обізнаності тих або інших працівників фірми в її справах. Підкуп зазвичай здійснюється через посередників, тому необхідною умовою є збирання інформації про них: треба точно знати, кому дати гроші, скільки, коли, через кого і за що. Проте всі такі витрати перекриваються однією важливою обставиною - працівникові фірми не потрібно долати фізичні й технічні перешкоди для проникнення в її секрети.

Отже, за лишається одне: знайти власників потрібної інформації, незадоволених своїм просуванням по службі, заробітком, характером стосунків з керівниками, тих, що гостро потребують грошей, готових заради збагачення на будь-яку зраду. Відома сумна статистика (дані Інтерполу), згідно з якою 25% службовців фірми готові продати її секрети у будь-який час кому завгодно, 50% йдуть на це залежно від обставин і лише 25% є патріотами підприємства. Одним із видів підкупу є переманювання цінних фахівців фірми до себе заради подальшого оволодіння їх знаннями. Історія конкурентної боротьби сповнена подібних прикладів. Для тих 50% працівників, які йдуть на співпрацю з конкурентами залежно від обставин, необхідні "обставини" нерідко створюють через шантаж. Шантаж буває двох видів. У першому випадку людину ловлять на "гачок", загрожуючи розголосом компромату на неї. У другому випадку їй просто погрожують фізичним впливом (знищити автомобіль, спалити дачу,

викрасти дитину, зґвалтувати доньку або дружину, залякати стареньких батьків і т.ін.).

"Вливання своїх людей " до складу персоналу фірми-конкурента. Для впровадження є два шляхи: перший - коли агент виступає під власним прізвищем і працює за професією; другий - коли він працевлаштується за підробленими документами, під прикриттям "легенди".

Впровадження власної агентури до конкурентів складніше за звичайний підкуп або шантаж, але, на відміну від завербованих інформаторів, свій агент є набагато надійнішим та ефективнішим як джерело конфіденційної інформації.

Залежно від ступеня цінності інформатора будуються відносини між сторонами, що співпрацюють. Чим він важливіший, тим більше потрібно дотримуватися заходів конспірації. Зокрема, зустрічі з ним маскуються під побутові контакти, відбуваються на конспіративних квартирах або в громадських місцях, через тайники і навіть за допомогою технічних засобів. Спілкування з менш цінними людьми може бути звичайним. При цьому сторони особливо не піклуються про свою безпеку. Отже, вибіркове приховане спостереження за власними працівниками може дати керівникові фірми (через його оперативних співробітників) вельми цікаві відомості для роздумів. Викрадення інформації можливе багатьма способами:

- розкрадання носіїв інформації (дискет, магнітних, оптичних дисків, перфокарт);
- копіювання програмної інформації з носіїв;
- читання залишених без нагляду роздруків програм;
- читання інформації з екрана сторонньою особою (під час відображення її законним користувачем або за його відсутності);
- підключення спеціальних апаратних засобів, що забезпечують доступ до інформації;
- використання спеціальних технічних засобів для перехоплення електромагнітних випромінювань (відомо, що за допомогою спрямованої антени таке перехоплення можливе стосовно ПЕВМ в металевому корпусі на відстані до 200 м, а в пластмасовому-до 1 км);
- несанкціонований доступ програм до інформації, або розшифровування програмної зашифрованої інформації. Останній спосіб називається "електронним грабежем", а людей, що використовують його, називають "хакерами". Цей вид злочинів найбільш поширений там, де є комп'ютерні мережі в масштабі фірми, організації, населеного пункту або регіону.

За оцінками швейцарських експертів, щорічні втрати, пов'язані з крадіжкою інформації з ЕОМ, становлять нині в Західній Європі близько $60 млрд. за рік (!). Наприклад, фірма "Британська енциклопедія" порушила кримінальну справу проти трьох операторів свого комп'ютерного центру, звинувативши їх у тому, що вони скопіювали і продали стороннім особам імена й адреси приблизно 300 тис. замовників.

Спостереження теж дає цінну конфіденційну інформацію, особливо якщо

воно пов'язане з копіюванням документації, креслень, зразків продукції і т.ін. Загалом процес спостереження складний, оскільки потребує значних витрат сил, часу і коштів. Тому його ведуть здебільшого вибірково: у визначеному місці, в певний час спеціально підготовлені люди і за допомогою технічних засобів. Наприклад, волокно-оптична система РК-1715 має кабель до 2 м завдовжки. Вона дає змогу проникати в приміщення через замкові щілини, кабельні й опалювальні канали, вентиляційні шахти, фалмнстелі та інші отвори. Кут огляду системи - 65°, фокусування - від 10 км до безкінечності. Працює при слабкому освітленні. З її допомогою можна читати і фотографувати документи на столах, позначки в настільних календарях, настінні таблиці й діаграми, прочитувати інформацію з дисплеїв.

Фотографування застосовують в економічному шпигунстві досить широко за допомогою сучасної апаратури за денного освітлення і вночі, на надблизькій відстані і на віддалі до кількох кілометрів, у видимому світлі і в інфрачервоному діапазоні (в останньому випадку можна виявити виправлення, підробки, а також прочитати текст на обгорілих документах). Сучасні шпигунські фотоапарати вражають уяву. Так, відомі телеоб'єктиви розміром із сірникову коробку, що, проте, чітко фотографують друкарський текст на відстані до 100 м! А мініатюрна фотокамера в ручному годиннику (РК-420) дає змогу робити 7 кадрів на одній касеті з відстані 1 м і більше без наведення на різкість установки витримки, діафрагми та інших тонкощів.

Велику небезпеку в економічному шпигунстві становлять люди, що володіють фотографічною зоровою пам'яттю. їм достатньо одного погляду, щоб охопити значний зміст, запам'ятати і відтворити його практично без спотворень. Особливо легко це вдається фахівцям у розвідуваній галузі діяльності, яким достатньо лише натяку, щоб зрозуміти основний зміст тексту (креслення, розробки). Наприклад, конкуруюча фірма послала на перегляд моделей одягу свого конкурента групу модельєрів, кожен із яких спеціалізувався на якійсь одній деталі демонстрованих моделей: рукав, комір, спинка і т.ін. В умовах суворої заборони на фотографування, відеознімання, зарисовування і навіть на розмови (щоб запобігти диктуванню на магнітофон) вони запам'ятали кожен свої деталі. Потім у себе на фірмі вони відновили в малюнках все, що бачили, по кожній моделі!

Прослуховування і підслуховування за значущістю перебувають на останньому місці серед основних форм і методів отримання конфіденційної інформації. Це зрозуміло, бо інформацію збирають випадково, безсистемно, близько 90-95% відсотків її становлять вислови, що не викликають ніякого інтересу у конкурентів. Крім того, потрібно багато часу для аналізу цієї інформації. Проте цей метод дуже широко використовують через його простоту.

Підслуховування телефонних переговорів найбільш поширене. Його здійснюють:

- за рахунок мікрофонного ефекту телефонного апарата;
- контактним підключення до лінії зв'язку;

- безконтактним підключенням до телефонної лінії;
- за допомогою телефонних радіозакладок;
- за рахунок так званого високочастотного "нав'язування'. Зазначимо, що підслуховувати можна не тільки стаціонарні телефонні лінії, а й переговори по радіотелефону, зокрема в системах стільникового зв'язку. Все залежить від того, який спосіб прослуховування використовують, за допомогою якої апаратури.

Крім того, підслуховувати можна розмови в приміщеннях або в автомобілях за допомогою попередньо встановлених радіозакладок ("жучків") або мініатюрних магнітофонів. І ті й інші камуфлюються під різні предмети, деталі одягу, побутові прилади, освітлювальну арматуру тощо. Наприклад, підслуховувальний пристрій, змонтований у вигляді стінного цвяха різних модифікацій, має довжину 1,5-3 см.

Загалом кількість моделей технічних пристроїв для підслуховування і запису розмов на ринку не піддається обліку. З їх допомогою можна приймати, підсилювати, очищати й записувати будь-які розмови (зокрема ті, що ведуться пошепки або під звук води, що ллється з крана) досить чітко і надійно.

Існують і складніші методи підслуховування, наприклад за допомогою лазерного опромінювання шибок у приміщенні, де ведуться "цікаві" розмови. Або спрямованим радіовипромінюванням, що примушує "відгукуватися і говорити" деталі радіоприймача, телевізора, настінного годинника та іншу побутову техніку. Проте подібні методи потребують складної і достатньо дорогої техніки, тому застосовують їх в економічному шпигунстві досить рідко.

Шпигунство як спосіб добування інформації, що становить комерційну таємницю

Термін "шпигунство" (економічне, промислове, комерційне, науково-технічне) означає активні дії, спрямовані на збирання або розкрадання цінної інформації, закритої для доступу сторонніх осіб.

Відповідно до західної теорії, промислове шпигунство - це добування законним і незаконним шляхом у конкуруючих фірм (монополій, а також партій, фізичних або юридичних осіб, правоохоронних органів і т.ін.) відомостей чи інформації з галузі наукових досліджень, виробництва продукції із застосуванням найбільш перспективної технології, а також персональних даних з метою їх використання в конкурентній боротьбі або навіть у корисливих цілях.

Економічне шпигунство - ширше поняття, яке охоплює і такі його підвиди, як промислове, виробниче, науково-технічне, комерційне шпигунство. Якщо таємницею володіє одна особа, це викликає інтерес до неї іншої особи, для задоволення якого чиняться дії, спрямовані на отримання нею певної матеріальної або іншої вигоди. Особа, що бере участь у подібній діяльності, має загальновідому назву "шпигун". У підприємництві конкурентна боротьба неможлива без отримання інформації. Прагнення отримати відомості в умовах закритого до них доступу законним шляхом неминуче породжує

недобросовісну конкуренцію, тобто об'єктивну потребу шпигувати за конкурентом. Без володіння інформацією про дії конкурента, передбачуваний попит на продукцію, перспективні наукові розробки важко, а деколи і неможливо бути конкурентоздатним. Виникають дві тісно пов'язаних обставини:

а) підприємець змушений виступати як захисник своїх таємниць (цінної інформації);

б) підприємець змушений з метою конкуренції здобувати (красти, купувати) чужі секрети, що захищаються. Те, що не захищається, особливої цінності не має.

Виникає запитання "як розглядати промислове (комерційне) шпигунство з позицій чинного законодавства?". У зарубіжній літературі про промислове шпигунство наголошується, що ця діяльність зовсім не вважається злочинною і не є підставою для кримінальної відповідальності. Якщо в процесі розкрадання секретної інформації підприємству, установі або працівникам завдано збитку, то кримінальному покаранню винна особа підлягає саме за останнє діяння, а не за сам факт розкрадання цінних відомостей. Загалом такий підхід є правильним, оскільки сам підприємець не зацікавлений у тому, що коли він здійснюватиме розкрадання інформаційних матеріалів (а займатися цим він змушений через ринкову діяльність), то перебуватиме під загрозою застосування до нього кримінального покарання. Здебільшого значно легше звернути увагу на охорону своїх таємниць, ніж вдаватися до кримінально-правового захисту.

Розглянемо детальніше ознаки промислового шпигунства. До них належать:

- суб'єкт (хто може займатися певним видом діяльності);
- предмет (на що посягає промислове та інше шпигунство);
- спосіб, засіб дії, за допомогою яких здійснюється оволодіння закритими відомостями;
- адресат (хто виступає замовником).

Суб'єктами промислового (комерційного) шпигунства можуть бути громадяни України, іноземні громадяни, особи без громадянства, що належать і не належать до працівників промислових підприємств, установ, фірм. Виконавцем шпигунства можуть виступати безпосередньо підприємець, працівники власної служби безпеки, приватних детективних розшукових фірм або окремі особи, що працюють у приватному порядку. Пошук промислової, комерційної інформації і оволодіння нею здійснюють в одних випадках за завданням замовника, а в інших - за власною ініціативою для подальшої її продажу зацікавленим особам.

Аналіз зарубіжної практики свідчить, що в приватних службах безпеки, які спеціалізуються на розкраданні чужих таємниць, є значна за чисельністю клієнтура замовників і покупців. Наприклад, у Великій Британії одне з приватних розшукових агентств, разом із розслідуванням фактів про промислове шпигунство, гарантуванням безпеки підприємств і фірм, займається також добуванням (розкраданням) інформації про конкурентні

приватні підприємства. Подібні фірми не прагнуть особливо конспірувати, приховувати свою діяльність, їх координати є у спеціальних довідниках. Нині в країнах ринкової економіки діють сотні й тисячі агентств та десятки тисяч промислових шпигунів.

Такі агентства починають утворюватися і діяти також на території України. Проте різкого зростання кількості таких служб слід очікувати тільки в умовах ринково-конкурентної економіки, що сформувалася аналогічно до західних країн.

З цілком зрозумілих причин видати секрети можуть і працівники фірми. Якщо особам, що не працюють на підприємстві, потрібно долати фізичні й технічні перешкоди для проникнення до таємниць, то працівники фірми можуть і не докладати подібних зусиль. Таємною інформацією вони вже володіють або мають можливість зібрати її. Мотивацією таких дій можуть бути користь, помста тощо. Тому при формуванні колективу працівників необхідно враховувати, кому з них можна довіряти свої таємниці, а кому не варто. Вирішують це питання самі підприємці. Так, працівники загальновідомого "Анта" на сторінках газет досить детально діляться інформацією про те, як вони займалися внутрішньою безпекою свого кооперативу. Спочатку приймали на роботу тільки тих, кого знали особисто і могли їм довіряти. Розширення штату працівників збільшувало небезпеку просочування інформації. Тому керівництво "Анта" ухвалює рішення про створення спеціального підрозділу - департаменту з перевірки людей, що поступали до них на роботу. На кандидатів заводили досьє, в яких концентрували результати їх вивчення і перевірок.

Наступною ознакою шпигунства є предмет посягання, тобто інформація, яка є цінною для її володаря і закрита для сторонніх осіб. Носії такої інформації найрізноманітніші: документи, креслення, схеми, патенти, дискети, касети, в яких містяться дані наукових досліджень, бухгалтерські матеріали, контракти, плани й рішення керівництва фірм. Предметом промислового шпигунства може бути інформація не тільки фірм, а й державних підприємств і установ.

Певні труднощі виникають при визначенні промислової таємниці підприємств, фірм, компаній зі змішаним капіталом. Наприклад, приватний і державний капітал; державний та іноземний приватний капітал; вітчизняний та іноземний приватний капітал. Неминуче зіткнення інтересів вітчизняного й іноземного власника як між собою, так і з державою. В останньому випадку необхідно враховувати наявність державної (військової) таємниці, службової таємниці, інших відомостей, визначених кримінальним законодавством, а також промислову таємницю. Відомості, що становлять державні секрети, перелічені у спеціальних нормативних актах, затверджених урядом держави. На їх підставі видаються відомчі акти, що визначають види таємниць, які підлягають охороні. Промислова ж таємниця може бути введена в переліки державних таємниць, а може і не належати до них. Посягання на секрети державних підприємств і установ переслідується кримінальним законом, тоді як підприємницькі секрети кримінальним законом не захищені.

Наступною ознакою промислового шпигунства є спосіб його здійснення. Дії із заволодіння інформацією чиняться таємно від оточення, шляхом її розкрадання, збирання, купівлі, видачі. Не є винятком і знищення, спотворення або саботаж щодо використання інформації. Мета цього - не дати власникові можливості використовувати її для отримання вигоди, бути конкурентоспроможним.

До засобів отримання таємниць належать різні технічні системи. Якщо в Україні основними власниками розвідувальних технічних засобів є спеціальні державні органи (служби), то на Заході вони перебувають у користуванні приватних осіб. Це дає змогу підприємцям широко використовувати засоби електронної розвідки для отримання необхідної інформації, зняття її з телефонних переговорів, ЕОМ, приміщень, де ведуться секретні переговори, і т. ін. Застосування цих та інших засобів залежить від інформації, яку має намір отримати суб'єкт. Один вид інформації може бути викрадений, інший - прослуханий, третій - сфотографований (або зроблені зарисовки), четвертий - записаний на магнітофон, п'ятий - знятий кінокамерою і т.д. Іноді використовують комплекс спеціальних заходів для її отримання. Залежно від виду отримання інформації вживають відповідних заходів захисту. Наприклад, існують прилади, за допомогою яких можна з відстані до 500 м лазерним променем знімати розмовну інформацію за рахунок вібрації шибок. У відповідь для запобігання просочуванню інформації у такий спосіб німецька фірма "Сіменс" почала випуск спеціальних віконних рам, що ослабляють на 110 дБ проникнення електромагнітних випромінювань у певних діапазонах.

Адресатами (замовниками) отримання промислової (комерційної) інформації виступають підприємці малого і великого бізнесу, керівники державних підприємств, а також уряди іноземних держав. Захист таємниць промислових і комерційних фірм і проникнення в них є двома сторонами однієї медалі. До них однаковою мірою виявляють цікавість як приватні особи, так і працівники державних служб.

Один із керівників американської розвідки, виступаючи в 2000 р. у національному прес-клубі, заявив, що економічна потужність є ключем до панування і влади у всьому світі. У доповіді цього керівника, виголошеній в американському університеті, прозвучало, що "у майбутньому ми станемо свідками різкого зростання напруженості в міжнародних економічних відносинах. Об'єктивна інформація про економіку іноземних держав стане практично важливою, і розвідка зобов'язана її здобувати". За кордоном вважають, що не менш важливе завдання лягає на плечі контррозвідувальних підрозділів, які зобов'язані припиняти будь-які спроби іноземних спецслужб здійснювати політичне, промислове та економічне шпигунство проти США.

У наших періодичних виданнях також з'являються дані про те, що вітчизняна розвідка перенацілює свої зусилля на збирання торговельно-економічної інформації.

Як бачимо, новим пріоритетом у сучасних умовах для розвідувальних і контррозвідувальних служб стають відомості економічного характеру. Тому

напрошується висновок про те, що зацікавленість певними видами приватної і державної економічної інформації на території України (враховуючи діяльність наших фірм і за кордоном) виявлятимуть не тільки приватні служби безпеки, а й іноземні спецслужби. До того ж, прямий захист підприємницьких структур не належить до функцій контррозвідувальних служб. Західні фірми витрачають на захист своєї інформації 15 % своїх доходів. У нас вести мову про такий захист рано. Разом із тим наш підприємець не прагне в разі потреби звертатися до державних правоохоронних органів.

Посягання на приватну інформацію можуть бути з боку суб'єктів приватного підприємництва і спецслужб іноземної держави, наприклад:

1. Проникненню до приватних таємниць фірми, підприємства конкуруючої приватної фірми (працівники приватного детективного агентства, власної розвідувальної служби) запобігають власними силами безпеки і технічними засобами. Особа, затримана в приміщенні (будівлі), може бути притягнута до кримінальної відповідальності за безпосередньо заподіяний збиток: розбій, умисне або необережне знищення чи пошкодження особистого майна громадян або як посягання проти власності об'єднань і організацій, злочин проти життя і здоров'я особи.

Промисловим (комерційним) секретом можна заволодіти також за допомогою підкупу працівників конкуруючої фірми, їх шантажу, погроз тощо. Якщо з'ясується, що витік інформації стався з вини свого ж працівника, то підприємець зможе тільки звільнити його, щоб запобігти витоку інформації в майбутньому. У таких випадках для підприємця важливіше запобігти просочуванню інформації, створивши надійний її захист, ніж витрачати сили й кошти на пошук шпигуна, що викрав секретні матеріали.

2. Приватна особа робить замах на інформацію підприємства змішаного типу (вітчизняний та іноземний капітал) на користь вітчизняного підприємства. У її діях немає складу злочину, за винятком випадків, коли в процесі розкрадання здійснено інший злочин (вбивство або нанесення тілесних ушкоджень охоронцеві чи іншим особам, знищення або пошкодження майна і т.п.).

3. Приватна особа діє на користь іноземної приватної або державної фірми, філії якої діють як на території власної держави, так і за кордоном, проти вітчизняних приватних і державних підприємницьких структур.

При посяганні на промислову (комерційну) інформацію приватного підприємства ознак складу злочину немає. Деяка зовнішня схожість такої діяльності, що пов'язана з отриманням інформації, має ознаки складу передачі іноземним організаціям відомостей, що становлять службову таємницю. Проте службова таємниця визначається нормативними актами тільки для державних підприємств.

Комерційна інформація про інші підприємства в обсязі 90-95% може бути отримана легально, а решта, як правило, найбільш цінна і ретельно охороняється. Добувають її промисловим шпигунством такими властивими йому методами, як викрадення документів і зразків нової продукції, шантаж,

підкуп працівників конкуруючої фірми, підслуховування розмов, фотографування й оптичне спостереження, несанкціоноване підключення до систем зв'язку та обчислювальних мереж, засилання і вербування агентів і навіть фізична ліквідація конкурентів або їх підприємств.

Одночасно з розвитком промислового шпигунства постійно вдосконалюються засоби захисту таємниць підприємців. Наприклад, у промислово розвинених країнах останніми роками постійно нарощуються обсяги виробництва спеціальних технічних засобів захисту входу в службові приміщення. Для цього використовують такі нововведення, як системи кодованих карток, біометричні системи, що реагують на голос, підпис, відбитки пальців, візерунки кровоносних судин, сітківку ока.

Найбільш доступними легальними джерелами отримання інформації є:

- усні виступи працівників підприємства на різних конференціях, семінарах та ін.;
- відкриті публікації підприємства та його окремих працівників;
- експонати різних ярмарків, виставок і презентацій;
- дані товарних і фондових бірж;
- оголошення про наявні вакансії, конкурси на заміщення посад та ін.

Систематизація й аналіз такої інформації пов'язані з великими витратами матеріальних і трудових ресурсів. Іноді цим займаються спеціально створені служби, оскільки обсяги інформації великі, а її достовірність іноді викликає сумнів.

У промислово розвинених країнах (наприклад, у США) відповідні державні органи мають спеціальні посередницькі служби, що надають клієнтам деякі види комерційної інформації про підприємства, котрі їх цікавлять, та організації. У нашій країні законодавчо визначено, що підприємство надає державним органам інформацію, необхідну для оподаткування і ведення загальнодержавної системи збирання та оброблення економічної інформації. Підприємства також публікують дані про свою діяльність, зокрема річні баланси. Водночас підприємство має право не надавати інформацію, що містить комерційну таємницю.

Для запобігання витоку комерційної таємниці через працівників державних органів управління і контролю керівник підприємства повинен знати їх реальні права і надавати їм тільки ту документацію, котра необхідна для виконання їхніх службових функцій. Насамперед це стосується працівників статистичної служби, антимонопольного комітету, міліції, фінансової, податкової, санітарної, пожежної та інших інспекцій. Підприємець також повинен знати порядок оскарження неправомірних дій державних службовців, посадових осіб і працівників правоохоронних органів, механізм відшкодування матеріального і морального збитку, заподіяного фірмі внаслідок їхніх дій. Кожен підприємець має бути ознайомлений із процедурами запрошення консультантів, адвокатів, експертів, а також з порядком їх участі в передачі інформації, віднесеної до категорії комерційної таємниці.

У конкурентній боротьбі підприємців промислово розвинених країн

використовують і такий легальний метод отримання інформації, як "зворотний інжиніринг", відомий ще з часів становлення автомобільної компанії Форда. При цьому у спеціальних лабораторіях розбирають і вивчають продукцію конкурентів для визначення можливих нововведень і таємниць технологи її виготовлення.

Застосування "зворотного інжинірингу" регулюється законодавством окремих країн або міжнародними угодами. Здебільшого встановлюють деякі цілком виправдані обмеження у використанні цього методу. Наприклад, призначені для дослідження цим методом вироби мають бути придбані на загальних підставах у місцях їх продажу і розповсюдження. Іноді забороняється відтворення продукції, захищеної будь-яким товарним знаком. Крім того, не можна запрошувати для участі в подібних дослідженнях фахівців, які раніше працювали на підприємстві - виробнику цієї продукції (протягом терміну, обумовленого в контракті під час попереднього працевлаштування).

Канали витоку інформації

Захист мовної інформації є одним із найважливіших у загальному комплексі заходів технічного захисту інформації (ТЗІ). Несанкціоноване ознайомлення із мовною інформацією з метою її подальшого використання є можливим шляхом перехоплення її зловмисниками. Для цього зловмисник може використовувати широкий арсенал портативних засобів акустичної мовної розвідки, які дають змогу перехоплювати мовну інформацію акустичним, віброакустичним, електроакустичним та оптикоакустичним каналами.

Основні з таких засобів:

- малогабаритні диктофони, магнітофони та пристрої запису на основі цифрової схемотехніки;
- спрямовані мікрофони;
- електронні стетоскопи;
- електронні пристрої перехоплення мовної інформації (закладні пристрої) з датчиками мікрофонного й контактного типів з передаванням перехопленої інформації по радіо, оптичному (в інфрачервоному діапазоні хвиль) та ультразвуковому каналах, мережі електроживлення, по телефонних лініях зв'язку, з'єднувальних лініях допоміжних технічних засобів або спеціально прокладених лініях;
- оптико-електронні (лазерні) акустичні системи та ін.

Портативна апаратура звукозапису та закладні пристрої із датчиками мікрофонного типу (перетворювачі акустичних сигналів, що поширюються в повітряному та газовому середовищах) можуть бути встановлені під час неконтрольованого перебування фізичних осіб ("агентів") безпосередньо у виділених приміщеннях. Ця апаратура забезпечує реєстрацію розмови середньої гучності на відстані 10-15 м від її джерела.

Електронні стетоскопи та закладні пристрої з датчиками контактного типу дають змогу перехоплювати мовну інформацію без фізичного доступу

"агентів" до захищуваного приміщення. При цьому датчики закладних пристроїв установлюються переважно біля місць можливих витоків такої інформації:

- мікрофонного типу (біля виходів кондиціонерів та вентиляційних каналів);
- контактного типу (перетворювачі віброакустичних сигналів, що поширюються по будівельних конструкціях споруд, інженерних комунікаціях та ін.) на зовнішніх поверхнях будівель, у віконних проймах та рамах, у суміжних (службових і технічних) приміщеннях за дверними проймами, на перегородках, трубах систем опалення та водопроводу, коробах вентиляційних та інших систем.

Відомо, що за допомогою таких засобів розвідки можна перехоплювати мовну інформацію в залізобетонних будівлях через 1-2 поверхи, по трубопроводах через 2-3 поверхи і по вентиляційних системах 20-30 м завдовжки.

Застосування для ведення розвідки спрямованих мікрофонів і оптико-електронних (лазерних) акустичних систем не потребує проникнення "агентів" не тільки у виділені (захищувані) приміщення та суміжні з ними, а й на охоронну територію об'єкта. Розвідку можна вести із сусідніх будівель чи автомобілів, що перебувають на автостоянках біля будівлі.

За допомогою спрямованих мікрофонів можна перехоплювати розмову із виділених приміщень за наявності в них вікон в умовах міста (на фоні транспортних шумів) на відстані близько 50 м.

Максимальна відстань ведення розвідки з використанням оптико-електронних (лазерних) акустичних систем, які знімають інформацію з внутрішнього скла, сягає 150-200 м в умовах міста (наявність інтенсивних акустичних перешкод, запиленість повітря).

Захисту мовної інформації можна досягти проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням електронних пристроїв перехоплення інформації. Канали витоку мовної інформації можна виявити на об'єкті, знайшовши підслуховувальні пристрої й системи.

Аналіз ризиків дає можливість виявити всі реальні загрози інформаційній безпеці об'єкта, які класифікують за кількома критеріями: за імовірністю прояву, за можливими збитками та ін. На цьому перший етап створення системи захисту інформації об'єкта завершується.

Створюють чи аналізують систему захисту мовної інформації у такій послідовності.

1. Вивчення об'єкта захисту (особливості конструкції будівлі, обстановка навколо об'єкта, опис приміщень та наявних технічних засобів). При цьому виявляють найнебезпечніші місця. В описі приміщення фіксують повну інформацію про приміщення та устаткування, яке в ньому розміщене, щоб у разі потреби можна було виявити можливі канали витоку інформації. Для більш повного виявлення таких каналів (природних і штучних) проводять

інструментальну перевірку. Виявлення природних каналів полягає у визначенні потенційної можливості перехоплення мовної інформації із приміщень об'єкта. Природні канали існують на будь-якому об'єкті і зумовлені процесами оброблення та передавання інформації. Виявлення штучних (спеціальних) каналів витоку інформації зводиться до виявлення на об'єкті підслуховувальних пристроїв і систем. Інструментальну перевірку можуть проводити організації, що мають відповідну ліцензію на це.

2. Побудова "часткових" моделей порушників і загроз за даними, отриманими на першому етапі. При цьому користуються загальними рекомендаціями щодо створення моделей порушників і загроз.

3. Виконання робіт зі створення системи захисту у складі організаційних, первинних технічних та основних технічних заходів (див. відповідні рекомендації). За наявності на об'єкті приміщень, де циркулює таємна інформація (приміщення 1-3 категорій), обов'язково проводять атестацію (державну експертизу) засобів інформатизації й технічного захисту інформації (див. відповідні рекомендації).

Розглянемо оснащення об'єкта засобами захисту мовної інформації на прикладі оснащення кабінету керівника фірми.

Припустімо, що в результаті інженерного аналізу та інструментальної перевірки в приміщенні було виявлено можливі функціональні канали витоку інформації (табл. 11.1).

Таблиця 11.1.

Функціональні канали витоку інформації у приміщенні

Канал витоку інформації	Опис
Акустичний	Мембранне перенесення енергії мовних сигналів через перегородки за рахунок малої маси і слабкого згасання сигналів
Акустичний	Витік інформації за рахунок слабкої акустичної ізоляції (щілини в стояках системи опалення, вентиляції")
Вібраційний	Витік інформації за рахунок поздовжніх коливань огороджувальних конструкцій і арматури системи центрального опалення
Електронні пристрої перехоплення мовної інформації із телефонних ліній зв'язку	Знімання інформації з телефонної лінії
ПЕМВН	Витік інформації за рахунок модуляції корисним сигналом ЕМ-полів. що утворяться під час роботи побутової техніки

За даними табл. 11.1 розробляють "часткову" модель порушника. Технічні можливості порушника перехоплення мовної інформації подано в табл. 11.2 як фрагмент його "часткової" моделі.

Таблиця 11.2.

Технічні можливості порушника з перехоплення мовної інформації

Вид апаратури	Варіант використання	Імовірність застосування
Радіомікрофони	Заносні, заставні	Імовірно
Апаратура перехоплення телефонних переговорів	Різні передавальні пристрої, які використовують як канали передачі через радіоефір або телефонну лінію	Імовірно
Мережні системи	Передача мережею 220В	Імовірно
Портативна звукозаписна апаратура	Запис інформації учасниками переговорів	Імовірно
Апаратура оптичної розвідки	Фото-, відеознімання обстановки в приміщенні	Імовірно
Кабельні (дротові) мікрофони	Закладені з верхніх помешкань у підвісну стелю	Малоймовірно
Стетоскопічні датчики	Дротові й радіостетоскопи	Імовірно
Спрямовані мікрофони	Тільки за відкритих вікон, кватирок	Малоймовірно
Лазерні мікрофони	Зняття інформації із шибки	Малоймовірно
Системи для перехоплення ПЕМВН устаткування, промодульованих мовним сигналом	Селективні нановольтметри. спеціалізовані комплекси	Малоймовірно

Система захисту інформації, на думку власника, має забезпечити:

- оперативне і непомітне для оточення виявлення активних радіомікрофонів, занесених у приміщення, що мають традиційні канали передавання інформації;
- протидію виявленим радіомікрофонам із традиційним каналом передавання інформації;
- протидію перехопленню інформації, переданої по телефонній лінії (на ділянці до АТС);
- протидію занесеним у приміщення диктофонам і схованим відеокамерам;
- протидію апаратурі, що використовується для передавання сигналів у мережу 220В;
- протидію кабельним і радіостетоскопам;
- протидію веденню фотовізуальної й оптико-електронної розвідки;
- протидію спробам несанкціонованого доступу до інформації, що зберігається на твердому диску ПЕОМ;
- реєстрацію телефонних переговорів двома телефонними лініями.

У результаті аналізу технічних вимог до системи захисту інформації слід

обрати варіант комплексу засобів захисту мовної інформації з використанням засобів, які є в Україні сертифікованими чи мають узгоджені технічні умови (табл. 11.3).

Таблиця 11.3.

