З розвитком комп'ютерної техніки і створенням комп'ютерних мереж як глобального масштабу, так і різних локальних мереж (наприклад, банківських) постає проблема захисту джерел інформації в цих мережах, бо будь-яке несанкціоноване вторгнення, скажімо, в банківську мережу може призвести до втрати важливої інформації, до втрати її секретності та, як наслідок, використання цієї інформації з якоюсь корисливою метою.

Найбільш поширені форми промислового шпигунства:

крадіжка інформаційного носія з даними, що являють комерційну або службову таємницю;

впровадження шпигуна, який мав би можливість доступу до конфіденційної інформації;

підкуп людини, що володіє такими даними;

прослуховування телефонів, перегляд кореспонденції, електронних листів тощо.

Так, наприклад німецькі підприємства втрачають 20 млрд щороку через промислове шпигунство. Щорічні збитки німецьких підприємств від промислового шпигунства складають щонайменше 20 мільярдів євро, повідомляє Deutschlandradio з посиланням на голову Комітету з економічної безпеки Бертольда Штоппелькампа (Berthold Stoppelkamp). Найчастішим об'єктом шпигунства є дослідження у галузі екологічно чистих технологій, особливо розроблення електроприводів і високоємних акумуляторів. Задіяні в цих дослідженнях учені, інженери й менеджери змушені приділяти підвищену увагу боротьбі з інсайдерськими витоками інформації [1].

Таким чином, промислове шпигунство, як інші види загроз, є однією із сучасних загроз існуванню підприємств, яка виникає і реалізується на основі недосконалого законодавства та недієздатності ринкових інституцій.

Для формування оптимальної сучасної системи економічної безпеки як на рівні підприємства, так і держави необхідно не тільки усвідомити необхідність її створення, але й здійснювати низку заходів на постійній основі, а саме: формування інформаційного масиву про небезпеки та загрози, які є новими для фахівців і керівників підприємства.

ЛІТЕРАТУРА:

1. Бабій Б.В. Промислове шпигунство як негативний фактор впливу на функціонування підприємства [Електронний ресурс] / Б.В. Бабій. – Режим доступу: http://www.economy-confer.com.ua/full-article/1041/

2. Банк Р.О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект [Електронний ресурс] / Р.О. Банк. – Режим доступу: http://ippi.org.ua/sites/default/files/17.pdf

3. Варналій В.С. Рейдерство в Україні: передумови та шляхи подолання [Електронний ресурс] / В.С. Варналій. – Режим доступу: http://www.nbuv.gov.ua/old_jrn/soc_gum/sp/2007_2/17.pdf.

4. Тивончук І.О. Особливості рейдерства в Україні [Електронний ресурс] / І.О. Тивончук, Г.Я. Глинська. – Режим доступу: http://vlp.com.ua/files/22_23.pdf

5. Гаршов І. Сутність сучасного тероризму і його основні характеристики [Елекронний ресурс] / І. Гаршов. – Режим доступу: http://personal.in.ua/article.php?ida=21

6. Загроза нинішньому світові – кібертероризм [Елекронний ресурс]. – Режим доступу: http://wartime.org.ua/3581-zagroza-ninshnomu-svtov-kberterorizm.html

7. Захист від фішинг-махінацій за допомогою Office [Електронний ресурс]. – Режим доступу: https://support.office.com/uk-ua/article

8. Довгань О.В. Кібертероризм як загроза інформаційному суверенітету держави [Електронний ресурс] / О.В. Довгань. – Режим доступу: http://www.nbuv.gov.ua/old_jrn/soc_gum/iblsd/2011_3/_private/7dodoas.pdf

9. Грінмейл як частина сучасних корпоративних відносин [Електронний ресурс]. – Режим доступу: http://www.uris-c.com.ua/2010/06/21/

10. Живко З.Б. Грінмейл як особливий вид поглинання компаній [Електронний ресурс] / З.Б. Живко, П.О. Муж, В.М. Мельникович. – Режим доступу: *irbis-nbuv.gov.ua/.../cgiirbis_64.exe?.*

11. Ісар І.В. Рейдерство в Україні: причини виникнення та шляхи подолання [Електронний ресурс] / І.В. Ісар. – Режим доступу: http://www.rusnauka.com/2_ANR_2010/Pravo/12_57137.doc.htm