Сертифіковані в Україні засоби захисту мовної інформації

Назва технічного засобу	***Основні характеристики***
Пристрій для захисту телефонних ліній ПЗТЛ "Рікас-1, "Рікас-2"	*Призначений для захисту мовної інформації від витоку абонентськими телефонними лініями внаслідок акустоелектричного перетворення в телефонному апараті в режимі "очікування виклику"*
Захисний пристрій "Базальт-3"	*Для захисту мовної інформації від витоку двопровідними лініями телефонного зв'язку внаслідок акустоелектричного перетворення в кінцевих абонентських пристроях, які перебувають у режимі "очікування виклику"*
Пристрій для захисту телефонного апарата (ПЗТА)	*Захист від загроз несанкціонованого доступу до мовної конфіденційної інформації, зокрема: о внаслідок високочастотного "нав'язування" в телефонному апараті, який перебуває в режимі "очікування виклику", з візуальною та звуковою індикацією загрози о за рахунок підключення телефонного апарата до лінії тільки в разі підняття телефонної трубки чи за наявності сигналу виклику Не призначений для захисту інформації, що містить відомості, які становлять державну таємницю*
Пристрій захисту "Базальт-1"	*Захист мовної інформації від витоку двопровідними лініями гучномовного зв'язку внаслідок акустоелектричного перетворення в кінцевих пристроях*
Пристрій захисту "Кварц-2"	*Генерація шумових сигналів у звуковому діапазоні частот*
Пристрій захисту "Базальт-4 ГА"	*Генерація шумових сигналів. Захист мовної інформації від витоку акустоелектричними та віброакустичними каналами*
Пристрій захисту "Базальт-2ГС"	*Генерація шумових сигналів. Захист мовної інформації від витоку двопровідними лініями електричного живлення внаслідок акустоелектричного перетворення*
Пристрій захисту інформації в аналогових телефонних абонентських лініях ПЗАТЛ	*Захист мовної інформації в аналогових абонентських лініях в режимі "очікування виклику" шляхом маскування шумоподібним сигналом. Додаткова функція захисту: неможливість набору номера з телефону, який підключається до абонентської лінії між пристроєм ПЗАТЛ та АТС*
Пристрій захисту телефонних та радіотрансляційних ліній (ПЗТРЛ) "Топаз-1"	*Захист мовної інформації від витоку лініями телефонного зв'язку і радіотрансляції за рахунок акустоелектричних перетворень та високочастотного зондування у кінцевих пристроях*
Комплекс технічного захисту інформації об'єкта "МАРС-ТЗО"	*Захист інформації на об'єктах від витоку інформації акустичним та віброакустичним каналами шляхом створення шумових сигналів у діапазоні частот від 180 до 5600 Гц*
Комплекс технічного захисту інформації об'єкта "МАРС-ТЗО^"	*Захист інформації на об'єктах від витоку інформації акустичним та віброакустичним каналами шляхом створення шумових сигналів у діапазоні частот від 180 до 5600 Гц*

У конкуретно-ринкових відносинах виникає багато проблем щодо збереження конфіденційної (комерційною) інформації. Адже бізнес тісно пов'язаний з отриманням, накопиченням, зберіганням, обробленням і використанням різних масивів інформації. Якщо інформація є цінною, то факт

таємного отримання її конкурентом приносить йому певний дохід, водночас ослаблюючи позиції тих, хто протистоїть йому на ринку.

Можливе також внесення певних змін в інформацію з корисливою метою, наприклад з метою дезінформації. Проте внести такі зміни нелегко, оскільки для правдоподібності її треба узгоджувати із загальним ходом подій за часом, місцем, метою і змістом, для цього потрібно добре знати обстановку в конкуруючій фірмі. Тому більш поширеною і небезпечною метою є знищення накопичених інформаційних масивів або програмних продуктів у документальній і магнітній формі.

4. ОХОРОНА ТАЄМНИЦЬ ПІДПРИЄМСТВА ТА ЇЇ НАЛАГОДЖЕННЯ

Світовий досвід захисту комерційних таємниць фірм показує, що успіх у цій справі дає тільки комплексний підхід, котрий поєднує адміністративно-організаційні й соціально-психологічні заходи. До перших належать:

- наявність служби безпеки, що відповідає, поряд з іншим, зі збереження комерційних таємниць;
- організація спеціального діловодства, що включає класифікацію документів за ступенем і терміном їх секретності, відповідний облік, зберігання, використання, знищення або розсекречення;
- оптимальне обмеження кількості осіб, що мають доступ до комерційних таємниць фірми, дотримання ними правил користування конфіденційною інформацією;
- наявність охорони на всіх об'єктах фірми, встановлення там, де потрібно, пропускного і внутрішньооб'єктного режиму;
- проведення заходів, що запобігають (або істотно ускладнюють) використанню конкурентами технічних засобів перехоплення або знімання інформації з її носіїв.

Розробляючи систему заходів захисту комерційних таємниць фірми, працівник, що відповідає за безпеку, має зробити таке:

1) скласти (разом із керівництвом та експертами) перелік відомостей, що становлять комерційну таємницю, в якому виділити найбільш цінну інформацію, що потребує особливої охорони;

2) установити терміни, протягом яких ті чи інші відомості секретними (або закритими для сторонніх осіб);

3) виділити категорії носіїв таємної й закритої інформації - конкретних працівників; документи, вироби, матеріали, технічні засоби зберігання, обробки, тиражування і передачі інформації; фізичне випромінювання;

4) перелічити просторові зони і час матеріалізації комерційної таємниці в носіях інформації (місця і час переговорів, ярмарків, виставок, нарад тощо);

5) скласти схему робіт з конкретними відомостями, матеріалізованими в конкретних носіях, з прив'язкою цих захисних заходів до місця й часу.

Усі елементи системи захисту комерційних таємниць фірми потрібно

постійно аналізувати для оцінювання її фактичного стану, виявлення недоліків і порушень. Такий аналіз має передбачати також моделювання вірогідних каналів витоку інформації, можливих прийомів і способів її несанкціонованого отримання конкурентами.

Зарубіжні фахівці найбільш вірогідними каналами просочування конфіденційної інформації вважають:

- спільну діяльність з іншими фірмами;
- проведення переговорів;
- екскурсії і відвідини фірми;
- рекламу, публікації у пресі, інтерв'ю для преси;
- консультації фахівців зі сторони, які отримують доступ до документації, яка стосується виробничої діяльності фірми;
- фіктивні запити про можливість роботи на фірмі, висновки з її операцій, здійснення спільної діяльності;
- розсилання окремим працівникам фірми різних анкет у вигляді наукових або маркетингових досліджень;
- приватні бесіди із працівниками фірми, нав'язування їм незапланованих дискусій з тих чи інших проблем.

Аналіз системи захисту комерційних таємниць, моделювання вірогідних загроз дає змогу намічати за потреби додаткові заходи безпеки. При цьому ступінь їх доцільності визначають виходячи з того, що витрати на забезпечення належної секретності мають бути істотно меншими, ніж можливий економічний збиток.

Проте, як кажуть, "ступінь надійності будь-якого шифру визначається не його складністю, а непідкупністю шифрувальника". Тобто, ключовими фігурами систем захисту комерційних таємниць є працівники фірм, причому не тільки ті, що працюють із закритою інформацією. Рядовий працівник, що не має доступу до комерційної таємниці, теж може надати допомогу конкурентам у електронному шпигунстві, забезпечити умови для розкрадання носіїв інформації, для зняття копій.

На думку зарубіжних фахівців, вірогідність витоку відомостей, які становлять комерційну таємницю, при проведенні таких дій, як підкуп, шантаж, переманювання працівників фірми, впровадження своїх агентів, становить 43%; отримання відомостей вивідуванням їх у працівників - 24%. Отже, персонал фірми є, з одного боку, найважливішим ресурсом підприємницької діяльності, а з другого - окремі працівники з різних обставин можуть стати винуватцями великих втрат і навіть банкрутства фірми. Саме тому організаційні й адміністративні заході захисту конфіденційної інформації потрібно поєднувати із соціальна психологічними заходами.

Можна виділити два напрями проведення соціально-психологічних заходів захисту: 1) правильний підбір і розстановка персоналу; 2) використання матеріальних і моральних стимулів.

Західні фахівці з економічної безпеки вважають, що від правильного підбору, розстановки і стимулювання персоналу збереження фірмових

таємниць залежить як мінімум на 80%!

У поняття підбору персоналу входить насамперед вивчених професійної придатності кандидатів на посади, вибір серед них тахін, що найбільше відповідають поставленим вимогам. Для правильного підбору визначальну роль відіграє всебічна інформація про особу кандидата та його попередню діяльність.

Завдання підприємця - надійно перекрити канали просочування конфіденційної інформації. Коли на підприємстві визначено перелік відомостей, що становлять комерційну таємницю, то потрібно зазначити джерела витоку цієї конфіденційної інформації. Потенційними джерелами витоку комерційної таємниці можуть бути:

1. Документація підприємства або просто документи (накази, бізнес-плани, ділове листування тощо). Це найпоширеніша форма обміну інформацією, її накопичення та зберігання. Важливою особливістю документів є те, що вони іноді є єдиним джерелом найважливішої інформації (наприклад, контракт, боргова розписка та ін.), а отже, їх втрата, викрадання, знищення можуть завдати непоправного збитку. Структура документів підприємства є предметом окремого розгляду, оскільки документи можуть мати не тільки різний зміст, а й різні фізичні форми - матеріальні носії. Різноманітність форм і змісту документів за призначенням, спрямованістю, характером руху і використанням є вельми принадним джерелом для зловмисників, що, природно, привертає їх увагу до можливості отримання інформації, яка їх цікавить.

2. Персонал підприємства (усі, хто працює тут, у тому числі й керівник). У деяких джерелах конфіденційної інформації люди відіграють особливу роль, оскільки здатні виступати не тільки джерелом, а й суб'єктом зловмисних дій. Вони не тільки володіють і розповсюджують інформацію в рамках своїх функціональних обов'язків, а й можуть аналізувати, узагальнювати її, робити певні висновки, а також за певних умов приховувати, продавати її та вчиняти інші кримінальні дії, аж до злочинних зв'язків із зловмисниками.

3. Партнери, контрагенти або клієнти, що користуються або користувалися послугами підприємства, найбільш обізнані із джерелами найважливіших секретів фірми. Тому вони заслуговують ретельної уваги під час аналізу системи захисту.

4. Вироблена продукція або надані послуги. Продукція є особливим джерелом інформації, за характеристиками якої активно полюють конкуренти. Заслуговує на увагу нова або така, яку готують для виробництва, продукція. Враховують етапи її "життєвого циклу": задум, макет, дослідний зразок, випробування, серійне виробництво, експлуатація, модернізація і зняття з виробництва. Кожен із цих етапів супроводжується специфічною інформацією, що виявляється різними фізичними ефектами, які у вигляді демаскувальних ознак можуть розкрити відомості, що охороняються.

5. Технічні засоби забезпечення виробничої діяльності. Ці засоби є широкою і ємкою групою джерел конфіденційної інформації. До групи засобів забезпечення виробничої діяльності належать, зокрема, телефони і телефонний

зв'язок, телевізори і промислові телевізійні установки, радіоприймачі, радіотрансляційні системи, системи гучномовного зв'язку, підсилювальні системи, кіносистеми, охоронні й пожежні системи та інші, які за своїми параметрами можуть бути джерелами перетворення акустичної інформації в електричні й електромагнітні поля, здатні утворювати електромагнітні канали просочування конфіденційної інформації..

6. Непрямі джерела (відходи виробництва, реклама, публікації у пресі). Більшість інформації можна отримати саме з непрямих джерел. Професійно проведена аналітична робота іноді дає чудовий результат. Зазвичай цьому джерелу не надають особливої уваги, тому воно є найбільш доступним. Наприклад, відходи виробництва, які називають непотребом, можуть багато про що розповісти щодо використовуваних матеріалів, їх складу, особливостей виробництва, технології. І отримати їх можна майже безпечним і законним шляхом на звалищах, смітниках, у місцях збору металобрухту, в корзинах для сміття в робочих кабінетах. Умілий аналіз цих відходів може багато що розповісти про секрети виробництва. У публікаціях - книгах, статтях, монографіях, оглядах, повідомленнях, рекламних проспектах, доповідях, тезах та ін.: можна мимовільно розкрити всі виробничі таємниці.

Із джерел конфіденційної інформації можна мати дані про склад, зміст і напрям діяльності підприємства (організації), що цікавить конкурентів. Природно, що така інформація їм украй потрібна, і вони знайдуть способи отримати її.

Тому грамотна система захисту, розроблена з урахуванням усіх її особливостей, дасть змогу запобігти багатьом проблемам.

Документація підприємства

Не всі документи фірми можуть містити комерційну таємницю. Зокрема, не містять комерційної таємниці:

- засновницькі документи, а також такі, що дають право на заняття підприємницькою діяльністю і деякими видами господарської діяльності, що піддягає ліцензуванню;
- документи за затвердженими формами статистичної звітності та звітності про фінансово-економічну діяльність, необхідні для перевірки правильності розрахунків і сплати податків та інших обов'язкових платежів;
- документи про сплату податків та інших обов'язкових платежів;
- документи, що засвідчують платоспроможність фірми;
- документи про чисельність, склад персоналу, заробітну плату та умови праці працівників, а також про наявність вільних робочих місць;
- документи про забруднення навколишнього середовища, порушення антимонопольного законодавства, недотримання правил охорони праці, реалізацію продукції, яка завдає шкоди здоров'ю споживачів, а також про інші порушення законодавства й розміри завданого при цьому збитку.

Проте важливим є будь-який документ. Навіть малозначущий документ за певного збігу обставин може виявитися надзвичайно важливим. Організація контролю за документацією підприємства дає змогу уникнути плутанини, адже на будь-якому підприємстві робочих документів дуже багато. Крім того, належна система обліку й контролю документів дасть змогу запобігти багатьом проблемам, причому не тільки у сфері безпеки. Відомі численні випадки, коли втрата чи випадкове знищення фінансових і ділових документів завдавали величезних збитків підприємству. Наведемо приклад: між двома підприємствами виникла суперечка з приводу виконання одного з договорів. Тоді одна з фірм попросила в другої фірми оригінал договору для ознайомлення. Отримавши договір, вона відмовилася виконувати його, стверджуючи, що такого договору не було. Та оскільки належної системи обліку і контролю документів на фірмі не було і договір вона віддала партнеру "під чесне слово", то мала серйозні проблеми у вирішенні суперечки.

Що ж являє собою система контролю і обліку документів? Узагальнено вона охоплює:

1. Облік усієї документації підприємства з класифікацією за сферою застосування, датою, змістом тощо.

2. Реєстрацію і облік усіх вхідних/вихідних документів підприємства з фіксацією у спеціальному журналі дати отримання/ відправлення документа, місця надходження або відправлення, класифікації (лист, рахунок, договір, запрошення тощо).

3. Реєстрацію документів, з яких роблять копії з фіксацією у спеціальному журналі (дата копіювання, кількість копій, для кого або з якою метою зроблено копії та ін.).

4. Дані про особливий режим знищення документів. Перед цим потрібно проконтролювати їх зміст, щоб уникнути випадкового знищення потрібних документів. Важливо, щоб документи, викинуті в корзину, були подрібнені за допомогою "шредера" (знищувача паперу) або вручну так, щоб їх неможливо було б відновити. Особливо цінні документи після подрібнення доцільно спалити. Про знищення документів обов'язково складають акт, який підписує відповідальна особа, а також особи, присутні при знищенні документів.

Для впорядкування системи контролю всі документи треба поділити на три категорії: 1) загального користування; 2) для службового користування; 3) таємні.

Поділ документів на категорії не є разовим заходом. Нові документи обов'язково оцінюють, після чого визначають категорію. Крім того, має діяти регулярна система "переоцінок", оскільки з часом або настанням певних подій ті чи інші документи можуть набувати нового або втрачати своє значення, тобто переходити з однієї категорії в іншу.

Документи різних категорій різняться не тільки призначенням, а й колом осіб, що мають доступ до них. Кожній категорії привласнюють свій гриф за допомогою штампів, спеціальних відміток або роблять їх різного кольору (наприклад, документи загального користування ~ білі, службового - жовті,

таємні - червоні).

Важливо, щоб ця система була ефективною. Для цього потрібно провести відповідну роз'яснювальну роботу з персоналом, а також інструктаж.

Краще, коли роботу з контролю за документами доручено окремому працівникові (наприклад, інспекторові режиму роботи з документами), в ідеалі цим займається група режиму служби безпеки підприємства.

Крім того, доцільно ухвалити відповідне положення про документообіг підприємства, у якому подані правила роботи з документами, особливості роботи з документацією, що має конфіденційний характер.

Розглянемо докладніше, як працювати з кожною категорією документів.

1. Документи загального користування підлягають попередньому контролю змісту, після чого беруть участь в документообігу (копіювання, передавання, пересилання тощо). Знищують їх у звичайному порядку, обов'язково здійснюючи системний контроль для уникнення плутанини.

2. Документи службового користування підлягають обов'язковому попередньому контролю їх змісту. їм привласнюють гриф "Для службового користування" і ознайомлюють з ними персонал, можливо, обмежене коло працівників з обов'язковим інструктажем щодо нерозголошення таємниці. Обов'язковою є систематизація і облік цих документів у відповідному реєстрі. Копіювати їх можна тільки в разі потреби. Кількість копій обмежена, за потреби записують кількість копій, мету копіювання і для кого зроблено копію. Знищують такі документи за спеціальним режимом (під контролем відповідального працівника із складання акта).

3. Секретні документи. Обов'язково контролюють їх зміст, привласнюють їм гриф "комерційна таємниця", "таємно" або інший. Ознайомлюють з ними тільки осіб, що мають до них доступ. Обов'язково складають список осіб, ознайомлених з інформацією. Бажано під час ознайомлена з цими документами брати підписку про нерозголошення таємниці. Копіювання можливе тільки з дозволу відповідального працівника з обов'язковою фіксацією кількості копій, мети копіювання і для кого зроблено копію. Знищує такі документи в особливому режимі відповідальний працівник (попереднє ознайомлення зі змістом документа, повне його знищення, зокрема й залишків, складання акту про знищення).

До будь-якого зникнення чи знищення документів, що містять важливу інформацію, потрібно ставитися відповідально. Обов'язково треба проводити внутрішнє розслідування. Результати його за потреби досліджують. Особи, винні у втраті документів, мають бути притягнуті до дисциплінарної відповідальності, а іноді - позбавлені доступу до документів, що містять комерційну таємницю. Важливо, щоб розслідування не було формальним, а з його результатів зроблено належні висновки. Допущені помилки мають бути виправлені за максимально короткий час.

Корисно випадки втрати чи знищення документів надалі використовувати як приклад під час інструктажу для працівників і служби безпеки.

Не слід забувати прості правила обережності під час роботи з

документами:

- не треба робити непотрібних копій документів;
- чернетки і начерки таємних документів потрібно знищити;
- таємні документи зберігати окремо від іншої документації, бажано в ізольованому приміщенні з обмеженим доступом;
- не варто тримати копіювальну техніку в одному приміщенні з документами, що становлять комерційну цінність, для того щоб уникнути їх несанкціонованого копіювання;
- не можна залишати документи на робочому місці без нагляду, навіть на короткий час;
- не можна, щоб сторонні особи читали, нехай навіть і випадково, робочі документи, що лежать на столі або в кабінеті працівника. У разі появи сторонньої особи документи потрібно прибрати у сховище, шафу, ящик столу;
- потрібно встановити заборону на винесення працівниками документів за межі підприємства без попереднього дозволу особи, відповідальної за збереження комерційної таємниці.

Люди - джерела конфіденційної інформації

Чому люди є найуразливішим джерелом конфіденційної інформації? Та тому, що це джерело найважче захистити від несанкціонованого "втручання". Адже якщо документи можна заховати в сейф, засекретити, обмежити доступ до них, непотрібні - знищити, то людину в сейф не засунеш, на рота їй замок не поставиш.

Крім того, людина є не просто вмістищем інформації, не просто її носієм, а ще й обробляє та аналізує інформацію, робить певні висновки Отже, отримавши та опрацювавши лише частину інформації, вона може оволодіти всією інформацією, не кажучи вже про ту, яка їй відома, може легко відтворювати, копіювати й поширювати дані.

Персонал підприємства часто володіє безцінною комерційною інформацією. Працівники іноді знають більше, ніж можна припустити, про фінансовий стан підприємства, його перспективні розробки та бізнес-плани, про комерційні пропозиції, про ділових партнерів, не кажучи вже про різні дані про керівників та ін. І підприємці не застраховані від того, що ця інформація не стане доступною для треш осіб. Що ж робити в такому разі, як обмежити можливість розголошування конфіденційної інформації персоналом? Відповідь дуже проста - потрібно розробити заходи, які дають змогу контролювати доступ до комерційних секретів підприємства.

З чого почати? З поділу інформації за рівнем доступу. На будь-якому підприємстві персонал умовно може бути поділений натри групи:

1. Керівники:

а) вищої ланки (власник підприємства, засновники, президент, начальник служби безпеки);

б) середньої ланки (начальники відділів і служб, менеджери та ін.).

2. Фахівці (найбільш численна група, до якої належать працівники, що володіють спеціальними знаннями і безпосередньо виконують основну роботу підприємства).

3. Обслуговуючий і технічний персонал (вантажники, різнороби, прибиральниці та ін.).

Очевидно, що всі ці групи мають володіти різними обсягами інформації. Керівники підприємства повинні мати доступ до будь-якої інформації, що стосується діяльності підприємства; керівники підрозділів - до інформації, що стосується роботи вверeного підрозділу; фахівці - до такого обсяг} інформації, який потрібен їм для професійного і добросовісного виконання своїх професійних обов'язків; обслуговуючий і технічний персонал мають мінімальний доступ до конфіденційної інформації. При допуск)' робочого персоналу до конфіденційної інформації слід керуватися золотим правилом: чим менше особа знає про щось, тим менше вона може розповісти.

Наведемо цікавий приклад. Відомо, то військовослужбовець нашої армії зобов'язаний захищати всі відомі йому дані, навіть ціною власного життя. Ці положення давно закріплені у військовій присязі. А в армії Ізраїлю - навпаки: потрапивши в полон, солдат зобов'язаний розповісти все, що йому відомо. Представники Ізраїлю говорять, що не робиться для того, щоб врятувати людське життя: людина для них - найбільша цінність, і ніяка інформація не варта життя солдата. Але така позиція, крім морально-психологічного аспекту, містить прагматичний підхід. Справа в тому, що кожен військовослужбовець знає рівно стільки, скільки йому належить. Отже, солдат не зможе видати стратегічно важливої інформації. Крім того, дізнавшись, хто потрапив у полон, можна легко й достовірно встановити, який обсяг і якої саме інформації став відомий ворогові, а не гадати, чи видав солдат інформацію, чи ні, і якщо видав, то яку саме. Завдяки цьому помітно спрощується нейтралізація наслідків розголошення секретної інформації. Цей приклад наочно ілюструє ефективність і дієвість такої системи, яку доцільно запозичити в ізраїльських військових і впровадити на підприємстві. Звичайно, не варто сприймати все буквально і дозволяти своїм працівникам розголошувати конфіденційні відомості. Якраз навпаки, їх треба проінструктувати про необхідність збереження інформації в таємниці. Але потрібно бути готовим до того, що персонал може видати цю інформацію. Тому відповідна система заходів дасть змогу застрахувати себе від серйозних втрат у разі розголошення таємниць підприємства. Цей комплекс заходів умовно можна назвати попередньою перевіркою працівників під час приймання на роботу. Аналізуючи нинішнє становище ринку праці, можна виділити такі основні методи підбору персоналу:

- оголошення в газетах;
- оголошення конкурсу на заміщення вакантної посади або на вакантне місце;
- підбір персоналу через кадрове агентство;
- наймання працівників по знайомству, простіше, "по блату", за гроші.

Кожен із зазначених способів має свої недоліки і переваги. Перші два

загалом прийнятні за обов'язкового дотримання умов, викладених нижче. Проте основний їх недолік у тому, що, самі того не бажаючи, опублікувавши оголошення про приймання на роботу, ви можете розголосити цінну інформацію комерційного характеру. Наприклад, один банк, опублікувавши у пресі оголошення про приймання на роботу фахівців із галузі пластикових кредитних карток, побічно розкрив цінну комерційну інформацію, а саме те, що найближчим часом він збирається вийти на ринок безготівкових розрахунків за допомогою кредитних карток.

Тому краще за все здійснювати підбір персоналу через кадрове агентство, яких нині багато. Дехто накопичує базу даних вакансій і резюме, не спромігшись перевірити кандидата. Отже, говорити про те, що пропоновані таким агентством працівники справді підійдуть, не можна. Адже вони не проходять ніяких перевірок - ні за рівнем підготовки, ні за особистими якостями, а агентство не несе ніякої відповідальності за свого кандидата. Тому дуже важливо ретельно підбирати справді надійне і професійне агентство з наймання, бо тільки звернення по допомогу до нього позбавить від безлічі клопоту і, крім того, забезпечить конфіденційність.

На жаль, керівники підприємств часто вдаються до наймання працівників по знайомству або за гроші. Таку практику слід вважати неправомірною, не кажучи вже про те, що такі дії можуть бути кримінально караними. Чому прийнято вважати, що родичі чи знайомі мають незаперечні переваги перед рештою кандидатів. Влаштовані по блату здебільшого виявляють найгіршу підготовку. Саме вони часто вчиняють різні порушення й розкрадання майна, будучи абсолютно впевненими у своїй безкарності. Адже, якщо працівник, що провинився, негайно буде звільнений, то родича або знайомого так просто звільнити буде незручно. Крім того, узявши на роботу такого "блатника", отримують "бомбу сповільненої дії"", яка коли-небудь та вибухне. Такі працівники часто думають, що їм на підприємстві все дозволено, поводяться зарозуміло стосовно інших, вважаючи, що дисципліна праці й загальні правила на них не поширюються.

Таким чином, на підприємстві формується вельми негативна атмосфера незадоволеності. Напевно, тому вже нині на деякі фірми (переважно іноземні) достатньо складно влаштуватися, якщо там працюють ваші родичі, а якщо вони ще й займають керівні посади - практично неможливо.

Попередня перевірка. Припустімо, працівник уже стоїть на порозі з твердим бажанням влаштуватися на роботу. Починати завжди треба із бесіди (інтерв'ю) з ним, ретельно підготувавшись до неї. Адже саме з інтерв'ю можна дізнатись багато чого. Корисно при цьому скористатися допомогою психолога. Професійний психолог, поговоривши з людиною, зможе з високою вірогідністю дати висновок про її професійні й особисті якості, про те, наскільки вона чесна і чи зможе вписатися в колектив фірми. Сьогодні вже існують спеціальні послуги з психологічного тестування кандидатів на посаду, які дають досить високі результати. Якщо такі послуги є недоступними, доведеться самим ставати психологом.

По-перше, в жодному разі не слід створювати атмосферу допиту, аби не зашкодити собі. Чесна й порядна людина, відчувши негативне ставлення до себе, може відмовитися від роботи. А зловмисник, навпаки, зачаїться, насторожиться, вміло приховає свої наміри.

По-друге, не слід поводитися зарозуміло, вважаючи, що коли людина прийшла влаштовуватися на роботу, то вона вже вам всім зобов'язана і все терпітиме.

По-третє, ніколи заздалегідь нічого не потрібно обіцяти: говоріть лише про реальні речі. Краще за все створити дружню атмосферу взаєморозуміння. Тоді кандидат трохи розслабиться і зможе говорити відвертіше. А ви при цьому уважно стежте, як людина поводиться, що і як говорить, наскільки скута чи, навпаки, розкута, скромна чи хвалькувата. Доцільно заздалегідь ознайомитися із спеціальними матеріалами. Деякі працедавці влаштовують кандидатам на посаду докладну екскурсію на підприємстві, ознайомлюючи з особливостями майбутньої роботи, чого не варто робити до попередньої перевірки. Можливо, ця людина не підійде, тоді краще, коли вона знатиме якомога менше.

Наступним кроком є перевірка достовірності документів і минулого кандидата. Насамперед слід установити його особу - найпростіше за паспортом. Потім потрібно з'ясувати робоче минуле кандидата - з трудової книжки, де зазначено попередні місця роботи, заохочення, причини звільнення;тощо. При цьому варто бути обережним: бланки трудових книжок нині можна купити на будь-якому ринку і заповнити як спаде на думку. Крім того, часто працівники тільки числяться в штаті підприємства, а насправді не виконують ніякої роботи або завдяки "зв'язкам" чи дружнім взаєминам отримували необхідні записи в трудовій книжці.

Не завадить також з'ясувати думку про кандидата його попередніх працедавців і людей, з якими він працював або вчився. Тому незайве попросити його заповнити картку обліку кадрів, надати автобіографію, характеристику з останнього місця роботи або рекомендації. Так само потрібно переконатися в професійній придатності кандидата - попросити надати документ про освіту (диплом про вищу освіту, диплом про закінчення коледжу, СПТУ, ПТУ, атестат та ін.). Складіть анкету для кандидата на посаду так, щоб дізнатися про нього якнайбільше, зокрема, про його близьких родичів, особисті інтереси, спортивні й наукові досягнення і т.ін. Не зайвим буде з'ясувати, чи не мав він раніше судимостей, чи не перебував на обліку в психо - чи неврологічному диспансері Якщо такої можливості немає, можете попросити кандидата надати необхідні довідки.

Але не слід вимагати від працівника документів, які не передбачені чинним законодавством! Припустімо, ви перевірили всі відомості, що цікавлять вас, про кандидата і тепер повинні прийняти одне з таких рішень: узяти його на роботу; відмовити. Розглянемо обидва варіанти. Отже, людина з якихось причин не підходить і потрібно відмовити їй у прийнятті на роботу. Як це зробити без істотного збитку для неї, головне - без збитку для підприємства? Справді, якої шкоди може завдати відмова прийняти когось на роботу?

Якщо ви різко відмовляєте людині в прийнятті на роботу, говорите, що вона недостатньо розумна, що в неї диплом не того формату, що вам не підходить колір її волосся або щось інше, то будь-яка нормальна людина після такої відмови затаїть образу, прийде додому, розповість про все своїм близьким, а також друзям, знайомим, а ті, у свою чергу, своїм друзям і знайомим. І піде негативна інформація, як круги по волі від кинутого каменя. Адже все це ваші потенційні клієнти. Можуть поширитись погані розмови про підприємство, які негативно позначаться на його діловій репутації. Як результат - зниження кількості клієнтів, обсягів замовлень, тобто прямий матеріальний збиток у вигляді недоотриманого прибутку.

Не забувайте, що кандидат на посаду під час приймання на роботу має певні гарантії, передбачені трудовим законодавством. Зокрема, не допускається пряме або непряме обмеження прав чи надання прямих або непрямих переваг при прийманні на роботу залежно від раси, національності, мови, соціального походження, майнового стану, міси" проживання, ставлення до релігії, переконань, належності до громадських об'єднань та інших обставин, не пов'язаних з діловими якостями працівників. Недотримання цих вимог може бути підставою подачі позову до суду про необґрунтовану відмову в прийманні на роботу. А це додаткові витрати на адвоката, додаткові витрата часу і нервів, до того ж і погана реклама для підприємства.

Тому відмова в прийнятті на роботу маг бути виражена м'яко й делікатно. При цьому доцільно уникати особистого контакту і кандидатом, краще послати йому відмову у письмовій формі поштою, ввічливо подякувавши за співпрацю і вибачившись за витрачений ним час. Якщо причиною відмови була негативна інформація про кандидата, яку отримали у процесі попередньої перевірки, не слід повідомляти йому про це. Багато бізнесменів, бажаючи показати свою обізнаність, розповідають про кандидата все, що їм вдалося дізнатися, насторожуючи цим його і примушуючи краще приховувати інформацію про себе. Тому, пояснюючи причини відмови, краще не інформувати кандидата про справжні мотиви, а створити в нього враження, він не підійшов з інших причин.

Якщо працівник підходить за діловими (трудовими) і людськими якостями, то для оформлення його на роботу можна використати наведені нижче способи, які дають змогу певним чином запобігти розголошуванню новим працівником комерційної таємніші.

1. Оформити приймання на роботу наказом, виданим на підставі заяви працівника про прийняття на роботу. При цьому інструктаж працівника та ознайомлення його з правилами, установленими на підприємстві, і положеннями (у т.ч. з Положенням про збереження комерційної таємниці) проводять до фактичного доступу працівника до роботи. Про ознайомлення з положеннями працівник лаг підписку встановленого зразка. Якщо на підприємстві немає таких зразків, то працівник може поставити розписку при ознайомленні з наказом про прийняття на роботу. Зміст її може бути таким:

"Із наказом і положеннями, що існують на менші, ознайомлений і зобов'язуюся їх дотримувати. Кісні роз пенсію, що в разі порушення існуючих

положень я нестиму відповідальність згідно з чинним законодавством".

З приводу розписок досі є різні погляди. Дехто вважає їх неефективними. Законодавство регулює ці питання дуже недосконало. Крім того, не визначено практичного механізму дозволу за таких ситуацій.

Проте є і позитивні моменти. По-перше, будь-яке зобов'язання зазвичай справляє великий морально-психологічний вилив на людину. Більшість людей прагнуть дотримувати навіть формальних зобов'язань, що залежить переважно від порядності працівника і роботи служби безпеки.

По-друге, якщо працівник порушить свої зобов'язання, то, відповідно до закону, нестиме дисциплінарну відповідальність. А якщо належним чином потурбуватися про юридичне забезпечення відшкодування заподіяного збитку, то можна мати позитивні результати.

2. Оформити приймання на роботу наказом, виданим на підставі укладеного з працівником індивідуального трудового договору. До трудового договору вводять окремий пункт про те, що працівник ознайомлений із положеннями, чинними на підприємстві, і зобов'язується їх дотримувати, а в разі їх порушення нестиме відповідальність. У цьому разі перед укладенням трудового договору потрібно провести інструктаж і надати працівникові для ознайомлення всі чинні положення (Положення про персонал, Положення про оплату праці, Положення про безпеку праці, Правила внутрішнього трудового розпорядку, Положення про збереження комерційної таємниці і т.ін). Підписавши договір, працівник автоматично зобов'язується дотримувати всіх зазначених положень. Інструктаж працівника не може бути формальним. Потрібно ознайомити його зі всіма правами і обов'язками. Це убезпечить у майбутньому не тільки від можливого просочування конфіденційної інформації, а й від багатьох інших бід (нещасних випадків на виробництві, непорозуміння з оплатою праці тощо)

Прийнятий на роботу працівник протягом певного часу (від 1 до 6 місяців) має підлягати негласному контролю. Це потрібно для того, щоб за цей період він адаптувався в колективі, між ним та іншими працівниками сформувалися міжособистісні зв'язки. Тому потрібно спостерігати за тим, як він влаштувався на новому місці, як поводиться, як справляється зі своїми трудовими обов'язками, хто приходить до нього із сторонніх (родичі, знайомі). Незайве через 1-3 місяці викликати працівника на бесіду, поцікавитися, що він думає про своє місце роботи, чи все його влаштовує. Здійснення таких нехитрих заходів може допомогти вчасно виявити на підприємстві неблагонадійного працівника. Проте слід пам'ятати, що більшість нових працівників знають або здогадуються про те, що певний час вони перебуватимуть під контролем. Тому в цей період вони прагнутимуть показати себе з кращого боку.

Отже, відомості, здобуті в процесі попередньої перевірки і протягом випробувального терміну не можуть бути цілком достовірними і підлягають регулярній оперативній перевірці.

Контроль персоналу

Як уже зазначалося, після попередньої перевірки кандидата та прийняття його на роботу призначають випробувальний термін, протягом якого він перебуває під особливим спостереженням з метою виявлення в нього негативних якостей. Упродовж випробувального терміну нові працівники можуть отримувати мінімум інформації про підприємство, і, природно, їх небажано знайомити з конфіденційною інформацією. Вони можуть мати доступ тільки до інформації, необхідної для виконання їхніх функціональних обов'язків, а будь-які спроби з їхнього боку дізнатися більше мають припиняти керівництво або служба безпеки (до речі, якщо ці спроби вельми наполегливі і постійні, варто приділити цьому працівникові особливу увагу).

Після закінчення випробувального терміну (періоду посиленого контролю за працівником) оцінюють результати, за якими вирішують, який обсяг конфіденційної інформації може бути доступним для нього. За підсумками такого контролю можливі три найбільш поширені ситуації:

1. Випробувальний термін пройдено успішно. Працівник зарекомендував себе позитивно, продемонструвавши відмінні особисті й ділові якості. За час перевірок він не припускався істотних порушень дисципліни, дотримував усіх заходів захисту конфіденційної інформації. З таким працівником не повинно бути жодних проблем. Його можна допускати до роботи з конфіденційною комерційною інформацією будь-якого рівня секретності. Проте це не означає, що контроль збереження ним комерційної таємниці має бути повністю знятий. Можливо, з часом або під впливом обставин його хороші якості істотно зміняться не в кращий бік. Крім того, не можна повністю уникнути вірогідності того, що прийнятий працівник є "впровадженим агентом", який вдало пройшов першу перевірку. Тому оперативний (повсякденний) контроль, хоча і менш інтенсивний, потрібно продовжити. Та й періодичні перевірки не будуть зайвими.

2. Протягом випробувального терміну працівник зарекомендував себе як хороший фахівець, але в нього виявлено певні вади. Він схильний до умисного або необережного розголошування конфіденційної інформації. Отже, за своїми психологічними і моральними якостями він може стати джерелом просочування конфіденційної інформації. Причини цього різні (наївність, балакучість, зловживання спиртними напоями тощо). Крім того, ця людина під час випробувального терміну може припускатися порушень установленого режиму збереження конфіденційної інформації (порушення правил роботи із секретними документами, допуск на своє робоче місце сторонніх осіб). Отже, такий працівник потенційно небезпечний. Тому, залишаючи його на роботі, фірма робить це на свій страх і ризик. Якщо його професійні якості влаштовують її, то такий працівник має бути обмежений у допуску до конфіденційної інформації і перебувати під посиленим контролем.

3. Працівник зарекомендував себе негативно. Його професійній особисті якості виявилися низькими. Він припускає істотних порушень дисципліни і розголошування конфіденційної інформації, що дає підстави з високою

вірогідністю стверджувати, що надалі він може стати джерелом витоку комерційної таємниці підприємства. Не виключено, що цей працівник є впровадженим або завербованим конкурентами агентом. Від такої людини, звичайно, потрібно якомога швидше позбавитися, оскільки вона становить серйозну загрозу і може завдати непоправного збитку підприємству. Як позбавитися - вирішує фірма, але в правових межах. У виняткових випадках таку людину можна використовувати для дезінформації, даючи йому свідомо помилкові або непотрібні дані.

Зауважимо, що повністю керуватися тільки результатами попередньої перевірки і випробувального терміну недоцільно. По-перше, практично всі працівники знають, що спочатку вони перебуватимуть під особливим контролем. Тому протягом випробувального терміну прагнуть поводитися позитивно, дотримуючись усіх інструкцій. По-друге, в початковий період новий працівник адаптується до нових умов. Він ще не знає про стосунки, що склалися у фірмі, правила й порядки, відчуває себе невпевнено і прагне справити приємне враження. Надалі після "освоєння" на новому місці його поведінка може кардинально змінитися.

По-третє, попередня перевірка і випробувальні терміни можуть бути проведені неефективно, і людині з негативними якостями вдасться благополучно пройти контроль з добрим результатом.

По-четверте, як уже зазначалося, люди з часом можуть істотно змінитися, причому не завжди позитивно. Тому навіть бездоганний працівник з часом або під впливом обставин може перетворитися на "слабку ланку".

Отже, персонал постійно має перебувати під пильним спостереженням і регулярно проходити спеціальні перевірки. Такі перевірки можуть проводити фахівці (працівники служби безпеки) або принаймні менеджери з персоналу чи експерти, що працюють за контрактом. Перевірки можуть бути:

1) регулярними (проводяться за певним графіком, наприклад, першого числа кожного місяця, 15 числа кожного місяця);

2) оперативними (проводяться за ковзним графіком несподівано для тих, кого перевіряють, крім того, обов'язково проводяться в разі ЧП, розголошування інформації або виникнення підозр стосовно конкретних співробітників).

Бувають також перевірки:

а) гласна - дотримання інструкції, режиму зберігання, користування і знищення документації та джерел конфіденційної інформації, обліку вхідної/вихідної кореспонденції і т.ін.;

б) негласна - проводиться таємно від тих, кого перевіряють, працівниками СБ або спеціально залученими для цього особами. Такі перевірки дають змогу отримати необхідний результат, оскільки особа, яку перевіряють, не підозрює про те, що перебуває під контролем, і поводиться розкуто й природно.

Крім перевірок служба безпеки підприємства регулярно повинна здійснювати певні заходи щодо збирання інформації та перевірки персоналу. Це зокрема:

1. Спостереження. За кожним працівником фірми ведуть спостереження співробітники СБ. Вони регулярно збирають інформацію про нього, причому як у робочий час, так і під час відпочинку, на сумісних, святкових заходах та ін. Не варто обмежуватися тільки спостереженням за працівником усередині офісу. За потреби доцільно простежити, як він виконує свої обов'язки за межами фірми, чи не відхиляється від звичного маршруту, з ким зустрічається і т.ін. Незайвим буде також спостереження за ним у неробочий час, аби виявити його неблагонадійну поведінку та небажані контакти.

2. Агентурна робота - явне і негласне збирання інформації серед найближчого оточення, співробітників, друзів, товаришів, знайомих, родичів. Інформацію, отриману від тих, з ким безпосередньо спілкується той, кого перевіряють, можна вважати високо-достовірною і цінною. При цьому джерело інформації (агент) може працювати за власним бажанням (аморальних міркувань), з примусу (наприклад, за провину), за певну винагороду, "втемну", коли не підозрює про свою роль або спеціально впроваджений в оточення для збирання інформації. Але будь-яку отриману від агентури інформацію потрібно перевіряти ще раз, щоб уникнути дезінформації через помилку, невірогідність або зведення рахунків.

3. Провокації та спеціальні заходи, під час проведення яких здійснюється провокація тих, кого перевіряють, на розголошування конфіденційної інформації. Способи провокацій різні - шантаж, підкуп, алкоголь, секс, дружні бесіди тощо. Крім того, можуть бути використані "оперативні пастки" (наприклад, "випадкове" розголошування інформації з подальшим контролем). Бажано використовувати для провокацій сторонніх осіб, з якими персонал підприємства не знайомий. У разі залучення до провокації працівника СБ або іншого є висока вірогідність того, що той, кого перевіряють, здогадається про це і захід не дасть бажаного результату.

Отже, спеціально створена система контролю персоналу дасть змогу позбавитися неблагонадійних осіб вже на першому етапі, а в разі успішного проведення попередньої перевірки виявити і вчасно нейтралізувати загрозу безпеці підприємства.

Звільнення

Жодне підприємство не може уникнути ротації персоналу. Одні працівники приходять на підприємство, інших доводиться з різних причин звільняти. Когось неминуче доведеться звільняти як такого, що не відповідає посаді або виконуваній професії, хтось захоче звільнитися за власним бажанням через особисті обставини, а деякі працівники можуть піти через те, що підприємство не в змозі задовольнити їх потреби, що зросли.

У будь-якому разі звільнення працівника - неприємна ситуація, котра, якщо не поставитися до неї з повною серйозністю, може обернутися справжнім ЧП. Ось деякі негативні моменти, які може спричинити звільнення:

1. У зв'язку зі звільненням працівника тимчасово "оголяється" ділянка роботи, за яку він відповідав. Через це зазвичай доводиться задіювати інших

працівників, даючи їм додаткове навантаження, що призводить до зниження ефективності роботи підприємства.

2. Виникає високий ризик того, що звільнений працівник може розголосити конфіденційну інформацію, яка стала йому відома в процесі роботи. Якщо він перейде на роботу до конкурентів, це може завдати серйозного збитку підприємству.

3. Якщо керівництво не було заздалегідь готове до звільненні працівника, виникає термінова потреба в новому працівникові. На все потрібні додаткові витрати грошей і часу. Потрібно або звертатися в агентство з працевлаштування, або шукати працівника потрібної спеціальності самостійно. А на це не кожного керівника підприємства вистачить терпіння. Тому виникає високий ризик того, що кандидата на роботу відбиратимуть поспішно, без належної перевірки. Висока вірогідність того, що новий працівник буде недостатньо професійно підготовленим і за особистими якостями не відповідатиме вимогам. Цілком можливо також, що на місце, що звільнилося, терміново буде влаштований "по блату" хтось із родичів або приятелів співробітників підприємства. Може статися, що у такий спосіб на підприємство буде впроваджений агент конкурентів.

4. Новому співробітникові потрібен певний час на адаптацію в новому колективі. В цей час він особливо уразливий і ризикує через незнання припустити помилок, які можуть завдати шкоди підприємству.

5. Ротація кадрів, особливо якщо вона перетворюється на так звану "текучку" (часту зміну працівників), завдає величезної шкоди іміджу фірми.

6. Звільнення працівника - це завжди проблема юридична. Тому, коли під час звільнення не були дотримані всі передбачені чинним трудовим законодавством формальності і працівник був звільнений, хоча й обґрунтовано, але з порушенням процедури, можна з упевненістю сказати, що проблеми зі звільненим працівником тільки починаються. За такої ситуації працівник має повне право звернутися до суду з вимогою про відновлення на роботі та виплату заробітної плати за час вимушеного прогулу, а так про відшкодування морального збитку. А тепер порахуємо, у що це виллється. Процедура розгляду справи в суді в наших умовах може тривати від одного до шести місяців у кращому разі, з урахуванням проходження всіх судових інстанцій. У разі ухвалення рішення не на вашу користь вам загрожує:

- відшкодування середньої заробітної плати за час вимушеного прогулу;
- моральний збиток (установлюється за рішенням судової інстанції, і якщо працівник доведе, що унаслідок ваших незаконних дій він не зміг влаштуватися на іншу роботу і його діловій репутації завдано моральної шкоди, розмір морального збитку може бути значним);
- відшкодування судових витрат, зокрема на адвоката (з урахуванням складності справи і тривалості її розгляду в судових інстанціях від - $50 до 250).

Таким чином, підприємству буде завдано збитку відразу в кількох напрямах:

1) просочування конфіденційної інформації;

2) матеріальні втрати (судові витрати, оплата адвоката, можливі штрафи й виплати);

3) серйозний збиток іміджу підприємства, пов'язаний із привернення уваги до судового процесу;

4) втрата часу (а час, як відомо, - гроші) на судові розгляди. До речі, трохи відволікаючись від теми, зазначимо, що є численні приклади, коли керівництво підприємства, займаючись тільки судовими розглядами із звільненими працівниками, зазнавало колосальних збитків через неможливість займатися прямою комерційною діяльністю. Отже, до цього питання варто поставитися максимально серйозно.

Розглянемо, до яких дій для збереження комерційної таємниці мають вдатися відповідальні за безпеку особи:

Звільнення за власним бажанням:

1. З'ясувати причини звільнення. Це важливо, оскільки іноді може допомогти визначити, які недоліки в діяльності підприємства заважають його ефективнішій і продуктивнішій роботі. Зазвичай причини звільнення за власним бажанням зазначаються у заяві працівника. Проте далеко не завжди можна виразити реальні причини його в казенних зворотах. Тому, якщо причини звільнення видаються непереконливими або сумнівними, слід з'ясувати їх під час ненав'язливої бесіди з працівником, що звільняється.

2. З'ясувати майбутнє місце роботи. Це не завжди вдається визначити, оскільки працівники зазвичай не хочуть розкривати своє майбутнє місце роботи. І все ж слід дізнатися про це для того, щоб убезпечити себе від того, щоб звільнений працівник, влаштувавшись у конкурента, не розкрив інформації комерційного характеру, накопиченої ним за час роботи на підприємстві.

3. Виявити мотивацію працівника, його лояльність. При звільненні слід дізнатися, чи не озлоблений він на підприємство або на вас особисто, чи не затаїв на підприємство чи на когось із колишніх співробітників образу. Озлоблена, негативно настроєна людина, напевно, побажає помститися і може стати джерелом просочування комерційної інформації або розповсюдження недостовірної інформації про підприємство через негативне ставлення до неї.

4. Виявити обсяг відомої йому інформації (особливо конфіденційної). Це неважко встановити, якщо за працівником під час його роботи на підприємстві здійснювався оперативний контроль. Така інформація має міститися в особистій справі кожного працівника. Якщо під час роботи не було дотримано процедури, потрібно оперативно з'ясувати, з якими документами працював співробітник, з ким із партнерів, клієнтів спілкувався, під час вирішення яких питань був присутній. Якщо цього не зробити, результати дуже швидко дадуться взнаки.

5. Установити можливі ризики загрози розголошуванню інформації і вжити заходів щодо їх нейтралізації. Якщо існує потенційна небезпека розголошення інформації (а вона існує практично завжди), слід її нейтралізувати. Краще за все розробити план заходів на випадок розголошення

секретів підприємства. Крім того, бажано поміняти коли доступу, комп'ютерні паролі, ключі криптозахисту, які були відомі тому, хто звільняється.

6. Перевірити, щоб той, хто звільняється, здав усі джерела конфіденційної інформації, що були в нього. Це стосується насамперед документів, чернеток, креслень, дослідних зразків, комп'ютерних програм тощо. Потрібно також перевірити, чи не було у відділі чи підрозділі, де працював службовець, що звільняється, пропаж чи втрат документів з важливою комерційною інформацією, зразків готової продукції, ключів від кабінетів і сейфів та інших предметів, що мають конфіденційний характер. У разі виявлення цих фактів потрібно провести ретельне внутрішнє розслідування і визначити винних та частку джерел конфіденційної інформації.

7. Провести спеціальний інструктаж з працівником, що звільняється, про нерозголошення конфіденційної інформації, взяти підписку про нерозголошення. Цей інструктаж має проводити особа, відповідальна за збереження комерційної таємниці на підприємстві. Під час такого інструктаж)' працівникові нагадують положення про захист комерційної таємниці, роз'яснюють, що в разі недотримання цих положень підприємство може зазнати матеріального збитку. Після оголошення інструкції з працівника беруть письмове зобов'язання про нерозголошення і повідомляють йому, що в разі його порушення він нестиме юридичну відповідальність. Доцільно також зробити наголос на моральній стороні цього питання, звертаючись до порядності й чесності того, хто звільняється. Ще одним серйозним аргументом на користь збереження працівником конфіденційної інформації може бути факт, що той, хто видає секрети колишнього місця роботи, створює собі негативну репутацію. Адже зрозуміло, що, зрадивши один раз, він з легкістю вчинить так знову. Отже, на новому місці роботи така балакучість може викликати обґрунтовану підозру.

За можливості потрібно відстежити подальшу долю працівника, періодично спілкуватися з ним на дружній основі. Краще провести негласну його перевірку на предмет стійкості до розголошування конфіденційної інформації. У європейських фірмах широко застосовується такий спосіб, коли звільненого працівника просять у письмовій формі викласти всі його зауваження, претензії і пропозиції щодо роботи підприємства. Іноді за це навіть пропонують додаткову винагороду. Отримана таким чином інформація є особливо цінною, ті, хто звільняється, можуть чесно звернути увагу на аспекти, про які ті, що працюють, бояться або соромляться висловлюватися. Отримана таким чином інформація, якщо її правильно використовувати, може бути корисною для підприємства.

Головне - запобігти негативному настрою, озлобленості на фірму і бажання помститися. Вельми поширеною на більшості підприємств є ситуація, коли до того, хто звільняється, різко змінюється ставлення з боку керівництва і співробітників. Ще вчора він був незамінним працівником, якого всі любили й поважали, а сьогодні він ворог номер один, який своєю заявою "глибоко образив" усіх. Тому намагайтеся не створювати різних перешкод звільненню

працівника. Бюрократизм, причіпки та необґрунтовані претензії характеризують вас далеко не з кращого боку. І в жодному разі не можна затримувати виплату йому винагороди або під різними приводами зменшувати її суму, оскільки саме цей чинник може найбільше вплинути на його настрій. Деякі ваші дії (наприклад, затримання видачі трудової книжки) можуть порушувати чинне законодавство, а отже, коли працівник звернеться до суду, то підприємству буде завдано збитку, про який ішлося вище.

Не дозволяйте собі ображати особу, що звільняється, висловлюватися в грубій формі про її особисті й ділові якості, погрожувати їй надалі розправою або створенням проблем, давати необґрунтовані негативні рекомендації тощо. Зауважимо, що за своєю ініціативою звільняються здебільшого кращі працівники. Причому більшість їх ставиться до підприємства позитивно або принаймні нейтрально. А ви своєю поведінкою можете зробити з цієї людини ворога, озлобленого на фірму та її керівників. Через те ця людина, по-перше, почне поширювати негативну інформацію про фірму. По-друге, дружні взаємини з людиною, яка у вас працювала, можуть бути корисними. Та й ви за нагоди зможете підкреслити, що виховали хорошого фахівця.

Звільнення з ініціативи адміністрації. Набагато складнішою є ситуація, коли звільнення відбувається з вашої ініціативи. Адже в цьому разі спочатку закладається негативна ситуація з високою вірогідністю виникнення конфліктів, і тому природно, що говорити про подальшу лояльність людини, що звільняється, практично не доводиться. І все ж зупинімося докладніше на тому, які дії слід вчинити. Почнемо з того, що іноді навіть найгіршого працівника не так просто звільнити. У відповідних статтях Кодексу законів про працю вичерпно перелічені причини звільнення. І буде зовсім непросто довести, що ваші аргументи є достатньо вагомими для звільнення.

Ми не заглиблюватимемося і детально не розписуватимемо кожну підставу для звільнення працівника з ініціативи адміністрації. Кожна підстава має свої особливості. На підприємстві має бути юрисконсульт, завідувач відділу персоналу, які відповідальні за правильне звільнення працівників. Тому даємо лише загальні відомості про це.

У разі звільнення будь-якого працівника видають наказ (розпорядження) адміністрації, у якому зазначають підстави звільнення згідно із законодавством про працю і з посиланням на відповідний пункт і статтю закону.

При звільненні працівника йому зобов'язані видати під розписку трудову книжку із занесенням до неї запису про причину звільнення. Це роблять у день звільнення. Якщо працівник відмовляється з якихось причин отримувати трудову книжку і не приходить за нею на підприємство, слід надіслати йому повідомлення рекомендованим листом або телеграмою про те, що він повинен забрати трудову книжку. Посилати саму трудову книжку рекомендованим листом не слід, оскільки в разі її втрати з якихось причин відповідальність буде покладена на вас. Якщо працівник відмовляється розписатися за отримання трудової книжки, складають акт.

У разі звільнення працівника підприємство зобов'язане провести з ним

повний остаточний розрахунок - виплатити йому всі належні йому суми. Цю виплату він також отримує в день звільнення.

Отже, вам вдалося дотримати необхідної юридичної процедури звільнення, і настав час подумати про безпеку фірми. Що для цього потрібно зробити?

1. Виявити обсяг відомої йому інформації (особливо конфіденційної). Насамперед потрібно ретельно простежити за тим, щоб звільнений працівник здав усі справи і передав відповідальній особі документи та інші матеріали, що містять комерційну таємницю. Якщо ж той, хто звільняється, повідомляє, що не може передати ці документи, бо втратив чи передав їх іншій особі або випадково знищив, - це тривожний сигнал для служби безпеки. Проведіть ретельне розслідування і будьте готові до просочування інформації.

2. Безпосередньо перед звільненням з колишнім працівником має поговорити хтось із керівництва фірми і служби безпеки. Під час бесіди потрібно спробувати налаштувати того, хто звільняється, на нейтральне ставлення до фірми, а якщо не вдається цього зробити, порадьте йому утриматися від негативних дій стосовно підприємства. При цьому не треба погрожувати йому фізичною розправою чи іншими протизаконними діями. Головне - він має усвідомити, що коли він спробує помститися підприємству, його очікують серйозні неприємності. Тому обов'язково візьміть у нього підписку про нерозголошення комерційної таємниці.

3. Якщо той, хто звільняється, мав допуск до секретної інформації, то потрібно провести її ревізію. За можливості змініть коди доступу, паролі й ключі до сховищ комерційної таємниці. Бажано переглянути режим безпеки й секретності та внести до нього деякі зміни. Адже людина, що звільнилася, могла знати про заходи безпеки, тому є ризик, що ця інформація стане відомою конкурентам і недругам. Краще заздалегідь спланувати свої подальші дії в подібній ситуації.

4. Установити, чи можливі негативні дії (погрози, шантаж, диверсія тощо) стосовно підприємства чи його співробітників з боку колишнього працівника. Якщо особисті якості працівника дають підстави припустити реальну загрозу помсти з його боку, слід розробити і провести заходи щодо нейтралізації загрози і дати йому зрозумілі, що за подібні дії він буде покараний.

5. Бажано встановити, з ким із співробітників той, що звільняється, підтримував дружні стосунки. Ці працівники повинні пройти спеціальний інструктаж і перебувати під контролем, оскільки через них можливі просочування інформації або інші негативні дії проти фірми.

6. Провести бесіду з персоналом, під час якої пояснити йому причини звільнення колеги. Інакше серед персоналу через брак інформації можуть виникнути небажані домисли й версії. Він вважатиме, що адміністрація звільняє працівників без особливих причин або за незначну провину. Така ситуація формує негативну мотивацію і знижує лояльність працівників.

Якщо персонал отримає від керівництва достовірну інформацію, то подібної ситуації вдасться уникнути.

7. Обов'язково потрібно оповістити всіх співробітників фірми, а також партнерів, постійних клієнтів та інших осіб, з якими вона підтримує тісні стосунки, про те, що працівника звільнено. Якщо цього не зробити, звільнений працівник може дістати доступ до конфіденційної інформації і матеріальних цінностей від осіб, які через незнання продовжують вважати його працівником підприємства.

8. Потрібно відстежити подальшу долю звільненого працівника. Якщо він влаштується на роботу до конкурентів, слід провести заходи щодо запобігання можливому просочуванню конфіденційно? інформації. Не варто спеціально поширювати про працівника негативні дані, дискредитувати його, "поливаючи брудом" бо ви, робитимете собі антирекламу. Якщо звернуться до фірми з проханням дати характеристику на її колишнього працівника, вона повинна дати об'єктивну інформацію без прикрашань.

9. Найголовніше - потрібно бути готовими до того, що звільнений працівник створить підприємству додаткові проблеми, але не слід своєю поведінкою провокувати його на негативні вчинки стосовно фірми або помсту.

Навіть у разі звільнення працівника за якусь провину можна підтримувати з ним хороші стосунки, отримуючи від нього важливу інформацію або послуги.

Процеси

Встановіть систему обмежень на використання відкритих каналів зв'язку для передачі конфіденційної інформації. Такими каналами є переговори з реальними і потенційними партнерами, ділове листування, надання документації компаньйонам і контрольним органам, реклама, спілкування з представниками преси, державних органів, громадських організацій.

Потрібно охороняти від можливого підслуховування або сканування свої телефони, факси, комп'ютери, офіси, автомобілі, квартири. Використовуйте апаратуру зв'язку (ЗАС), що засекречує, генератори перешкод, прилади для виявлення "жучків" і с кану вальних пристроїв, застосовуйте умовні кодові позначення. Якою б технічно складною не здавалася "кругова оборона" проти електронної "зарази", за нинішніх умов якраз складності, зрештою, може і не вистачити.

Вироби

Потрібно організувати надійний облік усіх товарів, промислових і експериментальних зразків, відомості про які не повинні стати надбанням конкурентів. Охороняти перелічені вироби слід на всіх етапах їх "руху" усередині фірми (придбання, виготовлення, випробування чи перевірка якості, транспортування, зберігання, експлуатація, ремонт).

Основні методи захисту інформації технічними засобами

Загалом технічними засобами захист інформації забезпечують, коли:

- джерело і носій інформації локалізовані в межах об'єкта захисту і містять механічні перешкоди від контакту з ними зловмисника чи

дистанційного впливу на них полів його технічних засобів добування інформації;
- співвідношення енергії носія і перешкод на виході приймача каналу витоку таке, що зловмисникові не вдасться зняти з носія інформацію належної якості;
- зловмисник не може знайти джерело чи носій інформації;
- замість справжньої зловмисник приймає несправжню інформацію, котру він оцінює як справжню.

Ці варіанти реалізують такими методами захисту:
- запобігання безпосередньому проникненню зловмисника до джерел інформації за допомогою інженерних конструкцій і технічних засобів охорони;
- приховування достовірної інформації;
- "підсунення" зловмисникові неправдивої інформації. Застосування інженерних конструкцій і охорона - найбільш давній метод захисту людей і матеріальних цінностей. Способи захисту на основі інженерних конструкцій у поєднанні з технічними засобами охорони також поширені. Разом вони утворюють так званий фізичний захист. Але цей термін не можна вважати вдалим, оскільки інші методи захисту інформації за допомогою технічних засобів також ґрунтуються на законах фізики. З огляду на те, що основу розглянутого методу становлять інженерні конструкції і технічні засоби охорони, доцільно визначити його як інженерний захист і технічна охорона об'єктів (ІЗТОО).

Основним завданням ІЗТОО є запобігання безпосередньому контакту зловмисника чи сил природи з об'єктами захисту - люди і матеріальні цінності, носії інформації, локалізовані в просторі. До носіїв інформації належать папір, машинні носії, фото - й кіноплівка, продукція, матеріали, тобто все, що має розміри й вагу. Носії інформації у вигляді електромагнітних та акустичних полів, електричного струму не мають чітких меж, і для захисту інформації на них методи інженерного захисту неприйнятні (поле з інформацією, наприклад, не можна зберігати в сейфі). Для захисту інформації на таких носіях застосовують методи приховування інформації.

Приховування інформації передбачає такі зміни структури й енергії носіїв, за яких зловмисник не може безпосередньо чи за допомогою технічних засобів виділити інформацію з якістю, достатньою для використання її у власних інтересах.

Розрізняють інформаційне й енергетичне приховування. Інформаційного приховування досягають зміною чи створенням несправжнього інформаційного портрета семантичного повідомлення, фізичного об'єкта чи сигналу. Інформаційним портретом можна назвати сукупність елементів і зв'язків між ними, що відображують зміст повідомлення (мовного чи цифрового), ознаки об'єкта чи сигналу. Елементами дискретного семантичного повідомлення, наприклад, є літери, цифри чи інші знаки, а зв'язок між ними визначається їх

послідовністю. Інформаційними портретами об'єктів спостереження, сигналів і речовин є еталонні ознаки їх структури.

Можливі такі способи зміни інформаційного портрета:

- видалення частини елементів і зв'язків, що утворюють інформаційний вузол (найбільш інформативну частину) портрета;
- зміна частини елементів інформаційного портрета при збереженні незмінності зв'язків між елементами, що залишилися;
- усунення зміни зв'язків між елементами інформаційного портрета при збереженні їх кількості.

Зміну інформаційного портрета об'єкта зумовлює зміна зображення його зовнішнього вигляду (видових демаскувальних ознак), характеристик випромінюваних ним полів чи електричних сигналів (ознак сигналів), структури і властивостей речовин. Ці зміни спрямовані на зближення структур об'єкта і навколишнього його фону.

В умовах ринку, коли виробник змушений рекламувати свій товар, найбільш доцільним способом інформаційного приховування є вилучення з реклами чи відкритих публікацій найбільш інформаційних зведень чи ознак - інформаційних вузлів, що містять таємницю, яка охороняється. До інформаційних вузлів належать принципово нові технічні, технологічні рішення й інші досягнення, що становлять ноу-хау. Вилучення з технічної документації інформаційних вузлів не дасть змоги конкуренту скористатися інформацією, що міститься в рекламі чи публікаціях. Цей спосіб дає змогу:

- зменшити обсяг інформації, що захищається, і тим самим спростити проблему захисту даних;
- використовувати в рекламі нової продукції відомості про неї, не боячись розголошення.

Інший метод інформаційного приховування полягає в трансформації вихідного інформаційного портрета в новий, який відповіли несправжній інформації чи несправжній ознаковій структурі, і "нав'язуванні" нового портрета органу розвідки. Такий метод ще називається дезінформуванням.

Він є одним із найефективніших способів захисту інформації, оскільки:

- створює у власника інформації, яка має бути захищена, запас часу, зумовлений перевіркою з боку розвідки вірогідності отриманої інформації;
- наслідки прийнятих конкурентом на основі удаваної інформації рішень можуть бути для нього гіршими порівняно з рішеннями, прийнятими за відсутності інформації, яку добувають.

Розрізняють такі способи дезінформування:

- заміна реквізитів інформаційних портретів, які мають бути захищені, у випадку, коли інформаційний портрет об'єкта захисту схожий на інформаційні портрети інших "відкритих" об'єктів і не має специфічних інформативних ознак. При цьому обмежуються розробленням і підтримкою версії про інший об'єкт, видаючи за його ознаки дані об'єкта, який потрібно захищати. Наприклад, нині велика увага

приділяється продукції подвійного застосування: військового і цивільного. Поширення інформації про виробництво продукції цивільного використання є надійним прикриттям для продукції військового призначення;

- підтримка версії з ознаками, запозиченими з різних інформаційних портретів реальних об'єктів. Застосовують, коли організація одночасно виконує кілька закритих тем. Використовуючи різні ознаки, що стосуються певних тем, можна нав'язати протилежній стороні неправильне уявлення про роботи, що ведуться, без імітації додаткових ознак;
- поєднання справжніх і несправжніх ознак, причому останніми заміняють незначну, але найбільш цінну інформацію, що стосується об'єкта, який підлягає захисту;
- зміна тільки інформаційних вузлів зі збереженням незмінною іншої частини інформаційного портрета.

Використовують переважно різні комбінації цих варіантів.

Іншим ефективним методом є енергетичне приховування інформації. Воно полягає в застосуванні способів і засобів захисту інформації, що запобігають виконанню енергетичної умови розвідувального контакту або утруднюють його.

Енергетичного приховування досягають зменшенням потужності сигналів, тобто носіїв (електромагнітного або акустичного полів і електричного струму) інформації і створенням перешкод. Зменшити відношення сигнал/перешкода (слово "потужність", як правило, опускається) можна двома методами: зниженням потужності або збільшенням потужності перешкоди на вході приймача.

Для конкретних видів інформації і модуляції сигналу існують граничні значення відношення перешкода, нижче яких забезпечується енергетичне приховування інформації.

Необхідність і ефективність інженерного захисту і технічної охорони підтверджується статистикою, за якою понад 50% вторгнень відбувається на комерційні об'єкти з вільним доступом персоналу і клієнтів і тільки 5% - на об'єкти з посиленим режимом обороти її застосуванням спеціально навченого персоналу і складних технічних систем охорони.

Тема 12. ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОДНА ІЗ ОСНОВНИХ СКЛАДОВИХ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1. ІСТОРИЧНІ АСПЕКТИ СТВОРЕННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА. СУТЬ І ПОНЯТТЯ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЗАХИСТУ ІНФОРМАЦІЇ.

Для сучасного етапу розвитку світової цивілізації характерний перехід від індустріального суспільства до інформаційного, формування якого пов'язують з інформаційною революцією, розвитком інформаційних технологій, що радикально змінюють суспільне життя. Цей перехід відбувається нерівномірно, що зумовлено як національною специфікою, так і станом розвитку світового співтовариства.