12. Сучасні загрози фінансово-економічній безпеці підприємств та шляхи їх зменшення [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/17910211/finansi/suchasni_zagrozi_finansovo-ekonomichniy_bezpetsi_pidpriyemstv_shlyahi_zmenshennya

13. Ткачук Т. Характерні особливості конкурентної розвідки та промислового шпигунства [Електронний ресурс] / Т. Ткачук. – Режим доступу: http://www.personal.in.ua/article.php?ida=451

14. Шабельникова Н.А. Информационный терроризм: основные проявления и возможные последствия / Н.А. Шабельникова // Информатизация и информационная безопасность правоохранительных органов. Труды XV международной научной конференции, 23 – 24 мая 2006 г. – М.: Изд-во Акад. управления МВД России, 2006. – С. 167 – 171.

15. Карт-бланш українських кардерів [Електронний ресурс]. – Режим доступу: http://cripo.com.ua/print.php?sect_id=1&aid=16686

4.5. Організаційно-функціональний механізм упровадження служби економічної безпеки підприємства в умовах нестабільного середовища

У сучасних нестабільних умовах ринкового господарювання важливого значення набуває економічна безпека всіх видів діяльності підприємства для його стабільного функціонування та розвитку, запобігання внутрішнім і зовнішнім негативним загрозам.

Необхідність упровадження служби економічної безпеки підприємства зумовлюється об’єктивно наявним завданням забезпечення стабільності

функціонування та досягнення головних цілей своєї діяльності. Перед кожним підприємством виникає проблема власної економічної безпеки і не лише під час кризи, але й під час поточної діяльності підприємства в умовах економічної стабільності.

Рівень економічної безпеки підприємства повинен залежати від того, наскільки ефективно її керівництво та фахівці функціональних служб апарату управління підприємством будуть спроможні уникнути можливих загроз і ліквідувати шкідливі наслідки негативного впливу зовнішнього й внутрішнього середовища [4, с. 78]. Варто систематизувати джерела негативних впливів на економічну безпеку підприємства: несвідомі чи свідомі дії посадових осіб, суб'єктів господарювання та підприємств-конкурентів; певний збіг об'єктивних обставин: стан фінансової кон'юнктури на внутрішніх і зовнішніх ринках, наукові відкриття та технологічні розроблення, форс-мажорні обставини тощо.

Об'єктивними доцільно вважати такі негативні впливи, які виникають не з волі керівництва підприємства або його окремих працівників. Суб'єктивні впливи мають місце внаслідок неефективної роботи підприємства в цілому чи окремих його працівників, передусім керівників і функціональних керівників підрозділів підприємства.

Головна мета створення служби економічної безпеки підприємства - гарантування стабільного та максимально ефективного функціонування в реальних умовах господарювання й забезпечення високого потенціалу розвитку підприємства в перспективі [6, с. 152].

Залежно від функціональної спрямованості цілі служби економічної безпеки підприємства можуть бути такими:

забезпечення високої фінансової ефективності роботи, фінансової стійкості, платоспроможності та незалежності підприємства від внутрішніх і зовнішніх факторів впливу;

досягнення належної конкурентоспроможності технічного потенціалу підприємства завдяки впровадженню інновацій;

досягнення ефективності управління підприємством шляхом реструктуризації діючої структури в ефективну органічну (гнучку) структуру управління підприємством;

досягнення високого рівня професійної кваліфікації та інтелектуального потенціалу управлінського і виробничого персоналу;

зменшення руйнівного впливу результатів виробничо-господарської діяльності на стан екології навколишнього середовища;

підвищення якісної правової захищеності всіх аспектів діяльності підприємства;

гарантування захисту інформаційного поля, комерційної таємниці й досягнення необхідного рівня інформаційного забезпечення роботи всіх виробничих підрозділів і функціональних відділів апарату управління підприємства;

ефективна організація безпеки персоналу, охорона капіталу та майна і комерційних інтересів підприємства.

Головна мета та функціональні цілі підприємства зумовлюють формування необхідних структуроутворюючих елементів і побудову організаційної структури управління служби економічної безпеки (рис. 4.8).