Поняття "інформаційне суспільство" нині використовують для визначення суспільства, в якому економіка, політика й культура залежать від створення, збереження та доступності інформації в національному і світовому масштабах. Є різноманітні підходи до становлення й розвитку інформаційного суспільства, навіть у розвинених країнах світу. Теоретичне обґрунтування розвитку інформаційного устрою значно відстає від практичних потреб, що зростають досить швидкими темпами.

Нині поняття "інформаційне суспільство" для України практично є популярним терміном європейських декларацій, ніж реальним явищем з чітким змістом. Однак зауважимо, що "інформаційний істеблішмент" зарубіжних країн - авторів поняття "інформаційне суспільство" донині не дійшов згоди стосовно форми й наповнення такого суспільства.

Як запевняють науковці, інформаційне суспільство в нашій країні буде створене не раніш як через чверть століття. Незважаючи на те, що насправді електронний простір, цифрова цивілізація людства ще "сплять", навколишній світ набуває дедалі більше ознак інформаційного суспільства. Тому про переваги й можливості інформаційної цивілізації ми можемо лише мріяти та прогнозувати, що вона буде чудовою, й чекати перетворення мрій на реальність.

Людство очікує, поки "прокинеться" потенціал, який накопичують комп'ютерні мережі світу від часу своєї появи. Ми можемо лише здогадуватись і прогнозувати, що чекає на інформаційне суспільство, так само, як і чого нам очікувати від нього. Теоретики соціології, політології, економіки, культури напророкували щодо його майбутнього чимало. Одні обіцяють радісну й безхмарну феєрію, інші малюють картину геть інфернальну, повертаючи терміни періоду рабовласництва. Отже, час дати відповіді на сьогоднішні запитання.

Вперше в достатньо чіткому вигляді ідея інформаційного суспільства

була сформульована наприкінці 60-х - початку 70-х років XX ст. Винахід самого терміна "інформаційне суспільство" приписується Ю.Хаяші, професорові Токійського технологічного інституту. Японський уряд уже тоді вважав дуже важливим для країни, зокрема для її економіки, з'ясування перспективи поширення комп'ютерних технологій. Тож доповіді з цієї проблеми готували одразу кілька груп дослідників. Проте наголос на економічних наслідках зумовив певну обмеженість і прикладний характер продукту роботи японських учених.

"Інформаційне суспільство" так і залишилося б просто японською локальною моделлю розвитку, якби паралельно в таборі її економічних суперників - американців не з'явилася ще одна концепція нового суспільства. Це був постіндустріалізм соціолога Деніела Белла.

Цей термін він запропонував ще 1962 р. А в 1974 р. з'явилася його основна праця - "Прихід постіндустріального суспільства". За Бел-лом, нове, постіндустріальне суспільство ґрунтується на теоретичному знанні, яке є його визначальним принципом, джерелом інновації та формування політики. В економіці це призводить до поступового занепаду виробництва товарів як основної форми економічної діяльності й заміни його виробництвом послуг. З'являється новий, домінуючий клас - клас професіоналів. У всіх сферах - економічній, політичній і соціальній - основний вплив на прийняття рішень чинять нові інтелектуальні технології і новий інтелектуальний клас.

І в 70-ті роки XX ст. відбувається конвергенція цих двох ідеологій, що виникли майже одночасно. Продукт схрещення ідей Хаяші та Белла залишив за собою назву та прикладну частину від винаходу японської команди технологів та економістів. Але решту - власне ідеологію, соціальний, психологічний, культурний аспекти, все те, що і становило основу майбутньої цивілізації третьої хвилі, - він взяв від соціологічного підходу Белла. Ідеологія постіндустріалізму мала досить солідну теоретичну основу й універсалістську орієнтацію для виконання функції фундаментальної соціальної концепції.

Інформаційне суспільство - соціологічна концепція, що визначає головним фактором розвитку суспільства виробництво й використання науково-технічної та іншої інформації. Концепція інформаційного суспільства є різновидом теорії постіндустріального суспільства, засновниками якої були З. Бжезінський, О. Белл, О. Тоффлер.

Розглянемо насамперед, що, на думку теоретиків і практиків, являє собою новий етап розвитку цивілізації, який, до речі, так і не має остаточної назви: Lifelong Learning Society (суспільство дожиттєвого навчання); Digital Society (цифрове суспільство); Net-Intellect Society (суспільство мережевого інтелекту); Global Society (глобальне суспільство); Information Society (інформаційне суспільство); Silicon Society (кремнієве /піскове суспільство).

Після виголошеної Мартіном Бангеманном у 1994 р. доповіді почали вживати термін "інформаційне суспільство".

Для довідки: Група на чолі з доктором права, віце-президентом Єврокомісії М.Бамгеманном сформована на вимогу Єврокомісії 1993 р. з метою

дослідження розповсюдження інформаційних технологій та з'ясування проблем, що виникають у цьому процесі.

Ця доповідь і поклала початок європейському інформаційному суспільству, дала основні його визначення, характеристики й ознаки в Європі. Назва "інформаційне суспільство" походить від назви основного ресурсу - інформації. Але так само правильним є й інші визначення, оскільки ґрунтуються на основних ознаках нової суспільної формації.

Це суспільство насправді є: цифровим і глобальним, бо воно характеризується дожиттєвим навчанням; мережевим, бо побудоване за мережевим інтелектом; піщаним і кремнієвим, адже пов'язане з "піщаною" технологією чіпів.

Для довідки: За гіпотезою американських фахівців з інформаційних технологій, основою мікропроцесорного виробництва с кремній (той же пісок на пляжі).

Відомим є визначення, яке називають Гейтсовою "цифровою нервовою системою". Білл Гейтс визначає її як суму персональних комп'ютерів, засобів електронної пошти та підключення до мережі Інтернет. Вимога така, що основні складові частини мають бути стандартними і спільними для урядових структур, громадян і комерційних підприємств, аби уможливити глобальну інтеграцію локальних місцевих або національних мереж. Тому "цифрова нервова система" може виступати одним зі складників інформаційного суспільства. Як бачимо, одностайної думки щодо назви немає.

Насправді як науковців, так і пересічних громадян цікавить, що ж нас чекає у невизначеному загадковому, так званому інформаційному суспільстві? Для цього ми маємо першочергово з'ясувати, де ми перебуваємо сьогодні і що діється навколо нас.

Республіканець Ньют Джингріч, голова Палати представників США в 1995р., запозичує межові знаки з попередньої цивілізаційної зміни: те, що відбувається з нами тепер, можна усвідомити, порівнявши з періодом між 1770 і 1800 рр., коли Сполучені Штати перетворилися з аграрної країни на індустріальну. Те, що ми переживаємо, відхід від індустріальної епохи, змушує ставити дуже схожі і сповнені глибокого змісту запитання до себе.

Постіндустріальне суспільство відрізняється від індустріального тим, що нині основним виробничим ресурсом стала інформація, тоді як у доіндустріальному та індустріальному була сировина та енергія: змінився сам характер виробничої діяльності - тепер є обробка та опрацювання, а було виробництво і видобування; тепер ми маємо наукомісткі технології на противагу колишнім трудомістким технологіям і капіталовкладенням.

Ситуація в Україні аналогічна американській, адже наша держава також пережила навальну індустріалізацію на початку ХХ ст. Проте тоді ми не встигли осмислити себе в новому середовищі, адже зміни нав'язувалися ззовні і планувалися чужими теоретиками.

Недаремно говорять, що "найлегший шлях передбачити майбутнє - винайти його". На основі цього вислову можемо вважати себе "винахідниками

українського майбутнього". Звичайно, хочеться, щоб місце нашої держави в майбутньому було чітко визначеним. Навіть якщо електронна планета насправді за виглядом і на дотик матиме розмір головки сірника, але й там Україні непогано було б мати вигідне місце, облаштоване саме за її "формами". Тому, що нам таки доведеться тривалий час жити в цьому цифровому світі. Адже термін життя цивілізацій вимірюється століттями.

А ми схильні погодитись із цим визначенням (стосовно нової цивілізації) футуристів та авторів найбільш знаних у світі теорій про інформаційне суспільство Елвіном та Хайді Тоффлерами. Так, термін "цивілізація" може звучати претензійно, проте жоден інший термін не може бути достатньо всеохопним, аби охоплювати такі поняття, як технологія, родина, релігія, культура, політика, бізнес, ієрархія, лідерство, системи цінностей, мораль і теорія пізнання.

За подальшої інформатизації у світі зсуви й радикальні зміни відбудуться на всіх цих рівнях суспільства. А коли змінюється стільки соціальних, технологічних і культурних параметрів одночасно, тоді виникають не лише зсуви, а й якісні зміни - не лише нове суспільство, а й зачатки абсолютно нової цивілізації. "Комп'ютерна революція" поступово призводить до зміни традиційного друку "електронними книгами", змінює ідеологію, перетворює безробіття на забезпечене дозвілля.

Соціальні й політичні зміни розглядаються в теорії інформаційного суспільства як наслідок "мікроелектронної революції". Перспектива розвитку демократії пов'язується з розповсюдженням інформаційної техніки. Тоффлер та Дж.Мартін відводять головну роль у цьому телекомунікаційній "кабельній мережі", яка забезпечує двосторонній зв'язок громадян з урядом, дасть змогу враховувати їх думку під час розроблення політичних рішень. Розробки в галузі "штучного інтелекту" розглядаються як можливість інформаційного трактування самої людини. Концепція інформаційного суспільства викликає критику з боку гуманістично орієнтованих філософів та науковців, які дотримуються думки щодо негативних наслідків комп'ютеризації суспільства.

Почнемо з технології як найбільш модифікованої сфери. Будь-яке виробництво із запровадженням інформатизації набуває тенденції до мініатюризації (і далі - мікро- й наномініатюризації). Речі навколо нас стають розумними - від виробничої лінії до холодильника, від собачого нашийника до розетки. Буквально за кілька років наш офіс, помешкання, транспорт замайорять повідомленнями: "Скінчилось молоко", "Накопичилось надто багато пошти", "Автобус буде біля вас за три хвилини сорок секунд", "Собака хоче води" і т.ін. Фахівці з інформаційних технологій подумали вже й про це. Заздалегідь ведуться розробки "усамостійненої" інтерактивної техніки. Механізм, влаштований у пральну машину, сам дистанційно замовить у торговельній комп'ютерній мережі пральний порошок, коли він скінчиться. Аналогічно електроніка холодильника підрахує бюджет родини на харчування, швидкість витрачання кожного продукту, склад місячного кошика споживання, знайде найдешевшу пропозицію за кожним пунктом і зробить попереднє

замовлення. Автоматика на нашийнику домашнього улюбленця ввімкне й вимкне воду для собаки чи кішки, відчинить і зачинить двері, виведе їх на прогулянку за контрольованим маршрутом, викличе ветеринара й замовить засіб від бліх.

Тоффлер не дає новій цивілізації визначення, але доводить що вона має принципово новий характер. Багато чого в цій виникаючій цивілізації суперечить традиційній індустріальній. Це водночас і технічно розвинена, і антиіндустріальна цивілізація. "Третя хвиля" несе із собою новий спосіб життя, що ґрунтується на джерелах енергії,які поповнюються; на методах виробництва, що роблять застарілими більшість фабричних збірних ліній; на якійсь новій родині; на новому інституті, який можна було б назвати "електронним котеджем"; на радикально перетворених школах та корпораціях майбутнього. Така цивілізація несе з собою новий кодекс поведінки та виводить нас за межі концентрації енергії, грошових коштів і влади.

Тож, як бачимо, ніщо не може бути випущене з поля зору в процесі запровадження інформаційних технологій у наше життя. Кожен аспект нашої життєдіяльності неминуче має набути цифрових характеристик, оскільки технології, "розірвані", розкидані в окремих речах, що нас оточують, марні. Як дорога іграшка, надто крихка для того, щоб її бодай торкатися.

Коли ж виникає інформаційна мережа, навіть локальна, користь від інформатизації зростає експоненціально, з кожним кроком ефективність збільшується майже на порядок. Сенс інформаційних технологій саме в їх синергізмі, ефекті об'єднаних можливостей і потенціалів.

Інформатизація характеризується системністю. Все потроху залучається до діалогу людина-довкілля, все набуває активного інтерфейсу, дружнього до користувача. Ще понад століття тому - в 1851 р. Натаніел Готорн, американський фантаст і натхненник розвитку телеграфу, зауважив, що електрика перетворила матеріальний світ на величезну нервову систему. Земна куля стала величезним мозком із чуттям і розумом.

Як уже зазначалося, можливості комп'ютерів, об'єднаних в мережу, - це не просто сума можливостей кожного з елементів. Відбувається астрономічне зростання. Вже тепер на симулювання такої складної хаотичної системи як, скажімо, вірус СНІД чи екологічний баланс, не потрібно багато часу. Плюс забезпечується доступ до роботи над цим практично необмеженої кількості фахівців.

Отже, завдяки новим можливостям обсяг і структура знань змінюються і кількісно, і якісно. Тож набута освіта вже не забезпечує сталого професійного рівня, достатнього на все життя. А постійне навчання паралельно з роботою вимагає зміни принципу освіти, для нового покоління - розроблення нової педагогіки: системи виховання особистості, адаптованої до інформаційного суспільства.

Розвиток телекомунікаційної інфраструктури - створення сучасної технологічної бази національної інформаційної інфраструктури й інноваційної інформаційної галузі, що забезпечуватиме швидке поширення ефективної й

конкурентоспроможної інформації і надаватиме широкі комунікаційні можливості для всіх прошарків населення. Ми повинні забезпечити себе належною інфраструктурою доступу до інформації і знань для того, щоб повною мірою використовувати переваги інформаційного суспільства.

Роль мас-медіа - формування в суспільній свідомості готовності перейти до інформаційного суспільства, вдосконалення системи демократії та плюралізму ідей. Потрібно сформувати в широких колах населення усвідомлення необхідності й бажаності змін, пов'язаних із переходом України до інформаційної стадії розвитку, а також психологічну готовність до участі в цих змінах.

Гармонізація інформаційного законодавства України з нормами ЄС. Метою адаптації законодавства України до законодавства Європейського Союзу є досягнення відповідності правової системи України сучасній європейській системі права. Це сприятиме політичній, підприємницькій, соціальній і культурній активності громадян України, а також створить необхідні передумови для отримання Україною статусу асоційованого члена ЄС.

Розвиток експортоорієнтованих 1КТ виробництв - створення необхідних умов для розвитку національного експортноорієнтованого ІТ-аутсорсінгу, що є чинним механізмом здобування українськими технологічними компаніями міжнародного ринкового досвіду.

Крім технології, науки, освіти й виховання, глобалізація інформаційних мереж змінює також фізичний спосіб роботи і навчання, додаючи до них префікс теле-, себто дистанційний. Отже, пошук роботи чи вступ до навчального закладу більше не означає зміни місця проживання. Більше немає потреби через це розривати родинні зв'язки. До того ж, телеробота дає змогу більше часу приділяти дітям, а отже, повертає традиції родинного виховання.

І духовне життя людини з поширенням інформатизації набуває нових рис завдяки новим можливостям. Виховується релігійна терпимість, оскільки різко збільшується доступність інших переконань, доступність вільного спілкування з їх носіями. Відвідування святинь у режимі он-лайн, персональна електронна капличка, електронний молитовник на молитов за секунду - людська вигадливість безмежна, особливо коли на ній можна заробити.

Анонімність, деперсоніфікація, ба навіть симуляція особи в Мережі (стать, вік, освіта, національність - будь-що може бути приховане чи змінене лише натисканням кількох клавіш). І, відповідно, система цінностей суспільства має зазнати певних трансформацій.

Ми не можемо сьогодні сказати, куди саме спрямують людство сили соціальної та психологічної адаптації. Проте ми точно знаємо, що шлях буде пройдено чималий. Одним із прикладів є переміщення до віртуальної реальності світових культури й мистецтва. Причому тут відбувається подвійний процес одночасно і виникають специфічні мережеві види культурної і мистецької діяльності, що можливі лише в гіперпросторі і створюються версії (себто в Мережі чи на дисках або інших носіях інформації відповідно) реальних

музичних творів, виставок, музеїв, бібліотек, пам'ятників тощо.

Перенесення в інформаційний простір культурних надбань практично всіх націй і часів робить їх доступнішими. Адже тепер не треба вишукувати вільних грошей і часу, аби відвідати Версаль чи Ермітаж. Не треба жодних дозволів і статусів для вивчення раритетів літератури чи мистецтва. Можна "власноруч" повторити роботу археолога чи реставратора, відомого художника чи ювелірного майстра.

Мистецтво стає справді близьким народові - двері в цілий світ втілює дедалі компактніше створіння (хіба це річ, якщо має дедалі більше розуму й несе дедалі більшу відповідальність і за нашу роботу, і за дозвілля, і за освіту!), яке мешкає на нашому робочому столі.

Комп'ютер уможливив активну взаємодію культурних просторів різних користувачів, об'єднавши їх у єдине культурне буття планети. Культурний простір стає глобальним.

Причини виникнення інформаційного суспільства зрозумілі, а от електронна готовність та електронне залучення ще недостатнє. Готовність - це первинна, фундаментальна основа успіху будь-якої діяльності. Електронне залучення - це інструмент, завдяки якому підвищується рівень електронної готовності.

Готовність до того чи іншого виду діяльності - це цілеспрямований вияв особистості, що охоплює її переконання, погляди, мотиви, почуття, вольові та інтелектуальні якості, знання, настановлення. Її досягають у процесі моральної, психологічної, професійної та фізичної підготовки, вона є результатом всебічного розвитку особистості з урахуванням вимог щодо особливостей діяльності, професії. Відтак готовність до діяльності є складним соціально-психологічним явищем.

Схема готовності людини до діяльності в умовах інформаційного суспільства передбачає три основних компоненти і складена авторами на підставі матеріалів А. О. Мойсеєнко (рис. 12.1).

Характерною властивістю інформаційного суспільства є безстроковість, тобто право на особисте інформаційне безсмертя. Якщо раніше протягом століть панувала книга - вона була безсмертям її авторів, то в мережі кожен користувач - сам автор свого безсмертя і залежно від його вкладу, вміння сформувати електронну версію своєї творчості, подати науковий матеріал - кожна людина може створити й закодувати архіви, документи, що їй належать, і потенційно необмежений час їх зберігати.

Цими матеріалами навіть після фізичної смерті можуть користуватися люди, тобто буде необмежений час тривати обмін інформацією між її "електронною версією" та цілим світом інших користувачів.

Для довідки: Електронною версією певної інформації можуть бути: архіви, наукові статті, публіцистичні матеріали ЗМІ, інтерв'ю, звернення, фото, відео, окремі сайти та блоги тощо.

Безсмертні віртуальні особистості, чиє життя триває в гіперпросторі, наповнені цифровими аналогами речей і явищ матеріального світу.

Рис. 12.1. Компоненти готовності людини

Базові показники інформаційного суспільства диктуватимуть і нову політичну реальність. Основним онлайновим блоком у цій сфері, що здійснюється за допомогою Мережі, є право кожного отримувати інформацію про діяльність влади в реальному часі. Більше того, навчені гірким досвідом історії політичних маніпуляцій і практики їх приховування, деякі автори наполягають на потребі безстрокового зберігання документів та інформації про цю діяльність.

Робити точний прогноз інформаційного суспільства, створювати його віртуальну модель нині складно. Можемо лише надати певну кількість можливих варіантів подій. Оця невизначеність і є однією з багатьох характерних рис нашого життя: останнього покоління старої і першого - нової цивілізації.

Важливим для аналізу проблеми електронної готовності є новий напрям, що називається інформаційною психологією, яка досліджує компоненти, притаманні поняттю електронної готовності (рис. 12.2).

Відомі критерії електронної готовності людини до інформаційного суспільства, за якими можна виокремити та проаналізувати п'ять категорій (рис. 12. 3).

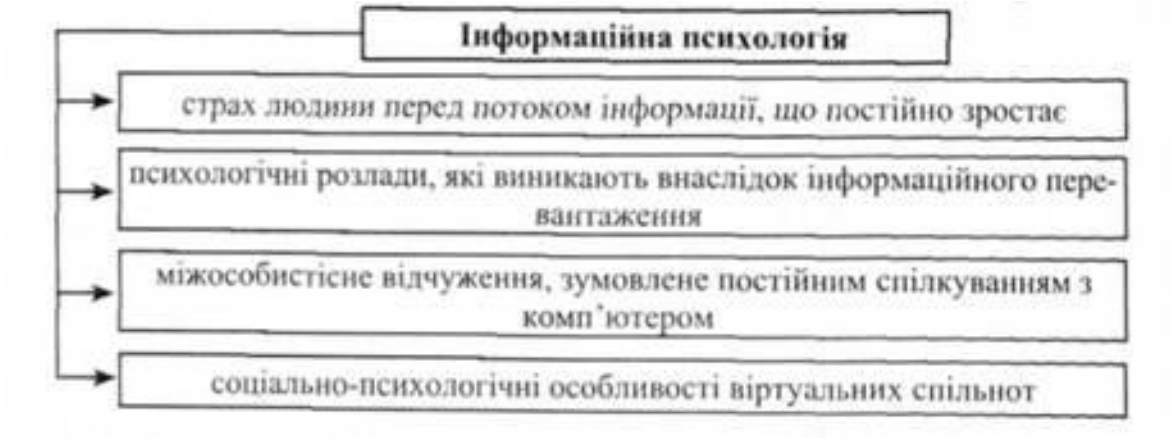


Рис. 12.2. Компоненти, які вивчає інформаційна психологія

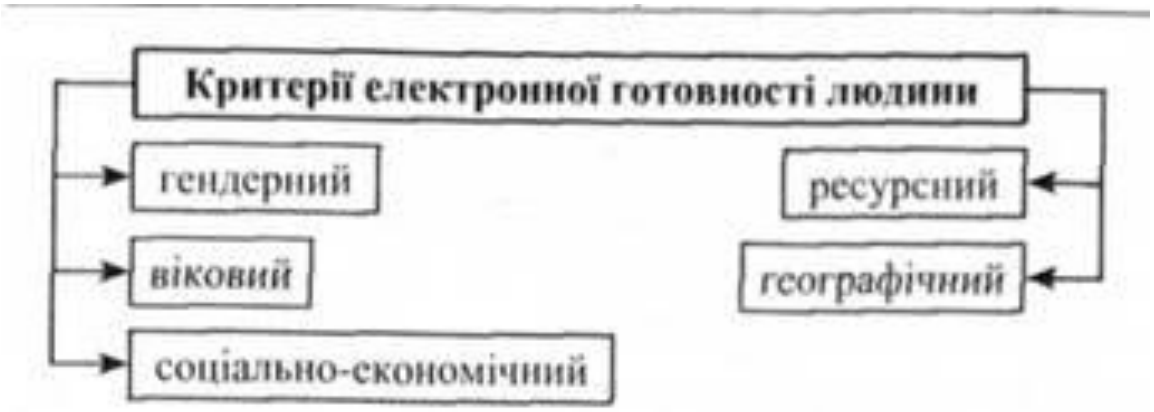


Рис. 12.3. Критерії електронної готовності людини

Категорії готовності населення до інформаційного суспільства:

1. Готовність жінок та чоловіків - тендерний критерій:

- чим вищий розвиток інформаційно-комунікативних технологій (ІКТ) у певній країні, тим менша різниця між кількістю користувачів сучасних ІКТ:
- співвідношення чоловіків і жінок 60 % на 40 % відповідно є нормальним для високотехнологічних країн світу - США, Фінляндії, Канади, Ірландії;
- в окремих випадках (залежно від географічного фактора) цей показник може становити і 70 % на 30 %.

2. Готовність молоді і старшого покоління - віковий критерій:

- у країнах з високим розвитком інформаційної інфраструктури загалом вищий відсоток Інтернет-користувачів, віковий ценз яких коливається в діапазоні від 50 до 60 років. Все ж основна проблема переходу до практичного використання сучасних ІКТ для цих людей полягає в низці причин, серед яких:
- зміна ментальності, зокрема, сприйняття речей та процесів реального світу;
- злам соціально-культурних стереотипів, якими керується більшість

представників їхнього покоління;

- використання шаблонів стосовно того, що нові інформаційні процеси - це винятково прерогатива молоді або ж того, що ПСТ є потенційно шкідливими для здоров'я;
- острах, що опанувати комп'ютерну грамотність виявиться не до снаги.

Не менше проблем існує і в представників покоління віком 20 - 50 років (можна сказати, тієї прогресивної частини людства, яка по-різному, але використовує альтернативи інформаційного суспільства).

У цьому контексті нагадаємо, що нині лише 10 % людства користується Інтернет.

Отож, проблеми, що стосується молодих "громадян інформаційного суспільства", полягають ось у чому:

- використання ІКТ здебільшого як індустрії розваг, а не освітнього чи ділового ресурсу;
- недоступність інформаційно-комунікаційних послуг через їх високу вартість у багатьох країнах;
- незнання (переважно через небажання дізнатися про сучасні інформаційні можливості:
  -голосування електронним шляхом;
  -заповнення офіційних документів та їх реєстрація в режимі он-лайн;
  -купівля і продаж товарів чи надання послуг через Інтернет;
  -отримання освіти, консультацій, діагностики лікування, юридичних послуг в електронному форматі тощо внаслідок особистих упереджень та стереотипів.

3. Готовність людей розумової та фізичної праці - ресурсний критерій: у цьому контексті все залежить від середовища, в якому відбувається повсякденна діяльність людини. Якщо особа використовує знаряддя й ресурси, властиві індустріальному чи аграрному суспільству, а вони не є інформатизованими, то, відповідно, не виникає й підстав говорити, що така людина належить до інформаційного суспільства. А якщо праця, освіта чи інша діяльність людини пов'язана з ментальними чи творчими процесами, то в більшості випадків така особа "автоматично" починає використовувати вигоди ІКТ.

На простішому рівні - це налагодження комунікацій через такі медіазасоби, як електронна пошта, он-лайн зв'язок, використання Інтернету для пошуку інформації та її опрацювання, участь у віртуальних конференціях і форумах.

На досконалішому рівні - це телеробота, дистанційне навчання, участь у мережевих дослідницьких проектах.

4. Готовність жителів великих і малих міст, а також сільської місцевості - географічний критерій:

- географічне розмежування є одним із критичних факторів, що впливають на показник електронної готовності в тому чи іншому регіоні світу. Технічно не завжди легко, вигідно чи дешево інформатизувати сільський

регіон. Отож, жителі таких регіонів потенційно обмежені у використанні сучасних ІКТ. Хоч у цивілізованих країнах це питання вирішується завдяки реалізації цільових фангових програм - "успішних прикладів втілення інформаційно-комунікаційних проектів" (англ. success stories). Географічно найбільшими регіонами розвитку інформаційного суспільства є великі міста, мегаполіси та столиці, бо сфера надання послуг і множина інформаційних потоків сконцентровані в них.

5. Готовність забезпечених громадян та людей із низьким рівнем доходів - соціально-економічний критерій:

- у цьому випадку традиційно побутує думка, що основна перешкода використання пересічними громадянами ІКТ полягає в неможливості придбати персональний комп'ютер, підключитися до Інтернету тощо. Однак справжня причина полягає в самому мисленні та свідомості громадян, більшість із яких живе ще за канонами індустріального чи навіть аграрного ладу, відкладає якісь кошти для купівлі засобів, що зазвичай використовуються за цих устроїв.

Електронне залучення громадян пов'язане з першими кроками інформаційної країни. Основні характеристики інформаційного суспільства показують, якими будуть результати використання електронного залучення як сучасного трансформаційного інструменту.

Наше суспільство не першим переживає такий переломний момент. Зокрема, тоффлерівська теорія третьої хвилі стверджує, що ця ситуація повторюється вже двічі: коли прийшла аграрна цивілізація першої хвилі, та індустріальна - другої.

Як стверджують науковці, тоді було легше, бо цивілізаційні хвилі чемно додержувались черги і рухалися від суспільства до суспільства поодинці. А коли в нинішній соціальній формації переважає окрема хвиля змін, модель майбутнього розвитку порівняно легко розпізнати. Зокрема, це далося взнаки за попередньої, другої, хвилі, коли індустріальне бачення майбутнього мало значний психологічний ефект. Загальне уявлення про індустріальне майбутнє визначало вибір, допомагало людям зрозуміти не лише те, ким вони є і ким були, а й те, ким вони вірогідно стануть. Це забезпечувало стабільність і відчуття самосвідомості навіть за екстремальних соціальних змін.

Сучасні ж суспільства зазнають ударів одночасно двох чи всіх трьох хвиль змін, без явних переваг тієї чи іншої. Тому образ майбутнього інформаційного суспільства змінюється, не є окресленим, і дуже важко визначити зміст перемін та конфліктів.

Все ж ми можемо цілком точно визначити одну дуже важливу ознаку того способу життя, який нас швидко "поглинає": нове суспільство - це суспільство розумової праці, що ґрунтується на застосуванні людських знань до всього, що виробляється, й до того, як це робиться. Нові ідеї будуть головним джерелом добробуту. Так, бюджети країн та корпорацій і сьогодні орієнтуються на:

- сировину;
- обсяги рухомої та нерухомої власності;
- запаси готової продукції;

- інші матеріальні вияви добробуту і гарантій на майбутнє. Проте новий принцип, орієнтація на нематеріальний - творчий, інтелектуальний - потенціал вже працюють у сучасному світі. Адже навіть коли кілька цивілізаційних хвиль співдіють, все ж можна виокремити сферу, що належить до кожної з них. Таким чином, вже певний час у суспільствах функціонує більш-менш потужний сектор третьої хвилі. І він вже використовує "новий спосіб домінування - створення й експлуатацію знань".

На думку Д. Белла, в наступному столітті вирішальне значення для економічного та соціального життя, для способів виробництва знання, а також для характеру трудової діяльності людини матиме становище нового соціального укладу, що ґрунтується на телекомунікаціях. Революція в організації та обробці інформації і знань, в якій головну роль відіграє комп'ютер, розгортається водночас із розвитком індустріального суспільства. Три аспекти останнього особливо необхідні для розуміння телекомунікаційної революції:

1) перехід від індустріального до сервісного суспільства;

2) вирішальне значення кодифікованого теоретичного знання для здійснення технологічних інновацій;

3) перетворення нової "інтелектуальної технології"" на ключовий засіб системного аналізу і теорії приймання рішень.

Актори цивілізації третьої хвилі є творцями нових принципів у сфері інформації і нововведень, менеджменту, культури і поп-культури, нових технологій, програмного забезпечення, освіти, педагогіки, медицини, фінансових систем, військового захисту й інших послуг, які вони поширюють на весь світ. Поширений акцент на послуги випливає власне з визначення інформаційного суспільства, яке виокремилося далеко не одразу.

Тож, повертаючись до питання акценту та послуг, Белл за основну рису постіндустріального суспільства (що перейшла до теорії інформаційного суспільства) визначає перехід від виробництва речей до виробництва послуг, причому послуг, пов'язаних передусім з охороною здоров'я, освітою, дослідженнями та управлінням.

Ця особливість постіндустріального суспільства тісно пов'язана зі змінами в розподілі занять: спостерігається зростання чисельності інтелігенції, професіоналів і "технічного класу".

І в 60-70-ті роки XX ст. це вже не було голою теоретичною викладкою. Адже кількість службовців вперше перевищила кількість робітників ще 1955 р.

І це не єдина характеристика, що зазнала змін від початку наступу інформаційних технологій на всьому фронті усталеного способу життя.

Елвін і Хайді Тоффлери цілком правильно відзначили, що вся структура суспільства змінюється, коли однорідність суспільства другої хвилі замінюється різнорідністю цивілізації третьої. Цивілізація, що настає, готує для нас новий кодекс поведінки й виводить від стандартизації, синхронізації й централізації, від концентрації енергії, грошей і сил.

Фактично ми стаємо свідками поворотного моменту спіралі історії. Це відбувається в нас на очах: глобальна інформатизація уможливлює інтенсифікацію й розширення масштабів прямих рівноправних взаємодій між людьми. Це явище далеко не нове. Людство вже знайоме з ним із попередніх часів. Однак раніше такі взаємодії могли відбуватися тільки в малих групах людей, у родинних чи сусідських спільнотах. Тепер така спільнота стала завбільшки з планету. Виходить, людство з відокремлених, індивідуалізованих, розмежованих мегаполісів знов повертається до способу співжиття, коли кожен об'єднаний з іншим. А всі наші передбачення майбутнього, переміщення до нового соціального простору, тепер уже інформаційного, насправді є ретрофутуризмом. Себто ми будуємо старе нове суспільство. Стосовно України ми лише накопичуємо сили й засоби для цього будівництва. А створення справжнього "дієвого поліморфного інтерактивного середовища" й прокладання потужної інформаційної магістралі - шлях, розрахований на багато кроків. Ми зробили лише перші кроки, і то навпомацки. Ми подолали певну відстань лише щодо розвитку двох елементів інформаційного простору - Hardware та Software. Але самих апаратного забезпечення (техніка та телекомунікаційні канали зв'язку) та прикладної математики й програмного забезпечення недостатньо.

Не вистачає елемента, що організує цей простір, дає змогу орієнтуватися в ньому та свідомо обирати напрям кожного наступного кроку. Ми маємо на увазі компоненту, яку становлять лінгвістичні засоби та організаційно-правове забезпечення.