Рис. 4.8. Функціональні складові служби економічної безпеки підприємства

Організаційними заходами щодо створення служби економічної безпеки підприємства повинні бути такі дії керівництва:

формування необхідних ресурсів (фінансових, інтелектуальних (персоналу), матеріальних, інформаційних);

стратегічне і тактичне планування фінансово-господарської діяльності підприємства в цілому;

стратегічне прогнозування та тактичне планування економічної безпеки за її функціональними складовими;

оптимізація діяльності щодо попередження і передбачення можливих загроз економічній безпеці, виявлення, аналіз та оцінювання реальних загроз економічній безпеці та прийняття рішення щодо їх усунення;

оперативне управління фінансово-господарською діяльністю підприємства в цілому;

здійснення функціонального аналізу рівня економічної безпеки підприємства;

загальне оцінювання досягнутого рівня економічної безпеки підприємства.

Варто зазначити, що лише при реалізації керівництвом зазначених заходів можна буде досягти належного рівня економічної безпеки підприємства.

При створенні служби економічної безпеки керівництву підприємства необхідно оцінити рівень її економічної безпеки. Із цією метою керівництву підприємства доцільно скористатися методологію оцінювання рівня економічної безпеки підприємства, яку оцінюють на підставі визначення сукупного критерію через зважування й підсумовування окремих функціональних критеріїв, які обчислюються за допомогою порівняння можливої величини шкоди підприємству та ефективності заходів щодо її запобігання.

Сукупний критерій економічної безпеки підприємства ($k_{себ}$) рекомендуємо розрахувати, користуючись формулою

$$k_{себ} = \sum_{i=1}^{n} k_i d_i, \qquad (4.2)$$

де k_i – величина окремого (поодинокого) критерію за і-ю функціональною складовою;

d_i – питома вага значущості і-ї функціональної складової;

n – кількість функціональних складових служби економічної безпеки.

Оцінювання рівня економічної безпеки підприємства здійснюється порівнюванням розрахункових значень $k_{себ}$ із реальними величинами цього показника по підприємству, а також по аналогічних підприємствах відповідних галузей діяльності області чи району [3, с. 78]. Після розрахунку впливу функціональних складових на зміну $k_{себ}$ повинен здійснюватися функціональний аналіз заходів за окремими складовими стосовно організації необхідного рівня економічної безпеки завдяки послідовним етапам (рис. 4.9).

Рис. 4.9. Процес проведення функціонального аналізу заходів за окремими складовими для забезпечення необхідного рівня економічної безпеки підприємства

Таким чином, оцінка ефективності діяльності функціональних структурних підрозділів підприємства з використанням даних про витрати на запобігання можливим негативним впливам на економічну безпеку та про розміри відверненої і заподіяної шкоди дає об'єктивну оцінку результативності діяльності всіх структурних підрозділів (відділів, цехів) підприємства з цього питання. Оцінювання ефективності роботи структурних підрозділів підприємства щодо економічної безпеки здійснюється з використанням таких показників: витрати на здійснення заходу; розмір відверненої шкоди; розмір заподіяної шкоди; ефективність здійснення заходу (як різниця відверненої та заподіяної шкоди, поділеної на витрати на здійснення заходу).

Серед функціональних складових належного рівня економічної безпеки фінансова складова вважається провідною й вирішальною, оскільки за ринкових умов господарювання фінанси є стимулом для діяльності підприємства [5, с. 143].

Етапи процесу охорони фінансової складової служби економічної безпеки підприємства зображено на рис. 4.10.

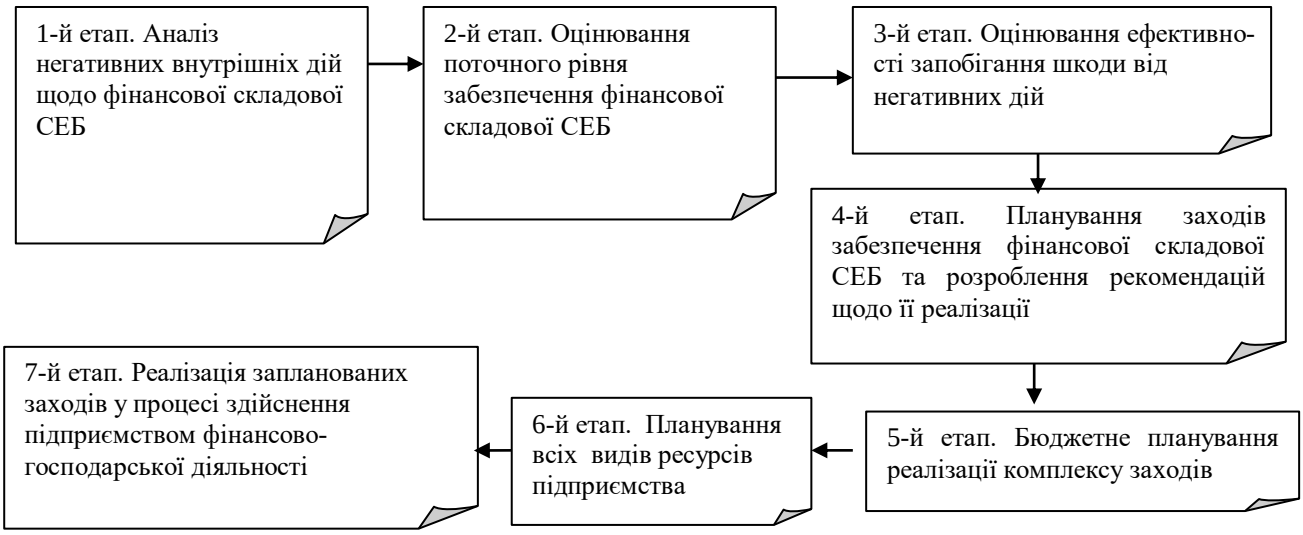

Рис. 4.10. Етапи процесу охорони фінансової складової служби економічної безпеки підприємства

Доцільно більш детально охарактеризувати організаційний процес здійснення охорони фінансової складової служби економічної безпеки підприємства.

Керівник фінансового відділу або провідний фахівець складової служби економічної безпеки підприємства спочатку повинен оцінити загрози економічній безпеці, що мають політико-правовий характер і включають:внутрішні негативні дії (неефективне фінансове планування та управління активами; невірно визначена ринкова стратегія; недієва цінова і кадрова політика);зовнішні негативні дії (спекулятивні операції на ринку цінних паперів; цінова та інші форми конкуренції; лобіювання конкурентами недостатньо продуманих рішень органів влади);непередбачувані обставини (стихійне лихо, страйки, військові конфлікти) та обставини, наближені до форс-мажорних (законодавчі акти, ембарго, блокада, зміна курсу валют тощо).

У процесі оцінювання поточного рівня забезпечення фінансової складової економічної безпеки підприємства повинні підлягати аналізу:

- фінансова звітність і результати роботи підприємства: платоспроможність, фінансова стійкість, структура й використання капіталу, формування прибутку;
- конкурентний стан підприємства на ринку: частка ринку, якою володіє суб'єкт господарювання, рівень застосування виробничих та інформаційних технологій, ефективність менеджменту;
- ринок цінних паперів підприємства: оператори й інвестори цінних паперів, курс акцій і лізинг.

Передумовою охорони фінансової складової служби економічної безпеки підприємства повинно бути планування комплексу необхідних заходів та оперативна реалізація запланованих дій у процесі здійснення підприємством фінансово-економічної діяльності.

Важливо зауважити, що належний рівень економічної безпеки значною мірою залежить від складу кадрів, їхнього інтелекту й професіоналізму.

Охорона інтелектуальної та кадрової складових служби економічної безпеки повинна охоплювати взаємопов'язані й водночас самостійні напрями діяльності фінансової складової служби економічної безпеки підприємства:

перший – зорієнтовано на роботу з персоналом, на підвищення ефективності діяльності всіх категорій персоналу;

другий – націлено 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 персоналу [2, с. 210].

Змістовну характеристику процесу охорони інтелектуальної та кадрової складової служби економічної безпеки підприємства наведено на рис. 4.11.

Рис. 4.11. Організаційні заходи з охорони інтелектуальної та кадрової складової служби економічної безпеки підприємства

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

Наступною важливою функціональною складовою служби економічної безпеки підприємства повинна бути техніко-технологічна складова.