Цей процес покладає на Україну тим більшу відповідальність, оскільки від його результату, від того, наскільки українським буде наш сегмент інформаційного простору, залежить наше майбутнє. Причому не лише ступінь участі в міжнародних ринках чи представлення в глобальних представницьких структурах, а й збереження власного культурного, мовного, інтелектуального середовища.

Нашим завданням, окрім усього іншого, є збереження такої національної та політичної одиниці, як Україна, а не просто ще одного ареалу дії норм і принципів, вироблених для інших учасників, що виявились сильнішими й більш стійкими перед навалою перемін.

Сьогодні гостро стоїть проблема вироблення стратегії розвитку-і не лише українського інформаційного суспільства, а й Української держави загалом. Всі без винятку - уряд, бізнесмени, інтелектуальна еліта, товаровиробники, кожен громадянин - повинні мати єдине спільне бачення майбутнього України. Стосовно цього твердження варто згадати слова Паули Уймонсн, експерта Програми розвитку ООН: "Хоча істинно, що інформаційні технології є інструментом соціального розвитку, самі по собі вони не змінять сьогоднішні суспільства. Говорити про інформаційну революцію щонайменше лицемірно, коли взяти до уваги, що фундаментальні аспекти сучасних суспільств швидше відтворюються, ніж змінюються в планах розвитку інформаційного суспільства.

Потрібно заново серйозно обміркувати принципи побудови наших

суспільств. Відправною точкою є знаходження однодумців, поширення ідей серед друзів і колег - людей, що безпосередньо пов'язані з новим способом життя.

Наступною стадією має бути організація мережі однодумців поза безпосереднім соціальним оточенням. Ціле суспільство має поділяти спільний погляд на необхідні перетворення. Це обов'язково має бути зроблено як за допомогою інструментів тилу Інтернету, так і інших засобів задля досягнення максимуму можливого.

Отже, одним впровадженням мікрочіпів інформаційне суспільство створити неможливо. Зміни мають бути системними, такими, що зачеплять кожний елемент суспільної будови, кожен прояв особистості в її самореалізації, що позначиться на самих принципах функціонування суспільного організму. І лише коли перетворення відбудуться в самій структурі суспільних відносин, ми зможемо говорити, що інформаційне суспільство відбулося.

Правовими основами інформаційного суспільства є закони і нормативні акти, що регламентують права людини на доступ до інформаційних ресурсів, технологій, телекомунікацій, захист інтелектуальної власності, недоторканність особистого життя, свободу слова, інформаційну безпеку. Інформаційна безпека суспільства і особистості набуває нового статусу, із суто технологічної проблеми перетворюючись на соціальну, від вирішення якої залежить стійке функціонування сучасних товариств.

Технологічними основами інформаційного суспільства є телекомунікаційні й інформаційні технології, які стали лідерами технологічного поступу, невід'ємним елементом будь-яких сучасних технологій, сприяють економічному зростанню, створюють умови для вільного обігу в суспільстві великих масивів інформації і знань, спричиняють істотні соціально-економічні перетворення і, зрештою, становлення інформаційного суспільства.

Суть і поняття інформації, інформаційної безпеки, захисту інформації

Загальне поняття інформації подано у філософії, де під нею розуміють відображення реального світу. Як філософську категорію ЇЇ вважають одним із атрибутів матерії, що відображає її структуру. Погляд на інформацію з огляду на її споживачів окреслює таке поняття: інформація - це нові відомості, що прийняті, зрозумілі й оцінені її користувачем як корисні. Інакше кажучи, інформація - це нові знання, які отримує споживач (суб'єкт) в результаті сприйняття і перероблення певних відомостей.

Термін "інформація" походить від лат. "informatio", яке має кілька значень:

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

Саме слово "informatio" складається із префікса in- (в-, на-, при-) і

дієслова formo (надаю форму, створюю), пов'язаного з іменником forma (форма).

В англійській мові слово "information" (в написанні "informacioun") вперше з'явилося в 1387 р. Сучасного написання це слово набуло в XVI ст. У східнослов'янські мови слово "інформація" прийшло із Польщі у XVII ст.

Із середини XX ст. інформація стала загальнонауковим поняттям, але досі в науковій сфері воно залишається вкрай дискусійним. Загальноприйнятного визначення інформації не існує, і воно використовується переважно на інтуїтивному рівні.

На нашу думку, інформація з погляду безпеки - це дані, відомості, документи, які мають бути захищеними через їх важливість для суб'єкта діяльності та можливі наслідки від незаконного втручання, розкриття чи розголошування.

Найбільш повну характеристику поняття "інформація" подано у визначеннях нормативно-правових актів. Загалом поняття "інформація" трапляється в багатьох законодавчих та підзаконних нормативно-правових актах. Це зумовлено:

- особливостями розвитку національного законодавства, яке формувалося, на основі потреби термінового врегулювання багатьох сфер суспільного життя;
- інформаційні відносини та інформація як їх предмет є складовою різних видів суспільних відносин;
- інформація може бути товаром, тобто об'єктом цивільно-правових відносин, а обіг управлінської інформації є предметом регулювання адміністративного права.

Основу правового статусу інформації визначає Закон України "Про інформацію". Інформацією у ст. 1 Закону визначено як документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі.

Цивільний кодекс України дещо коригує визначення поняття "інформація": це документовані або публічно оголошені відомості про події та явища, що мали або мають місце в суспільстві, державі та навколишньому середовищі (ст.200).

Існують також інші, переважно несумісні між собою, визначення поняття "інформація". Але практично всі численні погляди на сутність інформації групуються навколо двох концепцій - атрибутивної та функціональної.

Атрибутивна концепція інформації - одна із двох філософських концепцій (парадигм) інформації. Згідно з цією концепцією, інформація - це об'єктивна внутрішня властивість усіх матеріальних об'єктів, вона міститься в усіх без винятку елементах та системах матеріального світу.

Іншими словами, інформація є невід'ємним атрибутом (властивістю) матерії (звідси назва концепції").

Нині багато які вчені та філософи вважають, що доречно говорити про три іпостасі існування матерії:

1) речовина, яка відображає сталість матерії;

2) енергія, яка відображує рух, зміну матерії;

3) інформація, що відображує структуру, організацію матерії. Інформація, згідно з цією концепцією, міститься у формі властивих матеріальним об'єктам структур (така інформація називається структурною, потенційною, апріорною, внутрішньою, інформацією "в собі"). З цим підходом пов'язане визначення інформації як відображення різноманітності.

Інформація в загальному її розумінні є мірою неоднорідності розподілу матерії та енергії у просторі та в часі; мірою змін, якими супроводжуються всі процеси, що відбуваються у світі. Тобто інформація створює уявлення про природу і структуру матерії, про її впорядкованість та різноманіття. Вона не може існувати поза матерією, а отже, існувала й існуватиме вічно, її можна накопичувати, зберігати та переробляти.

Відповідно до цього, процес пізнання розглядають як декодування інформації, що міститься в предметах реального світу.

Функціональна концепція інформації- одна із двох філософських концепцій (парадигм) інформації. Поява цієї концепції пов'язана з розвитком кібернетики - науки про управління та зв'язок у живих організмах, суспільстві й машинах (це дало другу назву концепції -функціонально-кібернетична). Кібернетика формулює принцип нерозривного зв'язку (єдності) інформації з управлінням, з функціонуванням самокерованих та самоорганізовуваних систем (технічних, біологічних та соціальних).

Прихильники функціональної концепції не визнають існування інформації в неживій природі, а саму інформацію визначають як зміст сигналу або повідомлення, отриманого кібернетичною системою із зовнішнього світу.

Розвинута у працях "батька кібернетики" американського математика Норберта Вінера (Norbert Wiener, 1894-1964 рр.) концепція припускає, що процес управління в згаданих системах є процесом переробки (перетворення) певним центральним пристроєм інформації, одержуваної від джерел первинної інформації (сенсорних рецепторів) і передачі її в ті ділянки системи, де вона сприймається її елементами як наказ для виконання тієї або іншої дії. Після виконання самої дії сенсорні рецептори готові до передачі інформації про ситуацію, що змінилася, для здійснення нового циклу управління. Так організується циклічний алгоритм (послідовність дій) управління та циркуляції інформації в системі. Інформаційна система - програмно-технічна та організаційна система надання інформаційних послуг з використанням інформаційних технологій. При цьому важливо, що головну роль тут відіграє зміст інформації, переданої рецепторами і центральним пристроєм. Інформація, за Вінером, - це "позначення змісту, отриманого із зовнішнього світу в процесі нашого пристосування до нього і пристосування до нього наших почуттів".

Багато вчених вважають інформаційні процеси органічними якостями живих систем, які відрізняють їх від неживої природи, неодмінною субстанцією живої матерії, психіки, свідомості. В рамках цього підходу були висунуті твердження, що "специфіка життя пов'язана з наявністю інформації, за

допомогою якої через особливу регуляцію забезпечується процес функціонування системи", "життя - це спосіб існування органічних систем, який ґрунтується на використанні внутрішньої інформації" тощо. Інформація виступає як універсальна "життєва сила", котра керує метаболічними процесами в живих істотах (існує навіть термін "інформаційний метаболізм"), організовує відображення середовища й адаптацію до нього, забезпечує збереження і передачу спадкових ознак, які формують популяцію, біоценози та біосферу в цілому, визначає біологічну еволюцію.

Функціональна концепція інформації представлена двома течіями - кібернетичною й антропоцентричною.

Прихильники кібернетичної течії стверджують, що інформація (інформаційні процеси) присутні в усіх самокерованих (технічних, біологічних, соціальних) системах. Антропоцентрична течія обмежує сферу існування інформації та інформаційних взаємодій винятково людським суспільством та свідомістю. Існування інформації в живій, а тим більше в неживій природі заперечується; вважається, що інформація з'явилася в процесі антропосоціогенезу, й оперувати нею можуть винятково соціалізовані особистості, які володіють мовою, свідомістю та самосвідомістю. Фактично антропоцентристська течія ототожнює поняття "інформація" й "соціальна інформація", оскільки ніякої іншої інформації, крім соціальної, не визнає. Якщо є інформація, то завжди є охочі її отримати, звідси й вимога, що інформація має бути захищена від конкурентів, сторонніх осіб, часом і від партнерів.

У практичній діяльності використовують переважно такі категорії інформації: важлива; корисна; конфіденційна; відкрита; секретна; кодована; закрита.

Для кращого розуміння суті інформації та її особливостей розглянемо загрози, які виникають під час збирання, опрацювання, використання інформації та ухвалення управлінських рішень.

Фахівці науково-технічних, виробничих, економічних та інших служб підприємства повинні визначати загрози безпеці та навчитися правильно й конкретно (у вартісній формі) оцінювати передбачувані і реальні втрати компанії внаслідок просочування інформації, яка віднесена до категорії комерційної таємниці.

Під загрозою безпеці розуміють потенційні дії або події, які можуть прямо чи опосередковано спричинити втрати - призвести до розладу системи, спотворення інформації чи несанкціонованого використання ресурсів мережі, включаючи інформацію, що зберігається, передається або опрацьовується, а також програмні й апаратні засоби.

Нині не існує єдиної загальноприйнятої класифікації загроз, хоча є багато її варіантів.

Загрози поділяють на випадкові (або ненавмисні) і навмисні. Джерелом випадкових можуть бути помилки в програмному забезпеченні, вихід із ладу апаратних засобів, неправильні дії користувачів або адміністрації локальної обчислювальної мережі тощо. Навмисні загрози, на відміну від випадкових,

пов'язані із завданням шкоди користувачам (абонентам) локальної обчислювальної мережі і, в свою чергу, поділяються на пасивні й активні.

Пасивні загрози спрямовані на несанкціоноване використання інформаційних ресурсів локальної обчислювальної мережі, не впливаючи при цьому на її функціонування. Зокрема, пасивною загрозою є спроба отримання інформації, що циркулює в каналах передачі певної локальної обчислювальної мережі, шляхом підслуховування.

Активні загрози спрямовані на порушення нормального функціонування локальної обчислювальної мережі цілеспрямованим впливом на її апаратні, програмні та інформаційні ресурси. До активних загроз належать:

- порушення або радіоелектронне заглушення ліній зв'язку локальної обчислювальної мережі;
- виведення з ладу ЕОМ;
- виведення з ладу операційної системи ЕОМ;
- перекручування відомостей в користувальних базах даних;
- перекручування відомостей системної інформації локальної обчислювальної мережі та ін.

Компрометація інформації здійснюється внесенням несанкціонованих змін у бази даних, внаслідок чого її користувач змушений або відмовитись від неї, або докласти додаткових зусиль до виявлення змін і відновлення справжніх відомостей. У разі використання скомпрометованої інформації користувач може прийняти неправильні рішення з усіма наслідками.

Засобами реалізації загрози розкриття конфіденційної інформації може бути несанкціонований доступ до баз даних (БД), прослуховування каналів локальної обчислювальної мережі тощо. Щоразу отримання інформації, що є власністю якоїсь особи (або групи осіб), завдає її власникам істотної шкоди.

Помилково санкціоноване використання ресурсів локальної обчислювальної мережі теж може призвести до знищення, розкриття або компрометації цих ресурсів. Така загроза є переважно наслідком помилок програмного забезпечення локальної обчислювальної мережі.

Несанкціоноване використання ресурсів локальної обчислювальної мережі, з одного боку, є засобом розкриття або компрометації інформації, а з другого - має самостійне значення, оскільки, навіть не торкаючись користувальної або системної інформації, може завдати певних збитків абонентам або адміністрації локальної обчислювальної мережі. Зміна розміру збитків коливається в широкому діапазоні: від скорочення надходжень фінансових ресурсів до повного виходу мережі з ладу.

Несанкціонований обмін інформацією між абонентами локальної обчислювальної мережі може призвести до отримання одним із них відомостей, доступ до яких йому заборонено, що за наслідками прирівнюється до розкриття інформації.

Відмова в обслуговуванні - дуже істотна й досить поширена загроза, джерелом якої є сама локальна комп'ютерна мережа. Подібна відмова особливо небезпечна в ситуаціях, коли затримка з наданням ресурсів мережі абонентові

може призвести до тяжких для нього наслідків. Наприклад, відсутність в абонента даних, необхідних для прийняття рішень, може бути причиною його нераціональних або неоптимальних дій.

Відмова від інформації полягає у невизнанні адресатом чи відправником цієї інформації, фактів її отримання або відправки. Це, зокрема, може спричинити аргументовану відмову однієї зі сторін від раніше підтриманої угоди (фінансової, торгової, дипломатичної тощо) "технічним шляхом", формально не відмовившись від неї, що завдасть іншій стороні значних збитків.

Формування економічного середовища - створення економічно сприятливих умов для виробництва, запровадження й інвестування у сферу ІКТ з метою розвитку інформаційного суспільства. Йдеться не тільки про підтримку розвитку сектора ІКТ, а й про те, як трансформувати економіку України та зробити її конкурентоспроможною.

Інформаційна безпека - стан захищеності інформаційного простору, який забезпечує формування й розвиток цього простору в інтересах особистості, суспільства та держави.

Інформаційна безпека відіграє істотну роль у забезпеченні життєво важливих інтересів будь-якої країни.

Метою забезпечення інформаційної безпеки в Україні є створення розгалуженого, захищеного інформаційного простору, захист національних інтересів України в умовах формування світових інформаційних мереж, захист економічного потенціалу держави від незаконного використання інформаційних ресурсів, реалізація прав громадян, установ та держави на отримання, поширення й використання інформації.

Загрози інформаційній безпеці - фактор або сукупність їх, що створюють небезпеку функціонуванню та розвитку інформаційного простору, інтересам особистості, суспільства, держави.

Розвиток національної інноваційної системи - створення ефективної інноваційної системи і сприятливого бізнес-середовища, які стимулюватимуть інновації і підприємництво, складовими елементами якої є "наука - технологія - виробництво - ринок" і яка дасть можливість матеріалізувати інформацію і знання у вигляді якісних товарів і послуг.

Розвиток соціального капіталу - створення умов для самореалізації кожної людини. Саме завдяки людині і, що важливо, в її власних інтересах і розвивається інформаційне суспільство. Тому активне інвестування в людський капітал і є головною умовою такого розвитку. Третій сектор має стати активним учасником усіх процесів, що відбуваються в державі, партнером держави і бізнесу в процесі розвитку інформаційного суспільства, активним провідником ідей соціально-економічного розвитку України за допомогою ІКТ.

Захист інформації - сукупність засобів, методів, організаційних заходів щодо запобігання можливим випадковим або навмисним впливам природного чи штучного характеру, наслідком яких можуть 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 проводяться в їх інтересах.

Зазначимо, що порушення інформаційної безпеки зумовлюють безсистемність захисту інформації і слабка координація дій із захисту інформації в загальнодержавному масштабі.

Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, бо реалізація інформаційних загроз - це переважно завдана шкода в політичній, військовій, економічній, соціальній, екологічній та інших сферах.

Нині в Україні немає реальних гарантів інформаційної безпеки країни, комплексу нормативно-правових актів захисту інформаційних ресурсів та інформаційної інфраструктури. Процес інформатизації є стихійним, некерованим, з переважним використанням засобів інформатизації іноземного виробництва.

Така безсистемність процесів формування інформаційної інфраструктури зумовлює складність вирішення проблеми інформаційної безпеки, захисту інформаційних ресурсів. Специфіка цих проблем полягає в тому, що об'єктивно достатнього рівня захищеності інформаційної інфраструктури та інформаційних ресурсів можна досягти тільки у разі чіткого визначення об'єктів інформаційної безпеки України, забезпечення надійного функціонування державних та суспільних інститутів реалізації практичних заходів гарантування інформаційної безпеки.

Проблема інформаційної безпеки має особливе значення в умовах, коли в суспільстві зрозуміли, що інформаційні ресурси є об'єктом власності і мають товарну цінність. Вона не може бути вирішена без впровадження нових ідей, нових знань, нової політики у сфері інформатизації. Концептуальними є пропозиції щодо широкого залучення саме вітчизняних учених та виробників до вирішення цієї проблеми як складової національної безпеки. Вітчизняні фахівці мають гарантувати високу якість інформаційних послуг, безпеку інформаційних технологій, сучасну систему сертифікації програмних і технічних засобів, впровадження стандартизації, створення національних баз даних, систем телекомунікації, безпеку роботи в світовому інформаційному просторі.

Ігнорування проблем інформаційної безпеки може призвести до труднощів у прийнятті найважливіших політичних, економічних, соціальних, військових та інших рішень.

Напрямами інформаційної безпеки є:

1. Система заходів щодо запобігання несанкціонованому доступу до інформації, несанкціонованої її модифікації або порушення цілісності (Informational Security).

2. Захист політичних, державних і громадських інтересів країни, загальних моральних цінностей, запобігання закликам до порушення територіальної цілісності, заборона інформації, яка містить ідеї війни, насилля, дискримінації і посягання на права людини.

3. Запобігання розповсюдженню відомостей, що становлять державну таємницю, а також даних з обмеженим доступом і закритого типу, що переміщуються через державний кордон.

Інформаційне забезпечення урядів, різних державних органів, недержавних організацій та фірм залежить від їхніх потреб у кожному конкретному випадку.

Електронний уряд - система, створення якої сприятиме підвищенню якості, ефективності й прозорості управлінських процесів у державі, а також налагодженню взаємодії державних органів із громадянами, приватним сектором і одного з одним.

Стан захищеності інтересів громадян, суспільства та держави в інформаційній сфері називають інформаційною безпекою. Інформаційна безпека України складається із багатьох компонентів і залежить від:

- рівня забезпечення свободи слова в державі;
- захищеності громадян від впливу на їхнє світосприйняття зовнішніх чинників;
- захищеності населення від впливу на його психічне та фізичне здоров'я таких негативних чинників, як пропаганда жорстокості, насильства тощо;
- наявності в органів влади достатньої інформації для прийняття відповідних рішень.

Ситуація, що склалася в інформаційній сфері нашої держави, потребує невідкладного вирішення таких комплексних проблем:

1) розвиток науково-практичного підґрунтя інформаційної безпеки, а саме:

- визначення основних положень стратегії держави у сфері створення і забезпечення умов формування та використання інформаційного ресурсу;
- підтримка високих темпів його наповнення;
- утримання на відповідному рівні заданих критеріїв якості: доступності; достовірності; своєчасності; повноти;
- розроблення сучасних інформаційних технологій і технічних засобів для вирішення завдання захисту інформації в інформаційних системах;

2) створення нормативно-правової бази для розподілу і використання персональної інформації з метою:

- створення умов для інформаційних відносин між органами державної влади і громадськими;
- створення передумов для досягнення соціального компромісу;
- створення умов становлення соціального партнерства як основи демократичного розвитку суспільства;

- розроблення регламенту інформаційного обміну для органів державної влади і управління;
- створення реєстру інформаційних ресурсів;
- закріплення відповідальності посадових осіб, громадян за додержання вимог інформаційної безпеки;

3) розроблення механізмів реалізації прав громадян на інформацію загального користування;

4) визначення основних положень стратегії держави у сферах:

- використання засобів масової інформації на засадах досліджень процесів формування суспільної свідомості;
- удосконалення та розвиток індустрії інформування населення країни;
- розроблення методів і форм інформаційної політики держави; 5) розроблення методів і засобів оцінювання ефективності систем і засобів інформаційної безпеки та їх сертифікація.

Отже, інформаційна безпека України залежить від вирішення проблем формування суспільної свідомості, процесів виробництва та репродукції інформаційних ресурсів і доступу до них, створення цивілізованого ринку інформаційних продуктів та послуг, реалізації прав громадян на інформацію.

Серед численних проблем гарантування інформаційної безпеки України можна виділити кілька, які найбільше турбують пересічного громадянина - споживача інформації (глядача, читача тощо). Адже близько 35% повідомлень українських ЗМІ стосуються тем насильства, жорстокості, злочинної діяльності тощо. З професійного огляду подій зрозуміло, що для пошуку сенсації, привернення уваги читачів така тематика потрібна, а з огляду на її соціально-виховне значення - ні. Не кращою є ситуація і в царині електронних ЗМІ (телебачення, радіо). Подібна інформація ганьбить людську гідність, особливо негативно впливає на психіку дітей та молоді, спотворює їх світосприйняття, створює негативні настрої в суспільстві.

Наступна проблема українського інформаційного простору - засилля іноземної теле-, радіо -, електронної та друкованої продукції.

Небезпечність такого стану речей полягає в тому, що український інформаційний простір формується здебільшого за рахунок тем і проблем, нагальних для іноземної держави і висвітлюваних з позиції її власних інтересів. А оскільки українські громадяни мають невеликий вибір, особливо серед теле- і радіопрограм, їм просто прищеплюються позиції, які далеко не завжди відповідають дійсності та національним інтересам України. Крім того, зарубіжна інформаційна продукція створює серйозну конкуренцію вітчизняним ЗМІ і заважає їх нормальному розвитку. Останні втрачають прибутки не тільки через зменшення кількості передплатників, покупців, а й через зменшення обсягів реклами, розповсюдження якої їм замовляють.

Ще більш гострою є мовна проблема. З усіх українських періодичних видань лише 20% зареєстровані як україномовні; 65% з них фактично виходять російською мовою. На 90% російськомовним є ефір недержавних радіостанцій та український простір Інтернету. Такий стан речей порушує мовні права

громадян, заважає розвитку української мови, не сприяє підвищенню міжнародного іміджу держави.

Вирішення окреслених проблем є справою далеко не одного року. Для цього потрібно також впроваджувати належну послідовну державну політику і залучати значні кошти, зрештою, мають бути певні зміни в суспільній свідомості.

Нині держава вже зробила певні кроки в напрямі гарантування інформаційної безпеки України:

- законодавчо закріплено норму стосовно обов'язкового не менш ніж 50% наповнення теле- й радіоефіру за рахунок програм вітчизняного виробництва;
- врегульовано порядок використання мов в Україні.

Тому основний напрям вирішення перелічених проблем - виконання чинного законодавства та посилення контролю за цим.

Прикметно, що більшість політичних партій України, незалежно від політичного спрямування, визнають проблеми забезпечення свободи слова, інформаційної безпеки, по-різному оцінюючи такий стан, як задовільний, середній або незадовільний.

Практично не існує розбіжностей у визначенні напрямів вирішення цих проблем. Інша справа, що виникнення їх різні політичні сили пояснюють різними причинами: одні бачать їх у тиску з боку влади, інші - в матеріальній залежності від окремих осіб та груп осіб.

2. *КЛАСИФІКАЦІЯ І ХАРАКТЕРИСТИКА РІЗНИХ ВИДІВ ІНФОРМАЦІЇ*

Інформація - це об'єкт цивільних прав, що належать до категорії нематеріальних благ. Згідно зі ст. 178 ЦК України, 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.

Використовують переважно такі категорії інформації:

- важлива - незамінна та необхідна для діяльності; відновлення її після знищення неможливе або дуже трудомістке і пов'язане із великими витратами, а її помилкове застосування чи підроблення, спотворення й перекручування призводять до великих втрат;
- корисна - необхідна для діяльності, може бути відновлена без великих втрат, причому її модифікація чи знищення призводить до незначних втрат;
- конфіденційна - доступ до неї для частини персоналу або сторонніх осіб небажаний, оскільки може спричинити матеріальні й моральні втрати;
- відкрита - доступ до неї відкритий для всіх.

Керівництво має ухвалювати рішення про те, хто і як визначатиме ступінь конфіденційності і важливості інформації. Вітчизняне законодавство має бути сформоване так, щоб можна було розглядати інформацію як товар і регламентувати права інтелектуальної власності на ринку інтелектуального продукту, як це робиться у світовій практиці.

Для діяльності фірми важливою є інформація про:

- фінансовий стан;
- конкурентоспроможність продукції;
- кількість і якість персоналу.

Сукупність різної інформації, призначеної для ухвалення рішень у сфері підприємництва, можна вважати інформаційним забезпеченням підприємства. Розрізняють вхідну й вихідну інформацію. З огляду на захист інформаційних ресурсів важливою є вихідна інформація.

Вихідну інформацію для підприємства поділяють на:

1) інформацію про стан зовнішнього середовища;

- ринкова кон'юнктура;
- механізм регулювання діяльності фірми владними структурами держави;

2) інформацію про стан фірми або наявні передумови її створення. Інформація про фінансовий стан фірми міститься в головному елементі пакету фінансової звітності - балансі фірми.

Баланс фірми - це деталізована репрезентація фінансового стану фірми на конкретний момент часу ("фотографія в цифрах"), яка відображає, з одного боку, склад, розміщення й використання капіталу (майна) фірми, тобто все те, чим вона володіє на дату складання балансу, а з другого - показує джерела формування та накопичення капіталу (коштів).

Для характеристики ринкової кон'юнктури використовують дані, наведені в офіційних виданнях, статистичних та аналітичних оглядах, комерційних публікаціях, рекламних виданнях, наукових статтях тощо. Корисною і результативною є інформація, добута під час прямого опитування, анкетування та застосування інших прийомів, які широко застосовують у практиці маркетингових досліджень.

Інформація може існувати у вигляді: текстів, малюнків, креслень, фотографій; радіохвиль; магнітних записів; запахів і смакових відчуттів; хромосом, за допомогою яких успадковуються ознаки і властивості організмів; світлових або звукових сигналів; електричних і нервових імпульсів; жестів і міміки.

Досліджуючи поняття "інформація" з огляду на її важливість для бізнесу, слід визнати, що найбільш регламентованою і на певний період достатньо однозначною є інформація про механізм регулювання діяльності компаній, оскільки економічні та адміністративні важелі держави встановлюються відповідними нормативними актами:

- законами, затвердженими законодавчою владою (Верховною Радою);
- декретами, що прийняті виконавчою владою (Кабінетом Міністрів);

- інструкціями, положеннями, рішеннями, що прийняті установами, які мають відповідні права (від державних міністрів до місцевих органів самоврядування).

Тому показники механізму регулювання мають нормативний характер і є обов'язковими до виконання. Нехтування ними призводить до економічних або адміністративних санкцій. Обсяг і зміст нормативної інформації значний, динамічний, що зумовлює велику ймовірність похибок при обґрунтуванні доцільності діяльності компанії. Запобігти цим похибкам можна лише за постійного і систематичного відстеження нормативної документації. Тому в компанії обов'язково має бути відділ чи підрозділ, який би займався цією ділянкою роботи.

Інформація про стан фірми найдоступніша підприємцеві, оскільки формується за його участі. Є певні відмінності в обсязі, складі та джерелах отримання такої інформації для фірми, яка вже діє або лише створюється. На основі вже існуючої інформації можна створити певний інформаційний масив за звітною і плановою інформацією (річні, квартальні, місячні звіти фірми, бухгалтерські звіти, прогнози розвитку фірми тощо).

При створенні інформаційного масиву частина інформації відпадає (наприклад, на підприємстві може не бути певних виробничих потужностей, а отже, і відповідних економічних характеристик), а частина є неповною (наприклад, технічний рівень устаткування за паспортними даними високий, але можливість забезпечити високий рівень технології і організації виробництва ще невідома). Велика кількість інформації також є нормативною, але це внутрішньофірмовий рівень нормативності, наприклад: норми трудомісткості, енергоємності, матеріалоємності продукції, нормативи оборотних коштів, нормативи чисельності та ін.

До інформації, що характеризує стан фірми, можна віднести:

- організаційно-правові характеристики: 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.

Інформацію про регулювання діяльності фірми владними структурами держави можна поділити на такі види (рис. 12.9):

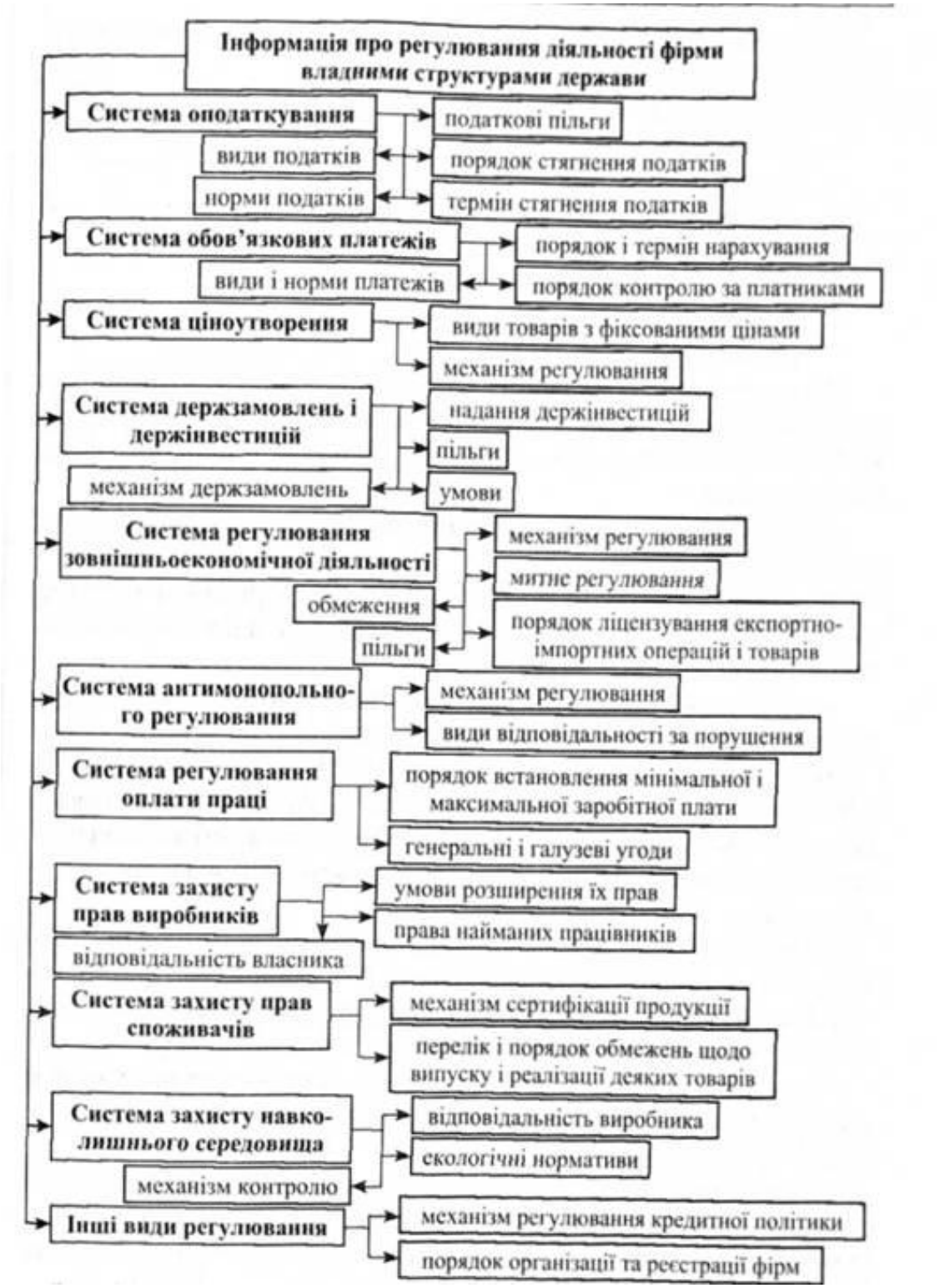


Рис.12.9. Інформація про регулювання діяльності фірми владними структурами держави

Інформацію про ринкову кон'юнктуру при створенні чи розвитку фірми класифікують так (рис. 12.10.):

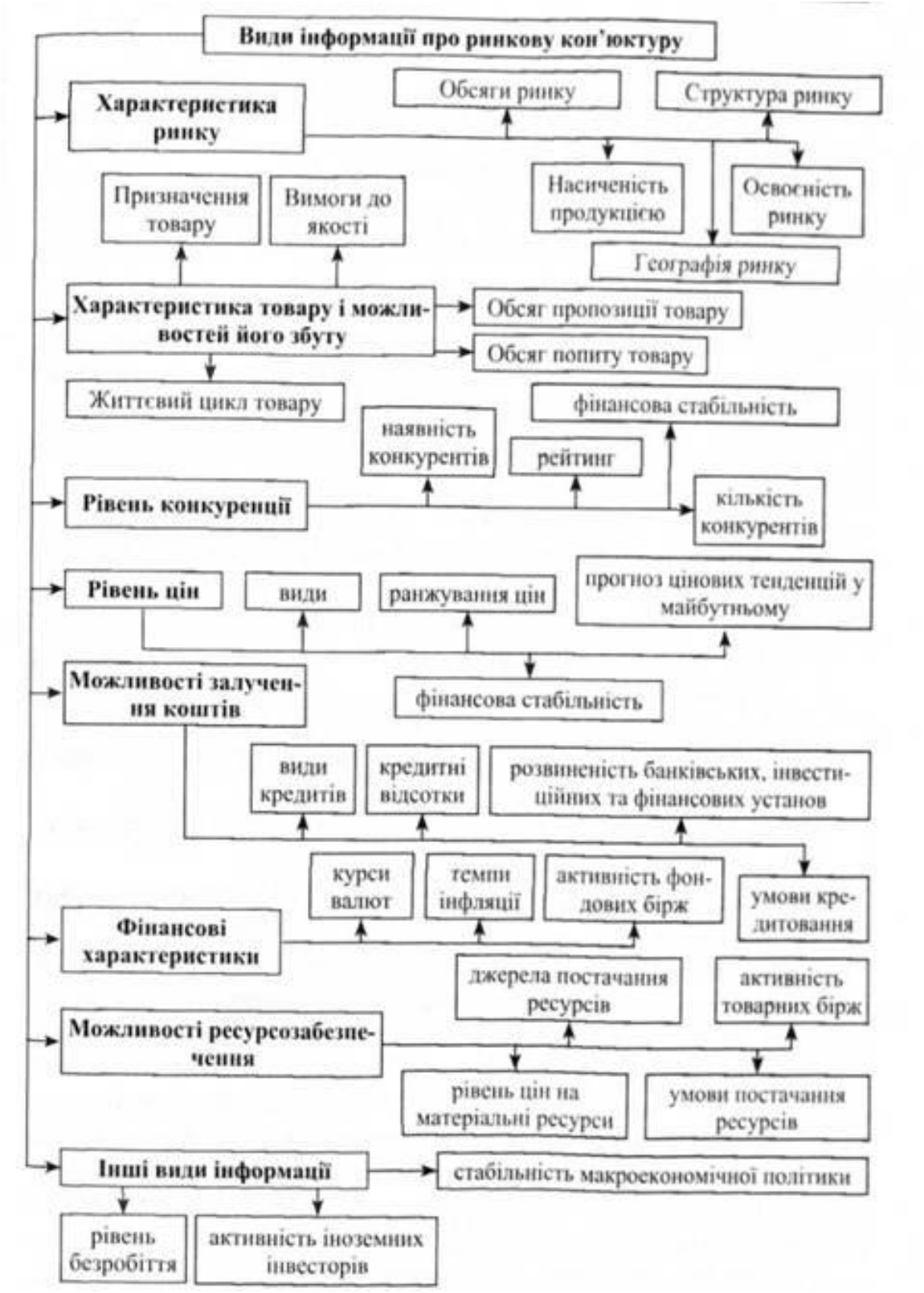


Рис. 12.10. Види інформації про ринкову кон'юнктуру

Основними видами інформації є:

- статистична;
- масова;
- інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування;
- правова; інформація про особу;
- довідково-енциклопедична;
- соціологічна.

Статистична інформація - це офіційна документована державна інформація, що дає кількісну характеристику подій і явищ, які відбуваються в економічній, соціальній, культурній та інших сферах життя України.

Масова інформація - публічно поширювана друкована та аудіовізуальна.

Друкованими засобами масової інформації є періодичні друковані видання (преса): газети; журнали; бюлетені; разові видання з визначеним тиражем.

Аудіовізуальні засоби масової інформації, радіомовлення; телебачення; кіно; звукозапис; відеозапис тощо.

Інформація про діяльність державних органів та органів влади місцевого і регіонального самоврядування - офіційна документована інформація, яка створюється в процесі поточної діяльності законодавчої, виконавчої та судової влади, органів місцевого і регіонального самоврядування.

Основні джерела цієї інформації: законодавчі акти України; інші акти, які приймають Верховна Рада та її органи; акти Президента України; підзаконні нормативні акти; ненормативні акти державних органів; акти органів місцевого й регіонального самоврядування.

Законодавчі та інші нормативні акти, що стосуються прав, свобод і законних інтересів громадян, не доведені до публічного відома, не мають юридичної сили.

Правова інформація - це сукупність документованих або публічно оголошених відомостей про право, його систему, джерела, реалізації юридичні факти, правовідносини, правопорядок, правопорушення та боротьбу з ними і їх профілактику тощо.

Джерелами правової інформації є:

- Конституція України;
- інші законодавчі і підзаконні нормативні правові акти;
- міжнародні договори та угоди;
- норми і принципи міжнародного права;
- ненормативні правові акти;
- повідомлення засобів масової інформації;
- публічні виступи;
- інші джерела інформації з правових питань.

Для забезпечення доступу до законодавчих та інших нормативних актів всіх громадян держава забезпечує видання цих актів масовими тиражами у най коротші строки після набрання ними чинності.

Інформація про особу - це сукупність документованих або публічно оголошених відомостей про особу.

Основними даними про особу (персональними даними) є: національність; освіта; сімейний стан; релігійність; стан здоров'я; адреса; дата і місце народження.

Джерела документованої інформації про особу.

- видані на її ім'я документи;
- документи, підписані особою;
- відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень.

Забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом.

Кожна особа має право на ознайомлення з інформацією, зібраною про неї. Інформація про особу охороняється законом.

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

Основні джерела цієї інформації: енциклопедії; словники; довідники; рекламні повідомлення та оголошення; путівники; картографічні матеріали тощо; довідки, що даються уповноваженими на те державними органами та органами місцевого і регіонального самоврядування, громадськими об'єднаннями, організаціями, їх службовими особами та автоматизованими інформаційними системами.

Система цієї інформації, доступ до неї регулюються бібліотечним, архівним та іншим галузевим законодавством.

Соціологічна інформація - документовані або публічно оголошені відомості про ставлення окремих громадян і соціальних груп до суспільних подій та явищ, процесів, фактів.

Основними джерелами соціологічної інформації є документовані або публічно оголошені відомості, у яких відображено результати соціологічних опитувань, спостережень та інших соціологічних досліджень.

Соціологічні дослідження здійснюються державними органами, громадськими об'єднаннями, зареєстрованими у встановленому порядку.

Джерелами соціологічної інформації £ 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.

Розрізнюють також інформацію: первинну, отриману безпосередньо у місцях її виникнення у процесі спеціальних досліджень, і вторинну - відомості за результатами досліджень, що проводилися раніше, аналітичні узагальнення (статистичні бюлетені, публікації, огляди) (рис. 12.11).

Рис. 12.11. Класифікація джерел інформації

Первинна інформація може бути отримана від:

- власного, створеного "під дослідження" підрозділу фірми;
- спеціалізованої консалтингової фірми (Агентство маркетингових досліджень);
- рекламного агентства.

Первинна інформація може бути отримана від:

- власного, створеного "під дослідження" підрозділу фірми;
- спеціалізованої консалтингової фірми (Агентство маркетингових досліджень)
- рекламного агентства.

Після замовлення такого дослідження зазначені структури розробляють анкету з ключовими запитаннями, наймають додатковий персонал, якщо такий потрібен, збирають дані за допомогою телемаркетингу, проводять опитування, систематизують дані, підбивають підсумки, передають результати замовникові, тобто обґрунтовують пропозиції та вибирають альтернативи.

Перевагами в цій галузі вважаються: вартість послуг; авторитетність; регіональна представленість.

Зрозуміло, що така авторитетна компанія матиме більшу вартість послуг, ніж, скажімо, але для проведення аналізу попиту на певний вид незначної кількості товару запрошувати таку широковідому компанію немає потреби. На рис. 12.12 схематично подано основні найбільш відомі інформаційні агентства.

Отримання первинної інформації часто потребує значних коштів, і інформацію консалтингова фірма часто збирає під інтереси клієнта, спотворюючи цим справжній стан справ. Тому вторинна інформація, яка, можливо, й не повністю відповідає потребам, має свої переваги:

- дешева;
- її швидко отримують;
- часто відомості можна мати лише з держстатистики. На цьому етапі визначають пропозиції щодо розв'язання проблеми.

Рис. 12.12. Найвідоміші інформаційні агентства

Вторинну інформацію можна знайти у спеціалізованих виданнях ("Маркетинг", "Все про бухгалтерський облік", "Вісник АПК", "Економіка України", "The Financial Times"), але найшвидше - за допомогою пошукових серверів Інтернету.

Так, основні макроекономічні показники в Україні розміщені на сайтах Державного комітету зі статистики. Тут можна знайти інформацію про розвиток сільського господарства, промисловості, інвестиційну та будівельну діяльність, транспорт, структурні зміни, експорт, імпорт, споживчий ринок, ціни і тарифи, фінанси, грошові доходи, ринок праці, демографічну ситуацію та ін. Така інформація, безумовно, потрібна для формування як державної політики щодо галузей господарства країни, так і для приватних підприємств та установ.

3. ЗАХИСТ ІНФОРМАЦІЇ

3.1. МЕТОДИ І СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Створення систем інформаційної безпеки (СІБ) в ІС і ІТ ґрунтується на таких принципах:

Системний підхід до побудови системи захисту означає оптимальне поєднання взаємозв'язаних організаційних, програмних, апаратних, фізичних та інших властивостей, підтверджених практикою створення вітчизняних і зарубіжних систем захисту і вживаних на всіх етапах технологічного циклу оброблення інформації.

Принцип безперервного розвитку системи є одним з основоположних для комп'ютерних інформаційних систем та актуальним для СІ Б. Способи уникнення загроз інформації в ІТ безперервно вдосконалюються, тому

гарантування безпеки ІС не може бути одноразовим актом. Це безперервний процес, що полягає у:

- обґрунтуванні та реалізації найбільш раціональних методів, способів і шляхів удосконалення СІ Б;
- безперервному контролі;
- виявленні її вузьких і слабких місць;
- установленні потенційних каналів просочування інформації;
- визначенні нових способів несанкціонованого доступу.

Розмежування і мінімізація повноважень з доступу до оброблюваної інформації і процедур оброблення - це надання як користувачам, так і працівникам ІС мінімуму певних повноважень, достатніх для виконання ними своїх службових обов'язків.

Повнота контролю і реєстрації спроб несанкціонованого доступу означає необхідність точно встановлювати ідентичність кожного користувача і протоколювання його дій для проведення можливого розслідування, а також неможливість здійснювати будь-яку операцію з оброблення і інформації в ІТ без її попередньої реєстрації.

Забезпечення надійності системи захисту полягає в неможливості зниження рівня надійності у разі виникнення в системі збоїв, відмов, навмисних дій зломлювача або ненавмисних помилок користувачів та обслуговуючого персоналу.

Забезпечення контролю за функціонуванням системи захисту - це створення засобів і методів контролю працездатності механізмів захисту.

Забезпечення економічної доцільності використання системи захисту, що виражається в перевищенні можливого збитку ІС і ІТ від реалізації загроз над вартістю розроблення й експлуатації СІ Б.

Система інформаційної безпеки повинна мати певні види власного програмного забезпечення, спираючись на які вона буде здатна виконувати свою цільову функцію.

1. Правове забезпечення - сукупність законодавчих актів, нормативно-правових документів, положень, інструкцій, вимоги яких є обов'язковими в рамках сфери їх діяльності в системі захисту інформації.

2. Організаційне забезпечення - гарантування інформаційної безпеки певними структурними одиницями.

3. Інформаційне забезпечення - відомості, показники, параметри, що є підставою для вирішення завдань, які забезпечують функціонування СІБ (показники доступу, обліку, зберігання, різні розрахункові завдання, пов'язані з діяльністю служби безпеки).

4. Технічне (апаратне) забезпечення - передбачає широке використання технічних засобів для захисту інформації та забезпечення діяльності СІБ.

5. Програмне забезпечення - різні інформаційні, облікові, статистичні й розрахункові програми, що забезпечують оцінювання наявності й небезпеки різних каналів витоку інформації та способів несанкціонованого доступу до неї.

6. Математичне забезпечення - математичні методи, які використовують

для різних розрахунків, пов'язаних з оцінюванням небезпеки технічних засобів, які мають зловмисники, сфер і норм необхідного захисту.

7. Лінгвістичне забезпечення - сукупність спеціальних мовних засобів спілкування фахівців і користувачів у сфері гарантування інформаційної безпеки.

8. Нормативно-методичне забезпечення містить:

- норми і регламенти діяльності органів, служб, засобів, що реалізовують функції захисту інформації;
- різні методики, що забезпечують діяльність користувачів при виконанні своєї роботи за жорстких вимог дотримання конфіденційності.

Нормативно-методичне забезпечення дотичне з правовим.

Нині провідну роль відіграють організаційні заходи захисту інформації. Тому виникає питання щодо організації служби безпеки.

Реалізація політики безпеки потребує налаштування засобів захисту, управління системою захисту і здійснення контролю функціонування ІС. Завдання управління і контролю зазвичай вирішуються адміністративною групою, склад і розмір якої залежать від конкретних умов. Часто така група працює у складі: адміністратор безпеки, менеджер безпеки та оператори.

У найбільшій мережі світу Інтернет атаки на комп'ютерні системи особливо актуальні, вони не знають державних кордонів, не враховують расових чи соціальних відмінностей. Відбувається постійна боротьба інтелекту, а також організованості системних адміністраторів і винахідливості хакерів.

Розроблена корпорацією Microsoft операційна система Windows NT як основа ІС набуває дедалі більшого поширення. І звичайно, хакери всього світу приділяють їй пильну увагу.

Чим більший і сучасніший спосіб отримання інформації, тим більший ризик збереження її конфіденційності. У такому сенсі неабияке значення має захист інформації під час одержання її через Інтернет. За даними CERT Coordination Center, у 1995 р. було зареєстровано 2421 випадок зломів локальних мереж і серверів. За результатами опитування, проведеного Computer Security Institute (CSI), з 1991 р. серед 500 найбільших організацій, компаній та університетів кількість незаконних вторгнень зросла на 48,9 %, а втрати від цих атак оцінюються в $66 млн. У зв'язку з такими колосальними втратами виникає проблема якісного та надійного захисту інформації на будь-якому рівні суспільного життя.

Одним із найбільш використовуваних механізмів захисту від хакерів є міжмережеві екрани - брендмауери (firewalls). Проте зауважимо, що внаслідок непрофесіоналізму частини адміністраторів і вад деяких типів брендмауерів понад 30% зломів відбувається після установки захисних систем. Така ситуація в захисті інформації є проблемою не лише європейських країн. Україна в цій ситуації теж не виняток, вона впевнено доганяє інші країни за кількістю зломів серверів і локальних мереж та завданими ними збитками.

Незважаючи на нібито правовий "хаос", будь-яка діяльність, пов'язана з

розробленням, продажем і використанням засобів захисту інформації, регулюється безліччю законодавчих і нормативних документів, а всі використовувані системи підлягають обов'язковій сертифікації.

Нині питанням безпеки даних у розподілених комп'ютерних системах приділяється велика увага. Розроблено безліч засобів для гарантування інформаційної безпеки, що призначені для використання на різних комп'ютерах з різними ОС. Одним із напрямів є міжмережеві екрани (firewalls), які контролюють доступ до інформації користувачів зовнішніх мереж.

Екран виконує свої функції, контролюючи всі інформаційні потоки між цими двома множинами інформаційних систем, працюючи як "інформаційна мембрана". У цьому сенсі його можна уявити як набір фільтрів, що аналізують інформацію, яка проходить через них, і на основі закладених у них алгоритмів приймають рішення щодо пропуску цієї інформації, затримання чи відмови в пересиланні. Крім того, ця система може реєструвати події, пов'язані із процесами розмежування доступу. Зокрема, фіксувати всі "незаконні" спроби доступу до інформації і додатково повідомляти про ситуації, які потребують негайної реакції.

Зазвичай такі системи роблять несиметричними. Для екранів визначають поняття "усередині" і "зовні", і завдання екрана полягає в захисті внутрішньої мережі від "потенційно ворожого" зовнішнього оточення. Найважливішим прикладом потенційно ворожої зовнішньої мережі є Інтернет.

Для запобігання загрозам інформаційній безпеці та їх усунення використовують правові, програмно-технічні та організаційно-економічні методи.

Правові методи передбачають розроблення комплексу нормативно-правових актів і положень, що регламентують інформаційні відносини в суспільстві, керівних і нормативно-методичних документів щодо гарантування інформаційної безпеки.

Програмно-технічні методи - це сукупність засобів:

- запобігання витоку інформації;
- усунення можливості несанкціонованого доступу до інформації;
- запобігання впливам, які призводять до знищення, руйнування, переключення інформації, або збоям чи відмовам у функціонуванні засобів інформатизації;
- виявлення вмонтованих пристроїв;
- запобігання перехопленню інформації технічними засобами;
- використання криптографічних засобів захисту інформації під час передачі каналами зв'язку.

Організаційно-економічні методи передбачають:

- формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації;
- сертифікацію цих систем відповідно до вимог інформаційної безпеки;
- ліцензування діяльності у сфері інформаційної безпеки;
- стандартизацію способів і засобів захисту інформації;

- контроль за діями персоналу в захищених інформаційних системах.

Важливими для запобігання інформаційним загрозам є мотивація, економічне стимулювання і психологічна підтримка діяльності персоналу, який забезпечує інформаційну безпеку.

Методи і засоби забезпечення безпеки інформації: Перешкода - метод фізичного втручання на шляху зловмисника до захищеної інформації (до документів, апаратури, носіїв інформації тощо).

Управління доступом - методи захисту інформації регулюванням всіх ресурсів ІС і ІТ. Ці методи протистоять можливим способам несанкціонованого доступу до інформації. Управління доступом виконує такі функції захисту:

- ідентифікацію користувачів, персоналу й ресурсів системи (закріплення за кожним об'єктом персонального ідентифікатора);
- пізнання (визначення достовірності) об'єкта або суб'єкта за пред'явленим ним ідентифікатором;
- перевірка повноважень (перевірка відповідності дня тижня, часу доби запрошуваних ресурсів і процедур у межах установленого регламенту);
- дозвіл і створення умов роботи в межах установленого регламенту;
- реєстрація звернень до конфіденційних ресурсів;
- реагування (сигналізація, відключення, затримка робіт, відмова в запиті) у разі спроб несанкціонованих дій.

Механізми шифрування - криптографічне закриття інформації. Цей метод захисту дедалі ширше застосовується під час опрацювання та при зберіганні інформації на магнітних носіях. У разі передавання інформації каналами зв'язку великої протяжності цей метод є єдино надійним.

Протидія атакам шкідливих програм припускає комплекс різних організаційних заходів і використання антивірусних програм. Мета протидії атакам:

- зменшення вірогідності інфікування АІС;
- виявлення фактів зараження системи;
- зменшення наслідків інформаційних інфекцій;
- локалізація або знищення вірусів;
- відновлення пошкодженої інформації в ІС.

Регламентація - створення таких умов автоматизованого опрацювання, зберігання і передавання інформації, що піддягає захисту, за яких норми і стандарти захисту найбільш ефективні.

Примус - метод захисту, за якого користувачі і персонал ІС змушені дотримуватися правил опрацювання, передавання і використання конфіденційної інформації через загрозу матеріальної, адміністративної або кримінальної відповідальності.

Спонука - метод захисту, що спонукає користувачів і персонал ІС не порушувати встановлених порядків за рахунок дотримання моральних і етичних норм, що склалися.

Усю сукупність технічних засобів поділяють на апаратні й фізичні. Крім того є програмні та організаційні, правові й морально-етичні засоби.

Апаратні засоби - пристрої, які вбудовують безпосередньо в обчислювальну техніку, або пристрої, котрі з'єднують із нею за стандартним інтерфейсом.

Фізичні засоби - це різні інженерні пристрої і споруди, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту і здійснюють захист персоналу (особисті засоби безпеки), матеріальних засобів і фінансів, інформації від протиправних дій (замки на дверях, фати на вікнах, засоби електронної охоронної сигналізації).

Програмні засоби - спеціальні програми і програмні комплекси, призначені для захисту інформації в ІС.

Із засобів ПЗ системи захисту варто виділити ще програмні засоби, що реалізовують механізми шифрування (криптографії).

Організаційні засоби здійснюють регламентацію виробничої діяльності в ІС і взаємин виконавців на нормативно-правовій основі так, що розголошування, витік І несанкціонований доступ до конфіденційної інформації стають неможливими або досить складними за рахунок проведення організаційних заходів. Комплекс цих заходів реалізує група інформаційної безпеки, але має бути під контролем першого керівника.

Законодавчі засоби захисту визначаються законодавчими актами країни, якими регламентуються правила користування, опрацювання і передавання інформації обмеженого доступу і встановлюють заходи відповідальності за порушення цих правил.

Морально-етичні засоби захисту - різні норми поведінки, які традиційно склалися раніше, формуються у спосіб розповсюдження ІС і ІТ в країні і світі або спеціально розробляються. Вони можуть бути неписані (чесність) або оформлені в якесь зведення (статут) правил чи розпоряджень. Ці норми зазвичай не є законодавчо затвердженими, але оскільки їх недотримання призводить до падіння престижу організації, вони вважаються обов'язковими для виконання. Характерним прикладом таких розпоряджень є Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США, Кодекс честі аудиторів.

Ні для кого не секрет, що інформація коштує дорого, а іноді навіть занадто дорого. Існує багато методів негласного зняття інформації:

- акустичний контроль приміщення;
- прослуховування телефонних ліній;
- перехоплення комп'ютерної інформації;
- приховане фото - та відеознімання;
- візуальний нагляд;
- підкуп працівників;
- підкуп родичів працівників;
- приймання паразитних електромагнітних випромінювань.

Акустичний контроль приміщення можливий за допомогою: мікрофона, з виведенням сигналу по кабелю; диктофона; стетоскопа; радіомікрофона; телефонної лінії; лазерного зняття інформації з віконного скла.

Спеціальні мікрофони мають дуже маленькі розміри. Інформація із мікрофона передається по кабелю в сусідню кімнату, де виконується її запис. Вузькоспрямований мікрофон дає змогу прослуховувати на відстані до кілометра.

Професійні цифрові диктофони, незважаючи на маленькі розміри, дають змогу безперервно записувати до 20 год розмов. Якщо використати функцію акустопуску (запис здійснюється лише тоді, коли хтось говорить), то залишений диктофон може записувати інформацію дуже довго. Останнім часом диктофони вмонтовують у предмети побуту.

Стетоскоп - прилад, що дає можливість прослуховувати крізь товсті стіни (до 1 м).

Радіомікрофон - основний пристрій для негласного отримання інформації. Залишений один раз в офісі "жучок" буде роками передавати акустичну інформацію радіоканалам. Розміри цих "жучків" залежать від розміру блоку живлення. Якщо "жучок" живиться від стороннього джерела (наприклад, від телефонної лінії), то він зовсім непомітний.

Телефонну лінію використовують не лише для прослуховування телефонних розмов, а й для прослуховування офісу (при цьому трубка лежить на телефонному апараті). Для цього використовують мікрофонний ефект, високочастотне нав'язування, системи "телемонітор", "телефонне вухо" та ін. Деякі системи дають змогу прослуховувати будь-яке приміщення, через котре проходить телефонний кабель, навіть з іншої держави.

За допомогою спеціального лазера можна прослуховувати офіс через зачинене вікно з відстані до кілометра.

Розвиток нових інформаційних технологій і загальна комп'ютеризація зробили інформаційну безпеку обов'язковою і однією з характеристик ІС.

Існує досить розповсюджений клас систем опрацювання інформації, при розробленні яких чинник безпеки відіграє першочергову роль, зокрема банківські інформаційні системи.

Безпека ІС - це захищеність системи від випадкового або навмисного втручання в нормальний процес її функціонування, від спроб розкрадання (несанкціонованого отримання) інформації, модифікації або фізичного руйнування її компонентів. Тобто це здатність протидіяти різним протизаконним діям на ІС.

Загроза безпеці інформації - події або дії, які можуть призвести до спотворення, несанкціонованого використання чи руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів.

Зняти інформацію з комп'ютера можна за допомогою: "хакерського" мистецтва; прихованої камери; спеціального радіоприймача, який приймає паразитичні випромінювання комп'ютера (як правило - монітора) із наступним детектуванням корисної інформації.

Багато хто вважає, що в рівній гладенькій стіні кімнати з євроремонтом неможливо сховати відеокамеру так, щоб її ніхто не побачив. Насправді це можливо.

Будь-яка побутова техніка має побічні електромагнітні випромінювання, які можуть бути промодульовані акустичним сигналом (голосом людини).

Існує безліч методів боротьби із несанкціонованим зняттям інформації. Але найважче боротися із новими, нестандартними методами зняття інформації. Зокрема, дуже важко звичайними методами знайти напівактивний мікрофон, котрий працює через резонатор з вібратором, без джерела живлення, що налаштований на частоту зовнішнього джерела електромагнітного випромінювання (наприклад, паразитне випромінювання розташованого недалеко заводу). Під дією зовнішнього поля в резонаторі виникає електрорушійна сила, що є джерелом випромінювання вібратора. Останній під дією акустичного сигналу коливається, тим самим модулюючи випромінюваний сигнал. Складність виявлення радіомікрофона полягає в тому, що для цього потрібне зовнішнє випромінювання з частотою резонатора. Адже цей радіомікрофон може бути виконаний у вигляді звичайної побутової речі, котра не має жодного радіоелемента.

Карту зайнятості радіоефіру складають як у разі ввімкнутих, так і вимкнутих електроприладів, як за опущеної, так і за піднятої телефонної трубки.

Для захисту інформації можна встановити спеціальне обладнання, зокрема:

1. Для захисту телефонних ліній використовуються:
- аналізатори телефонних ліній;
- прилади активного захисту;
- скремблери;
- фільтри;
- випалювачі засобів зняття;
- універсальні прилади.

2. Для захисту від радіозакладок використовують джерела радіошуму.

3. Для захисту від диктофонів:
- детектори диктофонів;
- прилади, що дистанційно стирають запис із касетних диктофонів.

4. Для захисту від лазерного перехоплення інформації з віконного скла використовують вібратор скла.

5. Для захисту від передачі інформації через лінію:
- фільтри;
- джерела шуму з діапазоном частот 50 - 300 кГц. До додаткових заходів належать:
- демонтаж усіх недіючих електричних кабелів;
- установлення в мережі водо - й теплопостачання діелектричних муфт;
- контроль оперативної обстановки біля офісу: охорона, встановлення камер.

3.2. ОРГАНІЗАЦІЯ І ФУНКЦІЇ ПІДРОЗДІЛІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ.

Інформаційна безпека є комплексом, в якому не можна виділити важливіші чи менш важливі складові. її не можна сприймати інакше, ніж комплекс.

Загрози інформаційній безпеці - чинник або сукупність чинників, що створюють небезпеку функціонуванню й розвитку інформаційного простору, інтересам особистості, суспільства, держави. Основним питанням початкового етапу впровадження системи безпеки є призначення відповідальних осіб за безпеку і розмежування сфер їх впливу. Системні програмісти та адміністратори відносять це завдання до компетенції загальної служби безпеки, тоді як остання вважає, що цим питанням мають займатися спеціалісти по комп'ютерах.

Вирішуючи питання розподілу відповідальності за безпеку комп'ютерної системи, слід ураховувати такі правила:

- ніхто, крім керівництва, не може прийняти основоположні рішення в галузі політики комп'ютерної безпеки;
- ніхто, крім спеціалістів, не зможе забезпечити правильне функціонування системи безпеки;
- ніяка зовнішня організація чи група спеціалістів життєво не зацікавлені в економічній ефективності заходів безпеки.

Організаційні заходи безпеки інформаційних систем прямо чи опосередковано пов'язані з адміністративним управлінням і належать до рішень і дій, які застосовує керівництво для створення таких умов експлуатації, які зведуть до мінімуму слабкість захисту. Адміністрація здійснює:

- заходи фізичного захисту комп'ютерних систем;
- регламентацію технологічних процесів;
- регламентацію роботи з конфіденційною інформацією;
- регламентацію процедур резервування;
- регламентацію внесення змін;
- регламентацію роботи персоналу й користувачів;
- підбір і підготовку персоналу;
- заходи контролю і спостереження.

До стратегічних рішень при створенні системи комп'ютерної безпеки потрібно віднести розроблення загальних вимог щодо класифікації даних, котрі зберігаються і опрацьовуються в системі.

Технічний захист інформації (ТЗІ) - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Технічний захист секретної інформації спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Консультативні послуги в галузі технічного захисту інформації -

розроблення та надання рекомендацій щодо організації (створення) комплексу технічного захисту інформації об'єкта інформаційної діяльності або інформаційної системи на підставі матеріалів їх дослідження; надання методичної допомоги в розробленні нормативно-правових актів, нормативних документів системи ТЗІ, проектної і робочої документації при створенні засобів або комплексів технічного захисту інформації, проведення експертизи таких документів.

Технічний захист інформації є важливим чинником реалізації організаційно-правових та інженерно-технічних заходів з метою запобігання витоку інформації за рахунок несанкціонованого доступу до неї, несанкціонованим діям та впливам на інформацію, які призводять до її знищення, порушення цілісності або блокування, а також протидії технічним розвідкам.

Слід дотримуватися заходів захисту в усіх точках мережі, за будь-якої роботи суб'єктів з корпоративною інформацією.

Правову основу технічного захисту інформації в Україні становлять:

- Конституція України;
- закони України;
- міжнародні договори України;
- угоди, обов'язковість виконання яких введена Верховною Радою України;
- укази Президента України;
- постанови Кабінету Міністрів України;
- розпорядження адміністрації Державної служби спеціального зв'язку та захисту інформації України;
- інші нормативно-правові акти з питань технічного захисту інформації.

Правову основу створення і діяльності ПЗІ становлять:

- Закон України "Про державну таємницю";
- Закон України "Про захист інформації в автоматизованих системах";
- Положення про технічний захист інформації в Україні;
- Положення про забезпечення режиму секретності під час оброблення інформації, що становить державну таємницю, в автоматизованих системах;
- інші нормативно-правові акти з питань захисту інформації;
- державні і галузеві стандарти;
- розпорядчі та інші документи.

Підрозділ захисту інформації (ПЗІ) здійснює діяльність відповідно до "Плану захисту інформації", календарних, перспективних та інших планів робіт, затверджених керівництвом компанії. Проте виконання будь-яких завдань структурними підрозділами залежить від суб'єктів системи технічного захисту, якості їхньої підготовки, професіоналізму, матеріального забезпечення і чіткої взаємодії з іншими структурами компанії та органами контролю.

Під суб'єктом (рис. 12.18) у цьому разі розуміють користувача системи, процес, комп'ютер або програмне забезпечення для оброблення інформації.

Кожен інформаційний ресурс (комп'ютер користувача, сервер організації або мережеве устаткування) має бути захищений від усіх можливих загроз.

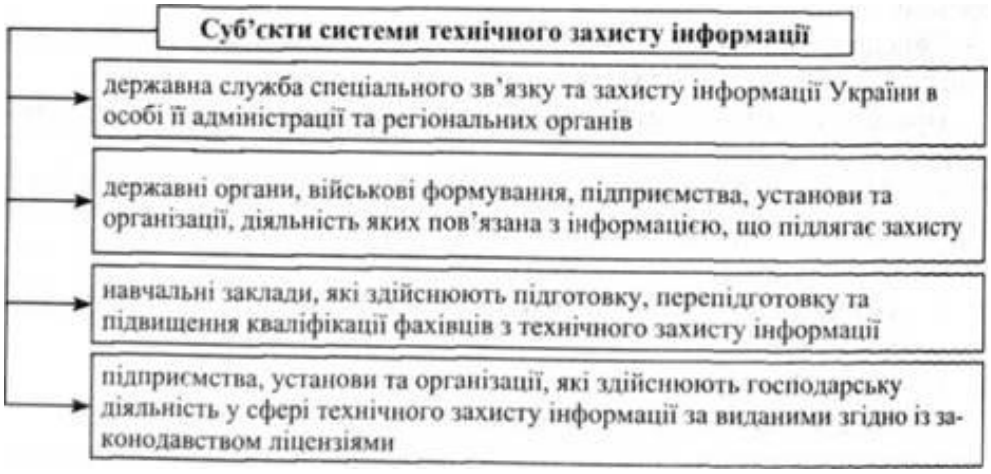


Рис. 12.18. Суб'єкти системи технічного захисту інформації

Державна політика у сфері технічного захисту інформації формується згідно із законодавством і реалізується Держспецзв'язком у взаємодії з іншими суб'єктами системи технічного захисту інформації.

Метою створення ПЗІ є організаційне забезпечення завдань керування комплексною системою захисту інформації (КСЗІ) на підприємстві та здійснення контролю за її функціонуванням. На ПЗІ покладається виконання робіт з:

- визначення вимог щодо захисту інформації в автоматизованій інформаційній системі підприємства (АІС);
- проектування;
- розроблення і модернізації КСЗІ;
- експлуатації;
- обслуговування;
- підтримки працездатності КСЗІ;
- контролю за станом захищеності інформації в комп'ютерних системах (КС).

Для проведення окремих заходів захисту інформації в КС, що пов'язані з напрямом діяльності інших підрозділів компанії, наказом керівництва визначають перелік, строки виконання робіт та виконавців - підрозділи або конкретних осіб. У своїй роботі ПЗІ взаємодіє з підрозділами компанії (режимно-секретним відділом, службою безпеки, відділом ділової розвідки, службою охорони та ін.), а також з державними органами, установами та організаціями, що займаються питаннями захисту інформації.

У разі потреби до виконання робіт можуть бути залучені зовнішні організації, що мають ліцензії на відповідний вид діяльності у сфері захисту інформації.

У будь-якому каналі зв'язку виникають перешкоди, що призводять до

спотворення інформації, яка надходить для опрацювання. Для зменшення вірогідності помилок вживають заходів щодо поліпшення технічних характеристик каналів, використання різних видів модуляції, розширення пропускної спроможності та ін. При цьому також потрібно вживати заходів щодо захисту інформації від помилок або несанкціонованого доступу.

Доступ - це надання можливості використовувати інформацію, що зберігається в ЕОМ (системі).

Будь-яка інформація в машині або системі потребує певного захисту, під яким розуміють сукупність методів управління доступом виконуваних у системі програм до інформації, що зберігається в ній.

Захисту підлягає будь-яка документована інформація, неправомірне поводження з якою може завдати збитку її власникові, користувачеві чи іншій особі.

Режим захисту інформації встановлюють щодо:

- відомостей, віднесених до державної таємниці уповноваженими органами на підставі чинного законодавства;
- конфіденційної документованої інформації власника інформаційних ресурсів або уповноваженою особою на законних підставах;
- персональних даних.

Завданнями підрозділу захисту інформації є:

1. Забезпечення безпеки інформації структурних підрозділів та персоналу компанії в процесі інформаційної діяльності та взаємодії між собою, а також у взаємовідносинах із зовнішніми вітчизняними та закордонними організаціями.

2. Дослідження технології опрацювання інформації з метою виявлення:

- можливих каналів витоку та інших загроз для безпеки інформації;
- формування моделі загроз; розроблення політики безпеки інформації;
- вивчення заходів щодо її реалізації.

3. Організація та координація робіт, пов'язаних із захистом інформації в компанії, необхідність захисту якої визначається чинним законодавством.

4. Підтримка необхідного рівня захищеності інформації, ресурсів і технологій.

5. Розроблення проектів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими має бути забезпечений захист інформації в компанії.

6. Організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу КС.

7. Участь в організації професійної підготовки і підвищенні кваліфікації персоналу та користувачів КС з питань захисту інформації.

8. Формування у персоналу і користувачів компанії розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації.

9. Організація забезпечення виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів із захисту інформації компанії.

10. Проведення контрольних перевірок виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів із захисту інформації компанії.

11. Забезпечення визначених політикою безпеки властивостей інформації під час створення та експлуатації КС.

12. Своєчасне виявлення та знешкодження загроз для ресурсів КС, причин і умов порушення її функціонування та розвитку.

13. Створення механізму та умов оперативного реагування на загрози для безпеки інформації, інші прояви негативних тенденцій у функціонуванні КС.

14. Ефективне знешкодження загроз для ресурсів КС або запобігання їм шляхом проведення комплексу правових, морально-етичних, фізичних, організаційних, технічних та інших заходів гарантування безпеки.

15. Керування засобами захисту інформації, керування доступом користувачів до ресурсів КС, контроль за їхньою роботою з боку персоналу ПЗІ, оперативне сповіщення про спроби НСД до ресурсів КС підприємства.

16. Реєстрація, збирання, зберігання, опрацювання даних про всі події в системі, які стосуються безпеки інформації.

17. Створення умов для максимально можливого відшкодування та локалізації збитків, завданих несанкціонованими діями фізичних та юридичних осіб, впливом зовнішнього середовища та іншими чинниками.

18. Зменшення негативного впливу наслідків порушення безпеки на функціонування КС.

Основними загрозами безпеці інформації і нормального функціонування 1С є такі:

- просочування конфіденційної інформації;
- компрометація інформації;
- несанкціоноване використання інформаційних ресурсів;
- помилкове використання інформаційних ресурсів;
- несанкціонований обмін інформацією між абонентами;
- відмова від інформації;
- порушення інформаційного обслуговування;
- незаконне використання привілеїв.

Просочування конфіденційної інформації - це її безконтрольний вихід за межі ІС або через коло осіб, яким вона була довірена за видом служби або стала відома в процесі роботи. Цей витік може бути наслідком:

- розголошування конфіденційної інформації;
- витоку інформації різними, переважно технічними каналами;
- несанкціонованого доступу до конфіденційної інформації різними способами.

Розголошування інформації, що призвело до ознайомлення з нею осіб, не допущених до цих відомостей, можна кваліфікувати як умисні або необережні дії посадових осіб і користувачів, яким ці відомості були довірені у зв'язку зі службовою потребою. Можливий безконтрольний витік конфіденційної інформації візуально-оптичним, акустичним, електромагнітним та іншими

каналами.

Несанкціонований доступ - це протиправне навмисне оволодіння конфіденційною інформацією особою, яка не має права доступу до відомостей, що охороняються. Найпоширенішими напрямами несанкціонованого доступу до інформації є:

- перехоплення електронних випромінювань;
- примусове електромагнітне опромінювання (підсвічування) ліній зв'язку з метою отримання паразитної модуляції;
- застосування підслуховуючих пристроїв (жучків);
- дистанційне фотографування;
- перехоплення акустичних випромінювань і відновлення тексту принтера;
- зчитування залишкової інформації в пам'яті системи після виконання санкціонованих запитів;
- копіювання носіїв інформації з подоланням заходів захисту;
- маскування під зареєстрованого користувача;
- маскування під запити системи;
- використання програмних пасток;
- використання недоліків мов програмування і операційних систем;
- незаконне підключення до апаратури і ліній зв'язку спеціально розроблених апаратних засобів, що забезпечують доступ інформації;
- зловмисне виведення з ладу механізмів захисту;
- розшифровування спеціальними програмами зашифрованої інформації;
- інформаційні інфекції.

Перелічені напрями несанкціонованого доступу потребують значних технічних знань і відповідних апаратних або програмних розробок з боку зломлювача. Використовують, наприклад, технічні канали витоку - фізичні шляхи від джерела конфіденційної інформації до зловмисника, за допомогою яких можна отримати відомості, що охороняються. Причиною виникнення каналів витоку є конструктивна й технологічна недосконаліть схематичних рішень або експлуатаційне спрацювання елементів. Все це дає змогу зломлювачу робити перетворювачі, що діють за певними фізичними принципами і мають властивий цим принципам канал передачі інформації - канал витоку.

Під час створення та експлуатації КСЗІ компанії підрозділ захисту інформації виконує такі функції:

1. Організація процесу керування КСЗІ.

2. Розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій.

3. Вжиття заходів у разі виявлення спроб НСД до ресурсів КС, порушення правил експлуатації засобів захисту інформації або інших дестабілізаційних факторів.

4. Забезпечення контролю цілісності засобів захисту інформації та

швидке реагування на їх вихід із ладу або порушення режимів функціонування.

5. Організація керування доступом до ресурсів КС - розподіл між користувачами необхідних реквізитів захисту інформації:

- паролів;
- привілеїв;
- ключів та ін.

6. Супроводження й активізація бази даних захисту інформації:

- матриці доступу;
- класифікаційні мітки об'єктів;
- ідентифікатори користувачів тощо.

7. Спостереження (реєстрація і аудит подій в КС, моніторинг подій тощо) за функціонуванням КСЗІ та їх компонентів.

8. Підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в КС, впровадження нових технологій захисту і модернізації КСЗІ.

9. Організація і проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій КС або КСЗІ.

10. Участь у роботах з модернізації КС:

- узгодженні пропозицій щодо введення до складу КС нових компонентів;
- нових функціональних завдань;
- режимів оброблення інформації, заміни засобів оброблення інформації тощо.

11. Забезпечення супроводження й активізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їх зберігання і тестування.

12. Проведення аналітичного оцінювання поточного стану безпеки інформації в КС:

- прогнозування виникнення нових загроз та їх врахування в моделі загроз;
- визначення необхідності її коригування;
- аналіз відповідності технології оброблення інформації;
- аналіз реалізованої політики безпеки поточної моделі загроз та ін.

13. Доведення власникам інформації технічних можливостей захисту інформації в КС і типові правила для персоналу і користувачів КС.

14. Негайне втручання в процес роботи КС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника.

15. Регулярне подання звітів керівництву компанії-власника (розпорядника) КС про виконання користувачами КС вимог захисту інформації.

16. Аналіз відомостей про технічні засоби захисту інформації нового покоління.

17. Обґрунтування пропозицій щодо придбання засобів для компанії.

18. Контроль за виконанням персоналом і користувачами КС вимог, норм,

правил, інструкцій щодо захисту інформації відповідно до визначеної політики її безпеки.

19. Контроль забезпечення режиму секретності у разі оброблення в КС інформації, що становить державну таємницю.

20. Контроль забезпечення охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що піддягають захисту.

21. Розроблення і реалізація спільно з РСВ компанії комплексних заходів безпеки інформації під час проведення заходів з науково-технічного, економічного, інформаційного співпраці з іноземними фірмами.

22. Розроблення і реалізація спільно з РСВ компанії комплексних заходів безпеки інформації під час проведення нарад, переговорів тощо, здійснення їх технічного та інформаційного забезпечення.

Більшість систем захисту в таких випадках використовують набори привілеїв, тобто для виконання певної функції потрібний певний привілей. Зазвичай користувачі мають мінімальний набір привілеїв, адміністратори - максимальний.

Набори привілеїв охороняються системою захисту. Несанкціоноване (незаконне) захоплення привілеїв можливе за наявності помилок у системі захисту, але здебільшого - в процесі керування системою захисту, зокрема у разі недбалого користування привілеями.

Чітке дотримання правил керування системою захисту, принципу мінімуму привілеїв дає змогу уникнути таких порушень.

3.3. СПЕЦИФІКА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ.

Технічний захист інформації - це не данина моді, а вимога часу. Адже на сучасному етапі розвитку суспільства інформація є чи не найдорожчим товаром, одним з найважливіших джерел процвітання будь-якої фірми. Широкомасштабне впровадження інформаційних технологій потребує значної уваги до питань технічного захисту інформації, оскільки несанкціонований витік її може призвести до втрати фірмою позицій на ринку і значних фінансових збитків.

Одним із напрямів захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ поділяють на два великих класи завдань:

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

Технічні канали - це канали побічних електромагнітних випромінювань і наведень (ПЄМВН), акустичні канали, оптичні та ін.

Для розв'язання всього комплексу завдань компанія має співпрацювати з провідними державними та недержавними підприємствами й організаціями, що працюють у галузі захисту інформації, в тому числі: зі Службою безпеки України, державним підприємством "Українські спеціальні системи" та ін.

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

1. прикладне й системне ПЗ:
- системи розмежування доступу до інформації;
- системи ідентифікації та аутентифікації;
- системи аудиту й моніторингу;
- системи антивірусного захисту.

2 апаратна частина серверів та робочих станцій:
- апаратні ключі;
- системи сигналізації;
- засоби блокування пристроїв та інтерфейсів вводу-виводу інформації.

3. комунікаційне обладнання і канали зв'язку:
- міжмережеві екрани (Firewall) - для блокування атак із зовнішнього середовища.

4. периметр інформаційної системи, для захисту якого створюються системи:
- охоронної та пожежної сигналізації;
- цифрового відеоспостереження;
- контролю та управління доступом (СКУД).

Захист інформації від її витоку технічними каналами зв'язку забезпечується:

- використанням екранованого кабелю та прокладанням проводів і кабелів в екранованих конструкціях;
- установленням на лініях зв'язку високочастотних фільтрів;
- побудовою екранованих приміщень ("капсул");
- використанням екранованого обладнання;
- установленням активних систем зашумлення;
- створенням контрольованої зони.

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.

3.4. ОСОБЛИВОСТІ ЗАХИСТУ ЕЛЕКТРОННОЇ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ. МІЖНАРОДНІ СТАНДАРТИ БЕЗПЕКИ ІОС.

Безпека електронної системи, як відомо, - це здатність її протидіяти спробам завдати збитків власникам і користувачам систем у разі появи різних збуджувальних (навмисних і ненавмисних) впливів на неї. Такими впливами можуть бути:

- спроба проникнення зловмисника;
- помилки персоналу;
- стихійні лиха (ураган, пожежа);

- вихід з ладу окремих ресурсів.

Розрізняють внутрішню і зовнішню безпеку електронної системи. Внутрішня безпека враховує захист від стихійного лиха, від проникнення зловмисника, отримання доступу до носіїв інформації чи виходу системи з ладу. Предметом внутрішньої безпеки є забезпечення надійної і коректної роботи системи, цілісності її програм і даних.

Нині склалися два підходи до гарантування безпеки електронних систем:

1. фрагментарний, за якого створюється протидія суворо визначеним загрозам за певних умов:

- спеціалізовані антивірусні засоби;
- автономні засоби шифрування тощо;

2. комплексний, який передбачає створення середовища оброблення інформації, яке поєднує різні заходи ля протидії загрозам:

- правові;
- організаційні;
- програмно-технічні.

Комплексний підхід використовують переважно для захисту великих систем, типові програмні засоби яких містять вмонтовані засоби яких захисту інформації, але цього недостатньо. В цьому разі потрібно проводити такі заходи:

- організаційні заходи контролю за персоналом, який має високий рівень повноважень щодо дії в системі: за програмістами; за адміністраторами баз даних мережі тощо;
- організаційні й технічні заходи резервування критично важливої інформації;
- організаційні заходи з відновлення працездатності системи у разі виникнення непередбачуваних ситуацій;
- організаційні й технічні заходи управління доступом у приміщеннях, де міститься обчислювальна техніка;
- організаційні й технічні заходи з фізичного захисту приміщень, в яких міститься обчислювальна техніка і носії даних, від стихійних лих, масових безпорядків тощо.

Міжнародні стандарти безпеки інформаційно-обчислювальних систем

Аналізуючи ситуацію в світі у сфері стандартизації щодо інформаційної безпеки за роки розвитку індустрії І Б, можна виділити такі тимчасові періоди, назва яких найбільш чітко характеризує природний розвиток цього процесу: поява стандартів (1988 - 1995 рр.), випробування практикою (1996 - 2000) і виживання сильних (від 2001 р. і дотепер).

Характерним для першого етапу є природний розвиток інформаційних технологій, за яким ледве встигала наука і практика у сфері ІБ. На цьому етапі формувалися понятійний апарат та основні підходи у сфері ІБ, аж до найкращих. Період кінця 80-х і особливо початок 90-х років характеризувався появою величезної кількості різних стандартів у сфері ІБ. Вони з'являлися як в окремих компаніях, або в консорціумах (X-Open, Good Practice тощо), так і в

таких авторитетних інститутах, як NIST (National Institute of Standards and Technologies) і комплекс BSI (British Standards Institute) з ISO (International Standards Organisation). Зазначимо, що NIST і BSI нині є основними світовими конкурентами у сфері стандартизації.

Природними недоліками стандартів на цьому етапі були:

- слабке практичне опрацьовування;
- брак єдиних підходів;
- брак єдиного розуміння інформаційної безпеки.

Лише час міг подолати ці недоліки, що й відбулося на другому і третьому етапах - практичне застосування стандартів стимулювало їх природний відбір.

Етап випробування практикою в середині 90-х років плавно перейшов в етап природного відбору і виживання сильних стандартів. Очевидно, сфера ІБ є досить замкнутою і обмеженою, через що є зайвою величезна кількість стандартів, які перетинаються один з одним і намагаються різними способами описати одну і ту саму наочну сферу.

На практиці вистачає кількох основоположних стандартів, які визнаються фахівцями й використовуються бізнесом на практиці. Таким чином, у цій битві стандартів виживали й вижили сильні, зокрема стандарт ISO 15408, що регламентує вимоги до захищеності ПО, або стандарт управління ISO 27001/17799 . Ці стандарти нині дістали статус міжнародних. Щоправда, є одне "але". Світ розділився на дві географічно незалежні з огляду на стандартизацію зони: Європа й Азія визнають стандарти ISO , а США вважає за краще використовувати стандарти N 1ST. Зазначимо маловідомий факт: багато які найбільш відомі стандарти ISO ґрунтуються на BSI: ISO 17799, ISO 9001, ISO 14001.

У 1985 р. Національний центр комп'ютерної безпеки Міністерства оборони США опублікував "Оранжеву книгу" ("Критерії оцінки достовірності обчислювальних систем Міністерства оборони"). В ній наведено основні положення, за якими американське відомство оборони визначало ступінь захищеності інформаційно-обчислювальних систем; систематизовано основні поняття, рекомендації та класифікацію за видами загроз безпеці інформаційних систем, методи захисту від них, які далі перетворилися на зведення науково обґрунтованих норм і правил, що описують системний підхід до гарантування безпеки інформаційних систем та їх елементів.

Запропонована в "Оранжевій книзі" методологія стала загальноприйнятою та увійшла в національні стандарти (рис. 12.19).

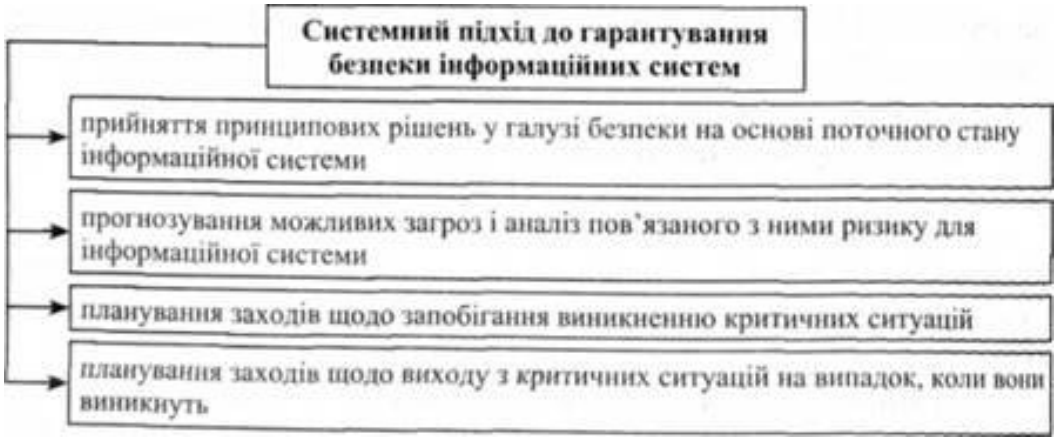


Рис. 12.19. Системний підхід для гарантування безпеки інформаційних систем

Поняття "політика безпеки" було також введене "Оранжевою книгою".

Політика безпеки - це сукупність норм, правил і методик, на основі яких в подальшому будується діяльність інформаційної системи в галузі опрацювання, зберігання і розподілу критичної інформації.

Інформаційна система - це не лише апаратно-програмний комплекс, а й обслуговуючий персонал.

Політика безпеки формується на основі аналізу поточного стану і перспективи розвитку інформаційної системи, можливих загроз і визначає:

- мету, завдання і пріоритети системи безпеки;
- галузь дії окремих підсистем;
- гарантований мінімальний рівень захисту;
- обов'язки персоналу щодо забезпечення захисту;
- санкції за порушення захисту.

Якщо політика безпеки проводиться не повною мірою або непослідовно, то ймовірність порушення захисту інформації різко зростає.

Визначення політики безпеки неможливе без аналізу ризику, який підвищує рівень поінформованості про слабкі й сильні сторони захисту, створює базу для підготовки та прийняття рішень, оптимізує розмір витрат на захист, оскільки більшість ресурсів спрямовується на блокування загроз, що можуть завдати найбільшої шкоди. Аналіз ризику складається з таких основних етапів (рис. 12.20).

Аналіз ризику завершують прийняттям політики безпеки і складанням плану захисту,що має такі розділи:

1. Поточний стан. Опис статусу системи безпеки в момент підготовки плану.

2. Рекомендації. Вибір основних засобів захисту, що реалізують політику безпеки.

3. Відповідальність. Список відповідальних працівників і зон відповідальності.

4. Розклад. Визначення порядку роботи механізмів захисту, в тому числі і засобів контролю.

5. Перегляд положень плану, які потрібно періодично переглядати.

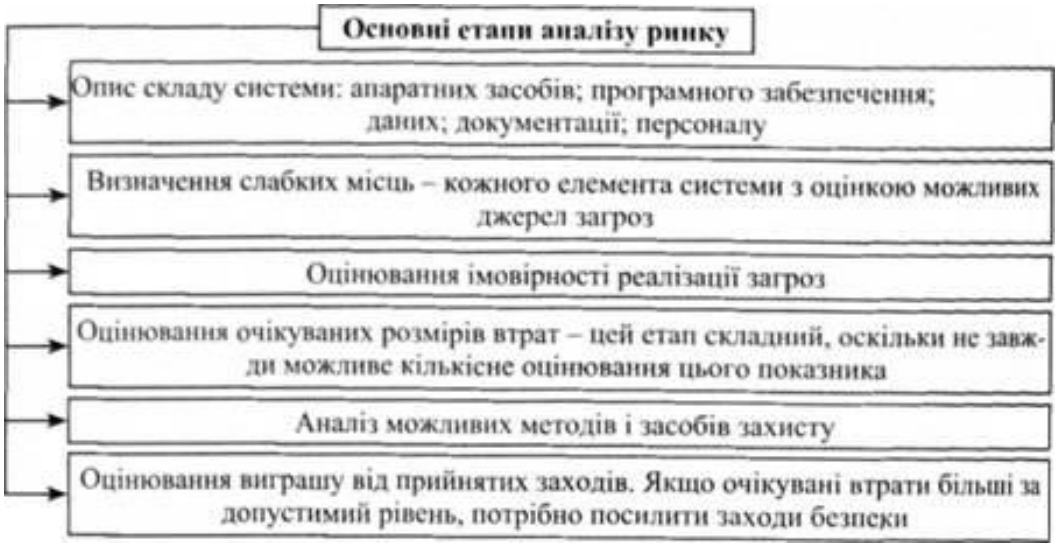


Рис. 12.20. Основні етапи аналізу ризику

У загальній системі гарантування безпеки захист інформації відіграє значну роль. Виділяють такі підходи до організації захисту інформації:

- фізичні;
- законодавчі;
- управління доступом;
- криптографічне закриття.

Фізичні способи передбачають застосування фізичних перешкод для зловмисника, які закривають шлях до захищеної інформації (надійна система допуску на територію чи в приміщення з апаратурою або носіями інформації). Ці способи захищають лише від зовнішніх зловмисників і не захищають інформацію від осіб, які володіють правом входу в приміщення. Практика свідчить, що 75% порушень здійснюють працівники організації.

До законодавчих способів захисту належать законодавчі акти, які регламентують правила використання й опрацювання інформації з обмеженим доступом і встановлюють міру відповідальності за порушення цих правил. Сюди належать також внутрішньо-організаційні методи роботи і правила поведінки.

Управління доступом - захист інформації з регулюванням доступу до ресурсів системи:

- технічних;
- програмних;
- елементів баз даних. Регламентується порядок роботи користувачів і персоналу, право доступу до окремих файлів в базах даних і т.ін.

Відповідно до встановленої класифікації даних, користувачів, апаратури,

приміщень відповідальні за безпеку розробляють багаторівневу підсистему управління доступом (рис. 12.21).

Для захисту від несанкціонованого під'єднання до системи здебільшого використовують перевірку паролів, засоби антивірусного захисту і контролю цілісності, контролю та управління захисними механізмами, програми відновлення й резервного збереження інформації.

Комплексний розгляд питань гарантування безпеки відображений у структурі безпеки, де зазначено загрози безпеки, послуги й механізми її забезпечення.

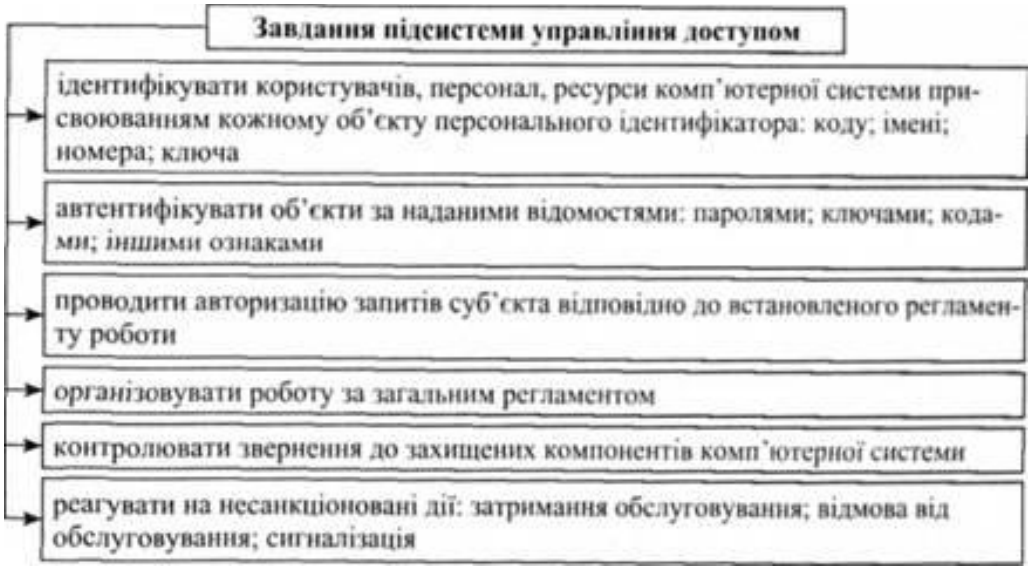


Рис. 12.21. Завдання підсистеми управління доступом

На концептуальному рівні служби безпеки специфікують напрями нейтралізації загроз. Усі напрями організації захисту інформації (фізичні, законодавчі, управління доступом, криптографічне закриття) реалізуються механізмами безпеки. В межах ідеології "відкритих систем" служби й механізми безпеки потрібно використовувати на будь-якому рівні еталонної моделі: фізичному; канальному; мережевому; транспортному; сеансному; представницькому; прикладному.

Протоколи інформаційного обміну поділяють на дві групи:

- віртуального з'єднання;
- дейтаграмні.

Відповідно до зазначених протоколів мережі поділяють на віртуальні й дейтаграмні. У віртуальних мережах інформація між абонентами передається віртуальним каналом і проходить три етапи (фази):

- створення (встановлення) віртуального каналу;
- передача віртуального каналу;
- знищення віртуального каналу (роз'єднання). При цьому повідомлення розбивається на блоки (пакети), які передаються в порядку їх

розташування в повідомленні.

У дейтаграмних мережах блоки повідомлень передаються від відправника до адресата незалежно один від одного та різними маршрутами, тому порядок доставки блоків може не відповідати порядку їх розміщення у повідомленні.

Отже, віртуальна мережа в концептуальному плані відповідає принципу організації телефонного зв'язку, а дейтаграмна - поштовому. Ці два підходи визначають деякі розбіжності у складі та особливостях служб безпеки.

Криптографічне закриття інформації у комп'ютерних системах є найефективнішим способом захисту інформації із властивим йому високим рівнем захисту. В основі цього способу лежать програми криптографічного перетворення (шифрування) та програми захисту юридичної вагомості документів (цифровий підпис). Шифрування забезпечує засекречування інформації і використовується низкою інших сервісних служб (рис. 12.22).

При цьому наявність чи знання загальнодоступного ключа не дає змоги визначити секретний ключ.

Рис. 12.22. Класифікація шифрування

Для використання механізмів криптографічного закриття інформації в локальній обчислювальній мережі потрібна налагоджена організація спеціальної служби генерації ключів та їх розподіл між її абонентами.

Російський стандарт шифрування даних ГОСТ 28147-89 - єдиний алгоритм криптографічного перетворення даних для великих інформаційних систем. Не накладає обмежень на ступінь секретності інформації. Має переваги алгоритму DEC і водночас позбавлений його недоліків.

Метод з відкритим ключем (RSA)

Шифрування проводиться першим відкритим ключем, розшифрування - іншим секретним ключем. Спеціалісти з криптографії вважають, що системи з відкритим ключем зручніше застосовувати для шифрування даних, що передаються, ніж при збереженні інформації. Існує ще одна галузь використання цього алгоритму - цифрові підписи, що підтверджують справжність документів і повідомлень, які передаються. Проте і він не є досконалим. Його недоліком є не до кінця вивчений алгоритм.

Захист інформації здійснюють:

- комплексним застосуванням різних засобів і методів;
- створенням структури захисту й охорони з кількома рівнями;
- постійним їх удосконаленням.

Успіх справи залежить від збалансованої й налагодженої взаємодії захисту операційних систем і гарантування безпеки баз даних.

У межах цієї програми розрізняють такі пасивні об'єкти захисту.

- файли;
- прикладні програми;
- термінали;
- ділянки оперативної пам'яті.

Активними є суб'єкти (процеси) захисту, котрі можуть виконувати над об'єктами визначені операції. Захист об'єктів здійснюється операційною системою засобів контролю за виконанням суб'єктами захисту сукупності правил, що регламентують ці операції. Статус захисту - це сукупність правил, які регламентують захист об'єктів.

Під час свого функціонування суб'єкти генерують запити на виконання операцій над захищеними об'єктами. Права (атрибути) доступу - це операції, які виконуються над захищеними об'єктами, а права доступу суб'єкта стосовно конкретного об'єкта є можливостями. Наприклад, правом доступу може бути "запис у файл", а можливістю - "запис у файл ЛГ' (JV- ім'я конкретного файлу, тобто об'єкта, в нашому випадку файлу "Наука").

Для формальної моделі статусу захисту в операційній системі використовують переважно матрицю доступу. Вона містить m рядків (за кількістю суб'єктів) і п стовпців (за кількістю об'єктів). При цьому елемент, що міститься на перетині 1-го рядка іу-го стовпця, є множиною можливостей і-го суб'єкта стосовно j-го об'єкта. Слід пам'ятати, що числа т і п на практиці здебільшого великі, а число множини можливостей елементів матриці доступу мале.

Досить простим у реалізації засобом розмежування доступу до захищених об'єктів є механізм кола безпеки. Коло безпеки характеризується своїм унікальним номером. Нумерація здійснюється "із середини - назовні", і внутрішні кільця є привілегійованими щодо зовнішніх. Суб'єкту (домену), що оперує в межах кола з номером, доступні всі об'єкти з номерами від / до N включно.

Доступ до ресурсів операційної системи може обмежуватися засобами захисту за паролями, який може бути використаний також як ключ для шифрування-дешифрування інформації в користувальних файлах. Самі паролі також зберігаються у зашифрованому вигляді, що утруднює їх виявлення і використання зловмисниками. Пароль може бути змінений користувачем, адміністратором системи або самою системою після встановленого інтервалу часу.

3.5. ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В РІЗНИХ СФЕРАХ ДІЯЛЬНОСТІ

Захисту підлягає будь-яка документацій на інформація, оскільки неправомірне її використання може завдати збитків її власникові, користувачеві та іншим особам. Неправомірний доступ до інформаційних ресурсів може завдати втрат громадянам, організаціям (юридичним особам) та державі загалом, а також базі нормативно-технічних документів з ТЗІ. Метою захисту інформації має бути:

- запобігання відтоку, розкраданню, втраті, перекручуванню, підробці інформації;
- запобігання загрозам державної безпеки, безпеки особистості, суспільства загалом;
- запобігання несанкціонованим діям зі знищення, модифікації, копіювання, блокування інформації; запобігання іншим формам незаконного втручання в інформаційні ресурси та інформаційні бази даних і системи, забезпечення правового режиму документованої інформації як об'єкта власності;
- захист конституційних прав громадян на збереження особистої таємниці та конфіденційності персональних даних, що є в інформаційних системах і ресурсах суб'єктів і об'єктів різних форм власності;
- збереження державної таємниці, конфіденційності документованої інформації згідно з чинним законодавством;
- забезпечення прав суб'єктів в інформаційних процесах під час розроблення, виробництва та застосування інформаційних систем, технологій і засобів їх забезпечення.

Режим захисту інформації має передбачати поділ інформаційних ресурсів за такими критеріями:

- відносне віднесення відомостей до державної таємниці уповноваженими органами на основі Закону України "Про державну таємницю";
- конфіденційність документування інформації власником інформаційних ресурсів чи уповноваженою особою на основі Закону України "Про захист інформації*";
- збереження персональних даних на основі Закону України "Про захист інформації".

Органи державної влади та організації, що несуть відповідальність за формування й використання інформаційних ресурсів, що підлягають захисту, а також органи та організації, що розробляють і застосовують інформаційні системи й технології для формування та використання інформаційних ресурсів з обмеженим доступом, керуються у своїй діяльності законодавством України.

Органи державної влади здійснюють контроль за дотриманням вимог щодо захисту інформації та експлуатації спеціальних програмно-технічних

засобів захисту, вживають організаційних заходів захисту інформаційних систем, що опрацьовують інформацію, з обмеженим доступом в недержавних структурах. Організації, які опрацьовують інформацію з обмеженим доступом, що є власністю держави, створюють спеціальні служби для захисту інформації. Однак є й приватні структури, які займаються наданням послуг щодо захисту інформації.

Власник інформаційних ресурсів або уповноважені ним особи мають право здійснювати контроль за виконанням вимог до захисту інформації та забороняти чи призупиняти оброблення інформації у разі невиконання цих вимог, а також може звертатися в органи1 державної влади з приводу оцінювання правильності виконання та дотримання вимог захисту його інформації в інформаційних системах. Ці органи дотримуються вимог конфіденційності інформації та результатів перевірки.

Власник документів інформаційних систем, згідно з чинним законодавством, забезпечує умови доступу користувачів до інформації та порядок надання їм інформації. Підставою для забезпечення рівня захисту інформації є чинне законодавство України.

Власник документів має сповіщати власника інформаційних ресурсів та систем про всі факти порушення режиму захисту інформації.

Захист прав суб'єктів у сфері формування та користування інформаційними ресурсами, розроблення, виробництва та застосування інформаційних систем, технологій і засобів їх забезпечення здійснюється з метою запобігання правопорушенням, неправомірним діям, відновлення порушених прав та відшкодування заподіяної шкоди.

Захист прав суб'єктів у вказаній формі здійснюється судами з урахуванням специфіки правопорушення та завданих збитків. Для перегляду конфліктних ситуацій і захисту прав учасників у сфері формування, використання інформаційних ресурсів та їх технологій і засобів їх забезпечення можуть створюватись тимчасові і постійні третейські суди.

Донедавна Інтернет використовували практично кожна фірма, кожне підприємство незалежно від форми власності та виду господарської діяльності, переважно для опрацювання інформації простих протоколів:

- електронна пошта;
- передавання файлів;
- віддалений доступ.

Нині завдяки великому поширенню технологій www дедалі активніше застосовують засоби розподіленого опрацювання мультимедійної інформації. Одночасно з цим зростає обсяг даних, що опрацьовуються в середовищах клієнт/сервер і призначені для одночасного колективного доступу великої кількості абонентів. Розроблено кілька протоколів прикладного рівня, що забезпечують інформаційну безпеку таких додатків:

- електронна пошта (PEM, PGP і т. і.);
- www (Secure HTTP, SSL і т.п.);
- мережеве управління (SNMPv2 тощо).

Проте наявність засобів гарантування безпеки у базових протоколах сімейства TCP/IP дасть змогу здійснювати інформаційний обмін між широким спектром різних додатків і сервісних служб.

Засоби безпеки протоколу IP дають змогу управляти захистом всього IP-трафіка від джерела інформації до її одержувача. Можливості управління безпекою IP (IP Security Management) в системі Windows 2000 дозволяють призначати і застосовувати політику безпеки IP, яка гарантує захищений обмін інформацією для всієї мережі.

Механізм безпеки IP є реалізацією протоколу безпеки IP (IP Security, IPSec), прозорою для користувача, адміністрування безпеки централізоване і поєднує гарантії безпечного обміну інформацією із легкістю застосування.

Захист мереж, заснованих на протоколі IP, сьогодні є реальною потребою, має велике значення і зростає з кожним роком. Нині у взаємозв'язаному діловому світі мереж Інтернет, інтранет, екстранет (extränet - корпоративна мережа, складові частини якої зв'язані через відкриті мережі, наприклад через Інтернет), філіалів і віддаленого доступу у мережах передається важлива інформація, конфіденційність якої має бути дотримана. Однією з основних вимог до мережі з боку мережевих адміністраторів та інших професіоналів, що обслуговують і використовують мережі, є вимога гарантії, що цей трафік буде захищений:

- доступу суб'єктів, що не мають на це прав;
- перехоплення, перегляду або копіювання;
- модифікації даних під час шляху в мережі.
- Ці проблеми характеризуються такими показниками:
- цілісність даних;
- конфіденційність;
- достовірність.

Одночасно захист від повторного використання (replay protection) запобігає прийняттю повторно надісланого пакету.

3.6. ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ СПРАВ

Інтенсивне впровадження сучасних інформаційних технологій в економіці, управлінні та особливо в кредитно-банківській діяльності зумовило виникнення нового класу злочинів - таких, які скоюють за допомогою комп'ютерних технологій, або "комп'ютерних" злочинів, тобто виникла нова форма злочинності - кіберзлочинність. Нині проблема боротьби з цією новою формою злочинності є актуальною через стрімкий розвиток комп'ютерних технологій на основі використання глобальної інформаційної мережі Інтернет.

Злочини, що вчиняються за допомогою комп'ютерних технологій, набули статусу міжнародних. Кіберзлочини зумовлені створенням міжнародних інформаційних систем, зокрема таких, як Інтернет, що об'єднує обчислювальні

центри й системи більш як 80 країн і забезпечує обмін даними між різними джерелами й користувачами. В розвинених країнах цей вид злочинності завдає величезних збитків власникам і користувачам автоматизованих систем, змушує їх витрачати великі кошти на розроблення та впровадження програмних, технічних та інших засобів захисту від несанкціонованого доступу до інформації, її перекручування чи знищення.

Ще в 90-ті роки у Сполучених Штатах Америки комп'ютерні шахрайства щорічно спричиняли збитки на суму понад $10 млрд. У Великій Британії, де комп'ютерна злочинність на той час зросла в 4 рази, за оцінками Конфедерації британських промисловців, щорічні збитки сягали 5 млрд. фунтів стерлінгів. Ризик стати потерпілим від таких злочинів набрав значних обсягів, що змусило страхову агенцію Ллойда у Лондоні розпочати страхування від комп'ютерних злочинів. Такий тип страхування також був введений у Німеччині.

За оцінками вітчизняних і зарубіжних фахівців, розв'язання проблем розслідування злочинів цього виду є складним завданням для правоохоронних органів як у нашій країні, так і за рубежем. Наприклад, у Великій Британії із 270 установлених злочинів з використанням засобів комп'ютерної техніки за останні 5 років було розкрито тільки 6; у ФРН із 2777 випадків розкрито тільки 170, тоді як інші 2607 кримінальних справ було припинено за різними обставинами; у Франції із зареєстрованих 70 злочинів розкрито лише 10; у США за 200 злочинів до кримінальної відповідальності було притягнуто лише 6 осіб. Наведені дані красномовно свідчать про рівень складності розслідування злочинів категорії, що розглядається.

Американські фахівці з проблем комп'ютерної злочинності підкреслюють, що реальні масштаби цієї проблеми нікому невідомі, а розміри збитків вимірюються мільйонами доларів США і продовжують зростати. Офіційна статистика США свідчить про те, що тільки 5% "комп'ютерних" злочинів стають відомими правоохоронним органам і близько 20% з них піддаються судовому переслідуванню.

Останнім часом і в Україні спостерігається стрімке зростання злочинів, пов'язаних із втручанням у роботу автоматизованих систем. Як правило, втручання це здійснюється з метою вчинення інших, більш тяжких злочинів:

- розкрадання майна;
- вимагання майна під погрозою знищення;
- спотворення інформації, що опрацьовується чи зберігається в автоматизованих системах;
- несанкціоноване ознайомлення з такою інформацією;
- викрадення конфіденційної інформації;
- знищення конфіденційної інформації тощо.

Висока латентність таких злочинів пояснюється насамперед тим, що державні й комерційні структури, які зазнали нападу, особливо в банківській діяльності, не дуже вірять у можливості розкриття таких злочинів правоохоронними органами. Однією з основних причин високої латентності та низького рівня розкриття злочинів у сфері комп'ютерної інформації є проблеми,

що виникають перед правоохоронними органами на стадії порушення такої кримінальної справи внаслідок складності кваліфікації злочинних діянь та особливостей проведення окремих слідчих дій.

Згідно з чинним законодавством, виділяють кілька основних обставин, які потребують обов'язкового визначення у кримінальних справах такої категорії, а саме:

- об'єкт та предмет злочину;
- об'єктивна та суб'єктивна сторони злочину;
- об'єктивна та суб'єктивна сторони самого суб'єкта злочину.

Відповідно до Закону України "Про захист інформації в автоматизованих системах", об'єктом злочину є правові відносини щодо захисту інформації в автоматизованих системах.

Згідно з Кримінальним Кодексом України, предметом злочину виступають:

- автоматизовані системи (АС) - системи, що здійснюють автоматизоване опрацювання бази даних і до складу яких входять технічні засоби: засоби обчислювальної техніки і зв'язку; методи і процедури; програмне забезпечення; носії інформації - фізичні об'єкти, поля і сигнали, хімічні середовища, накопичувані даних в інформаційних системах;
- інформація, яка використовується в АС,- сукупність усіх даних і програм, використовуваних в АС незалежно від засобу їх фізичного та логічного подання;
- програмні й технічні засоби, призначені для незаконного проникнення в автоматизовані системи.

При розповсюдженні програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи, намір є лише прямим, оскільки суб'єктивну сторону цього злочину визначає психічне ставлення злочинця до вчинюваних ним дій. Мотиви і мета вчинення злочинів можуть бути різними і свідчити про те, що робота автоматизованої системи порушена, наприклад, для вчинення інших злочинів.

Згідно з Кримінальним кодексом України, під втручанням у роботу АС розуміють будь-які зловмисні дії, що впливають на опрацювання інформації в АС, тобто на всю сукупність операцій:

- зберігання;
- введення;
- записування;
- перетворення;
- зчитування;
- зберігання;
- знищення;
- реєстрація.

Ці операції здійснюються за допомогою технічних і програмних засобів, зокрема, обміну через канали передавання даних. При втручанні в роботу АС

порушується її робота, а отже, спотворюється процес опрацювання інформації, наслідком чого є перекручування або знищення самої інформації чи її носіїв.

Під знищенням інформації розуміють її втрату, коли вона в АС перестає існувати для власників чи користувачів або блокується. Розрізняють внутрішнє і зовнішнє втручання в роботу АС, тобто у формі впливу на канали передачі інформації між технічними засобами її опрацювання і зберігання всередині АС та між окремими АС, внаслідок чого інформація, що передається для опрацювання, знищується або перекручується.

Перекручення інформації це зміна її змісту, порушення її цілісності, в тому числі й часткове знищення.

3.7. ЗАХИСТ ІНФОРМАЦІЇ СТОСОВНО ГРОМАДЯНИНА

Розвиток сучасного суспільства неможливий без інформаційного забезпечення всіх сфер діяльності людини, зокрема, без надійного захисту інформації. Особливої гостроти ця проблема набуває у зв'язку з масовою комп'ютеризацією, об'єднанням ЕОМ у комп'ютерні мережі та використанням Інтернет. Тому досить складним є завдання вибору з величезного масиву сучасних методів і засобів захисту інформації таких, що найбільше відповідають конкретним умовам діяльності та гарантують достатній рівень безпеки.

Різні технології захисту мають багато спільних ознак у розробленні та використанні, зокрема:

- засоби захисту операційної системи;
- мережеві екрани;
- криптографічні системи;
- системи визначення атак;
- системи визначення реакцій на атаку;
- системи моніторингу інформаційної безпеки.

Вивчення цих технологій ґрунтується на солідній теоретичній базі й аналізі вітчизняних та закордонних нормативних документів у галузі захисту інформації. Для кращого розуміння технологій захисту передбачено вивчення методики і засобів проведення атак на комп'ютерні системи та мережі.

Тому підприємства не тільки повинні мати якнайкращу техніку, володіти новітніми технологіями, а й мати спеціалістів із захисту інформації, які б відповідали таким вимогам:

- вміли ефективно організовувати захист інформації в комп'ютерних системах і мережах;
- володіли сучасними технологіями захисту інформації;
- мали достатню кваліфікацію для проектування й розроблення нових засобів і методів захисту.

Важливим чинником є також захист персоналу компанії, інформації про її працівників.

Згідно зі ст. 3 Конституції України, людина, її життя і здоров'я, честь і

гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Виходячи з положення Конституції, слід підкреслити, що чим більше значення проголошені ідеї мають для суспільства, тим важче вони втілюються в життя, тим довшим є їх шлях до конкретної особи.

Проблеми утвердження пріоритету людини в економічній, політичній і духовній сферах тісно пов'язані з нормальним обігом інформації та оптимізацією соціального управління. Перехід до ринкових відносин, формування правової держави, демократичних традицій, інститутів і норм - усе це є засобом досягнення мети, яка полягає у створенні сприятливих умов розвитку для окремої особи, а отже, і суспільства загалом. Економічна, політична і судова реформи потрібні для ефективного взаємовигідного соціального управління і повноцінного обміну інформацією, що забезпечує свободу і гідну життєдіяльність людини.

На підприємствах розвинених країн функціонує єдина служба безпеки, яка підпорядковується одному з керівників компанії. У складі цієї служби працюють підрозділи чи окремі спеціалісти (залежно від розмірів підприємства) за такими головними групами функцій:

- організація систем управління людськими ресурсами;
- планування чисельності персоналу;
- аналіз і регулювання умов праці;
- гарантування безпеки праці;
- організація праці;
- оцінювання та атестація персоналу;
- підвищення кваліфікації;
- захист інформаційних технологій;
- оплата праці;
- соціальні проблеми персоналу;
- захист персоналу;
- підбір і мотивація персоналу;
- захист інформації компанії;
- корпоративна розвідка;
- контррозвідка;
- організація взаємин між адміністрацією, профспілкою, працівниками.

Правовою основою систем управління людськими ресурсами є угоди і договори між суб'єктами соціально-трудових відносин. На республіканському рівні укладають генеральні угоди між представниками професійних спілок, роботодавців та урядом України; галузеві угоди - між галузевими профспілками, об'єднанням роботодавців та представниками держави.

На підприємстві основою регулювання соціально-трудових відносин є колективний договір на строк від одного до трьох років між роботодавцем і представниками найманого персоналу. У ньому фіксують взаємні обов'язки з основних питань умов та оплати праці:

- наймання;
- перекваліфікація;

- звільнення;
- гарантування безпеки і охорона здоров'я;
- тривалість робочого часу і часу відпочинку;
- форми, системи і методи оплати праці та умови функціонування;
- форми вирішення трудових спорів;
- форми надання послуг підприємства своїм працівникам: їда; транспортні послуги; лікування тощо;
- соціальні гарантії у разі погіршенні економічної кон'юнктури;
- компенсації у разі нещасних випадків;
- відповідальність за розголошення комерційної таємниці;
- певні зобов'язання щодо специфіки діяльності фірми. Економічними та політико-правовими формами, які створюють оптимальні умови для функціонування суспільства і прогресивного розвитку його інформаційного наповнення, є ринок, демократія і правова держава.

У суспільстві інформація є основою для взаємодії та дієвого функціонування економіки, політики, права, запорукою прогресу:

- ринкові відносини, що склалися на засадах самоорганізації, не можуть існувати без повноцінного інформаційного середовища, без нових інформаційних технологій, без усвідомлення того, що людина має саме те, чого їй не вистачає;
- демократичні інститути і норми не можуть реально існувати без інформаційної свободи та якісно нових структур у сфері комунікації, які допомагають приймати рішення;
- особистість, громадянське суспільство не можуть впливати на державу без концепції найбільш повного забезпечення прав людини, і насамперед права на інформацію, яке дає змогу наблизитися до аксіоми "управляє світом той, хто володіє інформацією".

Згідно зі ст. 200 Цивільного кодексу України:

- суб'єкт відносин у сфері інформації може вимагати усунення порушень його права та відшкодування майнової і моральної шкоди, завданої такими правопорушеннями;
- порядок використання інформації та захисту права на неї встановлюється законом.

Будь-яке монопольне розпорядження інформацією згодом впливає і на саму державу, заводить суспільство у глухий кут в економічній, політичній і правовій сферах. На перший погляд, дозування інформації з боку держави є вигідним для неї, але це тільки здається. Коли держава інформує своїх громадян "дозовано", неповно і неправдиво, то й зворотна інформація буде такою самою, а це унеможливить прийняття адекватних рішень. Досвід нашого суспільства переконливо це підтверджує. Обмеження інформації на міжнародній арені і всередині країни (надмірна засекреченість, брак достовірної статистики і гласності, надання на різних рівнях "вигідної"" інформації тощо) уже спричинилося до багатьох помилок. Так, у колишньому СРСР були закритими 70% нормативних актів, які стосуються прав і свобод громадян, внаслідок чого:

- людина була позбавлена можливості повною мірою використовувати свої конституційні та інші права, свободи;
- ускладнювалася боротьба зі свавіллям;
- створювалися перепони проти оскарження неправомірних дій державних органів і посадових осіб.

Це обмежувало правовий статус особистості, ставило її у залежність від державного апарату, чиновників, бюрократії.

На жаль, і нині в роботі міністерств, відомств, судів помітні намагання утаємничити свою діяльність, відсторонитись від громадян і громадськості. Створюються спеціальні структури "із захисту інформації"", ускладнюється доступ до її джерел. Використовуються заборонені або незаконні грифи, які обмежують доступ до інформації, зокрема: "Не для друку", "Опублікуванню не підлягає" та "Для службового користування". Тим самим порушується одне із найважливіших прав громадян - право на інформацію. При цьому ігнорується суттєвий принцип демократії-принцип відкритості і публічності влади. Для нашого суспільства він має особливе значення, оскільки давня традиція недовіри до влади може бути подоланою лише із запровадженням загальнодоступності інформації про діяльність влади.

Одним із ефективних засобів підвищення поваги до особистості є правова охорона особистого життя людини від неправомірних втручань. Відповідні правові норми, виконуючи свою ідеологічну функцію, виховують у людей вміння цінувати своє життя та поважати й не втручатися в особисте життя інших. Особливу роль у правовій охороні особистого життя відіграють норми Цивільного кодексу України від 16.01.2003 р., в яких дістали своє розгорнуте закріплення особисті немайнові права фізичних осіб, спрямовані на охорону особистого життя. У зв'язку з новизною цих норм та недостатністю практики їх застосування виникає потреба у їх науково-теоретичному розробленні.

Проблема цивільно-правової охорони особистого життя не є новою для юридичної науки, ґрунтовні її дослідження проводилися ще за радянських часів, а нині їх результати дещо втратили свою актуальність і значення. У сучасних наукових дослідженнях ця проблема розробляється або вужче (лише окремі її аспекти, зокрема, таємниці особистого життя), або ширше - в контексті загального дослідження особистих немайнових прав і компенсації моральної шкоди, завданої їх порушенням.

У сучасній науковій літературі немає праць, у яких би грунтовно й комплексно висвітлювалися проблеми цивільно-правового регулювання особистих немайнових відносин, що складаються з приводу особистого життя.

Згідно зі ст. 30 1 Цивільного кодексу:

- фізична особа має право на особисте життя;
- сама визначає своє особисте життя і можливість ознайомлення з ним інших осіб;
- має право на збереження у таємниці обставин свого особистого життя;
- обставини її особистого життя можуть бути розголошені іншими особами лише за умови, що вони містять ознаки правопорушення, що

підтверджено рішенням суду, а також за її згодою.

Згідно зі ст. 302 Цивільного кодексу фізична особа має право вільно збирати, зберігати, використовувати і поширювати інформацію. Збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Фізична особа, яка поширює інформацію, зобов'язана переконатися в її достовірності. Фізична особа, яка поширює інформацію, отриману з офіційних джерел (інформація органів державної влади, органів місцевого самоврядування, звіти, стенограми тощо), не зобов'язана перевіряти її достовірність та не несе відповідальності в разі її спростування. Фізична особа, яка поширює інформацію, отриману з офіційних джерел, зобов'язана робити посилання на таке джерело.

Особисте життя - це особлива частина приватної сфери людської життєдіяльності, яка полягає в різних відносинах, стосунках, явищах, подіях і т.ін., що не мають публічного значення, визначається й регулюється самою особою на основі соціальних умов, гарантується та охороняється правом від неправомірних втручань.

Сімейне життя - це сфера особистого життя осіб, що утворюють сім'ю, в якій задовольняються їхні спільні приватні інтереси.

Особисте життя є особистим немайновим благом, що охороняється правом. Зв'язок особистого життя і права треба визначати через поняття правової охорони, адже право регулює відносини, що складаються не в особистому житті, а з приводу особистого життя, і таке регулювання не зводиться лише до захисту цього блага. Аналіз наявних у літературі визначень поняття цивільно-правової охорони особистого життя вказує на їх невідповідність нормам чинного законодавства. Виходячи з цього В.І. Бобрик запропоновано власне визначення цивільно-правової охорони особистого життя як системи заходів, передбачених цивільним законодавством, що спрямовані на забезпечення неприпустимості неправомірного втручання у визначену людиною сферу особистого життя, окрім випадків, передбачених законом.

Правомірні втручання - це активні дії з дозволу фізичної особи або у випадках обмеження відповідних цивільних прав, передбачених законом. Втручання може здійснюватися лише за згодою особи, яка може бути надана конкретній особі, визначеному або невизначеному колу осіб. Обмеження суб'єктивних прав на охорону особистого життя встановлюються нормами переважно публічних галузей права. Щодо приватноправових обмежень має бути законодавчо закріплений гнучкий механізм визначення правомірності втручання, основою якого є зіставлення ознак втручання з такими критеріями:

- метою втручання - захист публічного інтересу або інформування громадськості про обставини, що становлять значний суспільний інтерес;
- способом втручання - завідомо законний;
- суб'єктом втручання:

- працівник державного органу;
- журналіст і засіб масової інформації;
- контролюючі органи;
- особою потерпілого - залежно від статусу дещо обмежуються права так званих "публічних", "квазіпублічних" та "відносно публічних" осіб;
- підставою втручання - у законі завжди має бути вказана ситуація або обставини, за яких дозволяється стороннє втручання в особисте життя.

Особливості особистих немайнових прав, спрямованих на охорону особистого життя, а також способів неправомірних втручань в особисте життя і характер завданої ними шкоди зумовлюють вибір уповноваженою особою форми захисту, яка може бути судовою, третейською, адміністративною або самозахистом. У разі судового захисту цих прав можуть бути застосовані такі способи:

- визнання права;
- відшкодування майнової шкоди;
- відшкодування моральної (немайнової) шкоди;
- поновлення порушеного права;
- заборона поширення інформації, якою порушуються особисті немайнові права.

Для того щоб кваліфіковано захищати свої права дозволеними законодавством способами, засобами, методами, їх насамперед потрібно знати, а також знати правові механізми їх здійснення.

Розглядаючи проблему в когнітивному (пізнавальному) аспекті, слід зазначити, що в публічному праві України існує багато правових шляхів захисту, в тому числі захисту інформації в автоматизованих системах, але відомості про них розпорошені у значній кількості нормативних актів. Причина цього в галузевому підході до проблем захисту прав у юриспруденції, що поряд з позитивними має й негативні аспекти:

- відсутність комплексності захисту;
- різне тлумачення одних і тих же понять у різних галузях права, зокрема щодо захисту законних прав в інформаційних відносинах від протиправних посягань, вирішення колізій.

Актуальність для практики питань захисту прав не забороненими законодавством засобами змушує правознавство (як науку) проводити комплексні й системні наукові дослідження, формувати комплексну наукову дисципліну - "Юридичну деліктологію" - науку про правопорушення та її методології. У ній має бути комплексно відображена й така інституція, як захист інформації в автоматизованих системах, у тому числі визначення й характеристика діянь, які є злочинами.

У зв'язку з цим виникає потреба в застосуванні у правознавстві здобутків таких наук, як інформатика й теорія систем. Зокрема, в теорії систем важливим є з'ясування сутності правознавства як великої, складної системи, що має характер гіперсистеми - взаємопов'язаної множини підсистем першого, другого та наступних порядків.

Якщо стосовно об'єкта суспільних відносин, який визначає їх об'єктивну сутність, немає норм у зазначених галузях права, то такі системи визначаються як міжгалузеві інститути права.

СПИСОК ЛІТЕРАТУРИ

Базова

1. Андрушків Б.М. Економічна та майнова безпека підприємства та підприємництва. Антирейдерство / Андрушків Б.М., Малюта Л.Я.та ін. – Тернопіль: Вид.Терно-граф, 2008. – 424с.

2. Андрушків Б.М. Основи менеджменту: методологічні положення та прикладні механізми / Б. М. Андрушків, О. Є. Кузьмін. – Тернопіль : «Лілея», 1997. – 292 с.

3. Белов Г.В. Экологический менеджмент предприятия: учеб.пособие / Г. В. Белов. – М. : Логос, 2006. – 240 с.

4. Білорус О.Г. Глобалізація і безпека розвитку бізнесу: [монографія] / Білорус О.Г. – К., 2003. – 733 с.

5. Бойко М. Д. Правовий самозахист: [навч. посібник] / Бойко М. Д. – К.: Атіка, 2006. – 323с.

6. Дерягина С.Е. Эколгический менеджмент на предприятии / С. Е. Дерягина, О. В. Астафьева, М. Н. Струкова, Л. В. Струкова. – Екатеринбург : ИПЭ УрО РАН – УГТУ УПИ, 2007. – 146 с.

7. ДСТУ ISO 14001-97. Системи управління навколишнім середовищем. Склад та опис елементів і настанови щодо їх застосування. – К. : Держстандарт, 1998.

8. ДСТУ ISO 14004-97. Системи управління навколишнім середовищем. Загальні настанови щодо принципів управління, систем та засобів забезпечення.

9. ДСТУ ISO 14010-97. Настанови щодо екологічного аудиту. Загальні принципи.

10. ДСТУ ISO 14011-97. Настанови щодо екологічного аудиту. Процедури аудиту. Аудит систем управління навколишнім середовищем.

11. ДСТУ ISO 14012-97. Настанови щодо екологічного аудиту. Кваліфікаційні вимоги до аудиторів з екології. Державні стандарти України (Вид. офіц.). – 1997. – 227 с.

12. ДСТУ ІСО 14001-97. Системи управління навколишнім середовищем. Склад та опис елементів і настанови щодо їх застосування. – К. : Держстандарт, 1998.

13. Екологічне підприємництво: Навч. пос. / В.Я. Шевчук, Ю. М. Саталкін. – К. : Мета, 2001. – 191 с.

14. Екологічний менеджмент: Навч. посіб. / За ред. В.Ф. Семенова, О. Л. Михайлюк. – К. : Знання, 2006. – 366 с.

15. Екологічний менеджмент: Зб. наук. пр. / За ред. В.А. Гайченка. – К. : МАУП, 2006. – 266 с.

16. Економічна безпека підприємств, організацій та установ : навч. посібник [для студ. вищих навч. закладів] / [В.Л. Ортинський, І.С. Керницький, З.Б. Живко та ін.]. К. : Правова єдність, 2009. 544 с.

17. Закон України «Про охорону навколишнього природного середовища» (із змін. та допов.) від 25 червня 1991 р. № 1264-XII.

18. Зеркалов Д. Рейдер. Международная и национальная безопасность / Зеркалов Д. – К., 2007. – 312с.

19. Кирич Н.Б. Екологічний менеджмент: еколого-економічні засади раціонального природокористування: навч.пос. / Н.Б. Кирич, І.А. Кінаш, О. Б. Погайдак. – Тернопіль : ТзОВ «Терно-граф», 2011. – 268 с.

20. Кобецька Н.Р. Екологічне право України: Навч. посіб. – К. : Юрінком Інтер, 2007. – 352 с.

21. Кожушко Л.Ф. Екологічний менеджмент: підручник / Л.Ф. Кожушко, П. М. Скрипчук. – К. : «Академія», 2007. – с. 432.

22. Мельник Л.М. Конспект лекцій з дисципліни «Екологічне управління інноваційним розвитком підприємства» для студентів спеціальності «Управління інноваційною діяльністю» усіх форм навчання / Л.М. Мельник. – Тернопіль : ПП Паляниця В.А., 2015. – 74 с.

23. Малюта Л.Я. Методичні вказівки для практичних занять, виконання завдань самостійної та індивідуальної роботи з дисципліни «Економічна та майнова безпека бізнесу» / Л.Я Малюта, О.А. Сороківська. – Тернопіль: ТНТУ, 2011. – 66 с.

24. Сороківська О.А. Економічна безпека. Конспект лекцій з курсу. / О.А.Сороківська. – Тернопіль: ТДТУ, 2008. – 155с.

25. Туник И. Антирейдер: пособие по противодействию корпоративным захватам/ Туник И., Поляков В. – М., 2007. – 298с.

26. Шапоренко О.І. Екологічний менеджмент / О.І. Шапоренко. – Донецьк : вид-во Норд-Прес, 2004. – 312 с.

27. Шлемко В. Економічна безпека України: сутність і напрями забезпечення / Шлемко В. Бінько І. – К., 2012. – 144 с.

28. Шерстюк Р. П. Інноваційні шляхи активізації природоохоронного провайдингу в умовах підприємства (Європейські акценти) / Р. П. Шерстюк, Н. Б. Кирич, І. Б. Гевко. та ін.; за ред. проф. Б. М. Андрушківа. – Тернопіль: Терногpаф. – 2011. – 576 с.

Допоміжна

1. Андрушків Б.М. Основи організації підприємницької діяльності або абетка для підприємця: навчальний посібник [реком. Міністерством освіти і науки України] / Б.М. Андрушків, Ю.Я. Вовк, В.В. Гецько, П.Д. Дудкін, Н.Б. Кирич, О.Б. Погайдак, І.І. Стойко. – Тернопіль : Вид. ТНТУ. – 2010. – 300 с. – (лист МОН №1.4/18-Г-783 від 25.03.10р.).

2. Економіка підприємства: [підручник] / За загальною редакцією С.Ф. Покропивного. – К.:КНЕУ, 2000. – 435 с.

3. Економіка підприємства: [підручник] / За загальною редакцією Й.М. Петровича. – Львів: «Новий Світ-2000», 2004. – 680 с.

4. Козаченко А.В. Экономическая безопасность предприятия / Козаченко А.В., Пономарев В.П., Ляшенко А.Н. – К., 2003. – 280 с.

5. Концепція економічної безпеки України. Інститут економічного прогнозування / Керівник проекту В.М. Геєць. – К., 1999. – 56 с.

6. Кузьмін О.Є. Основи менеджменту / Кузьмін О.Є., Мельник О.Г.. – К., 2003. – 414 с.
7. Лук'янихін В.О. Екологічний менеджмент у системі управління збалансованим розвитком: Монографія. – Суми : ВТД «Університет. кн.», 2002. – 314 с.
8. Мунтіян В.І. Економічна безпека України / Мунтіян В.І. – К., 2004. – 462с.
9. Олейник К.А. Экологические риски в предпринимательской деятельности (вопросы методологии). – М. : Анкил, 2002. – 208 с.
10. Пастернак-Транушенко Г. Економічна безпека держави / Пастернак-Транушенко Г. – К., 2002. – 302 с.
11. Підприємницьке право: [підручник] / За заг. ред. доц. Шишки Р. Б. – Х.: Вид-во Ун-ту внутр. справ. «Еспада», 2000. – 341 с.
12. Потравный И.М., Семенченко П. М. Формирование экологически ориентированной предпринимательской деятельности и оценка эффективности природоохранных мероприятий. – Мариуполь : Приазов. гос. техн. ун-т, 1999. – 83 с.
13. Саніахметова Н. О. Правовий захист підприємництва в Україні: [навч.посібник] / Саніахметова Н. О. – К.: Юрінком Інтер, 1999. – 290 с.
14. Экология, охрана природы, экологическая безопасность / Под ред. А.Т. Никитина. – М. : Новь, 2000. – 648 с.
15. Lambert D. La defence de l'economie: la conjugaison des efforts de l'Etat, de l'enterprise et d'individu // Strategigue. – 1990. – №2. – P. 83-98.
16. Nolan R.L. Managing the Computer Resource: A stage Hypothesis, Communications of ACM. – 2003. – №16. – P.399-405.

Інформаційні ресурси

1. Всеукраїнська екологічна ліга – http://www.ecoleague.net
2. Екоклуб «Зелена хвиля» – http://ecoclub.kiev.ua
3. Екологічні новини – http://greenhome.com.ua
4. Еколого-гуманітарне об'єднання «Зелений світ» – http://www.greenworld.org.ua
5. Український екологічний портал – http://www.ecoport.org.ua
6. Экологический портал – http://portaleco.ru
7. Міжнародний, суспільно-політичний тижневик «Дзеркало тижня» – http://dt.ua
8. http://www.business-guide.com.ua/enterprises. – список найуспішніших підприємств, які ефективно використовують функції та методи менеджменту.
9. http://www.ternstat.tim.net.ua. – статистичні дані підприємств усіх галузей економіки, які діють на теренах Тернопільської області.
10. http://www.ukrstat.gov.ua. – Офіційний сайт Комітету статистики України.
11. Наукова бібліотека ім.Вернадського - http://www.nbuv.gov.ua.
12. http://www.lib.com.ua - Електронна бібліотека.

13. http://www.nauka-osvita. com.ua - Економіка. Проблеми теорії та практики.
14. http://www.pro-invest.com - Управління підприємством.
15. http://www.ptpu.ru - Проблеми теорії та практики управління.
16. http://www.ifc.org - Сайт Міжнародної Фінансової Корпорації.