Процес охорони техніко-технологічної складової економічної безпеки підприємства має передбачати здійснення керівництвом і відповідальними фахівцями декількох послідовних етапів:

перший етап повинен охоплювати аналіз ринку технологій стосовно виробництва продукції, аналогічної профілю підприємства чи організації-проектувальника (збирання та аналіз інформації щодо особливостей технологічних процесів, котрі виготовляють аналогічну продукцію, аналіз науково-технічної інформації стосовно нових розробок у цій 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;

на третьому етапі проводиться:

- аналіз товарних ринків за профілем продукції, що виготовляється підприємством, та ринків товарів-замінників;
- оцінювання перспектив розвитку ринків продукції підприємства;
- прогнозування можливої специфіки необхідних технологічних процесів для випуску конкурентоспроможних товарів.

четвертий етап має здійснюватися переважно для розроблення технологічної стратегії розвитку підприємства що має включати:

- виявлення перспективних товарів, які виготовляються;
- планування комплексу технологій для виробництва перспективних товарних позицій;
- бюджетування технологічного розвитку підприємства на засадах оптимізації витрат за програмою технологічного розвитку, для вибору альтернатив, опрацювання власних розробок або придбання патентів і необхідного устаткування на ринку;
- розроблення загального плану технологічного розвитку підприємства на основі впровадження інновацій;

на п’ятому етапі повинен оперативно реалізовуватися інноваційний план технологічного розвитку підприємства в процесі здійснення ним виробничо-господарської діяльності;

шостий етап має бути завершальним, на цьому аналізуватимуться результати практичної реалізації заходів щодо охорони техніко-технологічної складової служби економічної безпеки на підставі спеціальної карти розрахунків ефективності таких заходів [1, с. 110].

Оцінювання рівня техніко-технологічної складової служби економічної безпеки підприємства за окремим функціональним критерієм (ОФК) повинне здійснюватися на підставі аналізу розрахунку (ОФК) за формулою

$$ОФК = \frac{З_{відв.}}{В_{ркз.} + З_{завд.}}, \quad (4.3)$$

де $З_{відв.}$ – сумарний відвернений збиток від реалізації комплексу заходів для охорони техніко-технологічної безпеки підприємства;

$В_{ркз.}$ – загальна сума витрат на реалізацію такого комплексу заходів;

$З_{завд.}$ – сумарний завданий збиток за техніко-технологічною складовою його економічної безпеки.

Як додаток до плану охорони техніко-технологічної складової служби економічної безпеки підприємства потрібно розробити планову карту розрахунку ефективності заходів з виокремленням прогнозованих показників.

У такій карті, як правило, зазначають: розмір можливих збитків від негативних впливів; витрати на реалізацію заходів для відвернення очікуваної (можливої) шкоди й охорони техніко-технологічної безпеки підприємства; можливе значення окремого функціонального критерію ефективності заходів, що здійснюються для охорони цієї складової економічної безпеки; функціональні підрозділи підприємства, які є відповідальними за реалізацію пропонованого комплексу заходів.

Досить важливою повинна бути і політико-правова складова служби економічної безпеки підприємства. Загальний процес охорони політико-правової складової служби економічної безпеки підприємства також має здійснюватися за типовою схемою, яка охоплює такі дії організаційно-економічного спрямування: аналіз загроз негативних впливів; оцінювання поточного рівня забезпечення; планування комплексу заходів, спрямованих на підвищення цього рівня; здійснення ресурсного планування; планування роботи відповідних функціональних підрозділів підприємства; оперативна реалізація запропонованого комплексу заходів щодо організації належного рівня правової безпеки.

Основними причинами виникнення внутрішніх негативних впливів підприємства можуть бути: низька кваліфікація працівників юридичної служби відповідного суб'єкта господарювання та помилки у підборі персоналу цієї служби; недостатнє фінансування юридичного забезпечення підприємницької або іншої діяльності; небажання чи нездатність підприємства активно впливати на зовнішнє політико-правове середовище його діяльності.

Оцінювання реального стану політико-правової безпеки підприємства має здійснюватися за кількома напрямами:

рівнем організації та якості робіт щодо охорони правової складової загального рівня економічної безпеки;

бюджетно-ресурсним забезпеченням робіт;

ефективністю діяльності виробничих і функціональних підрозділів підприємства.

Суттєвими функціональними складовими служби економічної безпеки мають бути інформаційна, екологічна та силова складові підприємства.

Конкретні специфічні функції служби економічної безпеки в сукупності потребують створення інформаційної складової. Інформаційна складова повинна реалізувати такі функції: