МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

І. П. Отенко
Н. О. Москаленко

ОРГАНІЗАЦІЯ ТА УПРАВЛІННЯ СИСТЕМОЮ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ

Навчальний посібник

Харків
ХНЕУ ім. С. Кузнеця
2016

УДК 658.14/.17:005.934(075)
ББК 65.290-98я7
О-82

Рецензенти: директор Інституту бізнесу, економіки та інформаційних технологій Одеського національного політехнічного університету, д-р екон. наук, професор *С. В. Філиппова*; завідувач кафедри адміністративного та фінансового менеджменту, заступник директора Інституту адміністрування та післядипломної освіти Національного університету "Львівська політехніка", д-р екон. наук, професор *Н. Ю. Подольчак*; завідувач кафедри управління та фінансово-економічної безпеки Навчально-наукового інституту бізнес-технологій "УАБС" СумДУ, д-р екон. наук, доцент *Є. О. Балацький*.

Рекомендовано до видання рішенням ученої ради Харківського національного економічного університету імені Семена Кузнеця.
Протокол № 10 від 27.05.2016 р.

Отенко І. П.

О-82 Організація та управління системою фінансово-економічної безпеки : навчальний посібник / І. П. Отенко, Н. О. Москаленко. – Харків : ХНЕУ ім. С. Кузнеця, 2016. – 224 с.

ISBN 978-966-676-680-2

Розглянуто роль та місце фінансово-економічної безпеки в управлінні організацією і систему фінансово-економічної безпеки організації. Наведено опис організації управління фінансово-економічною безпекою, координації та планування, кадрової безпеки, а також моніторингу та контролю в системі фінансово-економічної безпеки організації.

Рекомендовано для студентів спеціальності "Менеджмент" освітньої програми "Управління фінансово-економічною безпекою", професіоналів і керівників підрозділів економічної та корпоративної безпеки.

УДК 658.14/.17:005.934(075)
ББК 65.290-98я7

ISBN 978-966-676-680-2

Зміст

Вступ

Управління фінансово-економічною та корпоративною безпекою бізнесу є невід'ємною складовою більшості підприємств, установ та організацій державних, громадських і підприємницьких структур у розвинених країнах. Для вітчизняної практики управління фінансово-економічною безпекою це достатньо новий напрям, який ще не отримав широкого розповсюдження. Разом з тим прискорення темпів розвитку бізнесу, прагнення до нових ринків збуту, вимогливе ставлення до стандартів ведення бізнесу з боку іноземних партнерів, розширення та збільшення кількості економічних злочинів у світі породжують нові ризики для організацій. Для їх мінімізації та попередження потрібно використовувати сучасні інструменти та механізми контролю, попередження, підтримки, одним з яких є фінансово-економічна безпека.

Серед найбільш значущих факторів на глобальному рівні, що обумовлюють розвиток систем безпеки в усьому світі, підготовку відповідних фахівців і розвиток широкого спектра послуг з безпеки бізнесу можна зазначити такі:

мінливий світовий порядок, в якому конкуренція на глобальному ринку визначена прагненням до конкурентних переваг;

висока загроза від хакерства та світового тероризму;

розвиток шпигунства, його розширення та зміна – від витікання національних секретів до крадіжок корпоративної інформації та використання Інтернету для ведення мережевого шпигунства за допомогою техношпигунів або мережевих агентів;

е-комерція або е-бізнес як прогресивна частина корпоративного бізнесу;

тиск з боку військової суперсили або регіональних союзів – таких, як НАТО, Європейський Союз; географічне поширення ісламістського фундаменталізму; конфлікти з колишніми дружніми країнами;

збільшення труднощів, пов'язаних як зі старими, так і новими загрозами з використанням нових і старих методів;

перехід від ручної праці до влади мозку та високих технологій.

Управління фінансово-економічною безпекою є сферою, яка, з одного боку, привертає увагу та викликає інтерес як у фахівців, професіоналів у цій галузі та суміжних з нею, так і у студентів, які бажають у майбутньому зайняти своє місце в цікавих і економічно привабливих сферах діяльності. З іншого боку, виникають неоднозначні оцінки з боку, наприклад, аудиторів і керівників щодо питань доцільності організації відповідних служб і змістовності їх роботи. Проте у світовій практиці компаній та підприємств, які охоплюють міжнародний ринок і мають велику базу продуктів і клієнтів, служби корпоративної та відділи економічної безпеки існують з часів закінчення "холодної" війни. Сьогодні вони є незалежними підрозділами у структурі організацій з великим штатом менеджерів з безпеки, професіоналів та аналітиків з фінансово-економічної безпеки, бізнес-розвідки, комплаєнсу, внутрішніх аудиторів тощо.

В Україні питанням фінансово-економічної безпеки слід приділяти більше уваги як на державному, так і на корпоративному рівнях. Відсутність державної системи в сфері фінансово-економічної безпеки та державної підтримки запровадження стандартів та інструментів щодо її забезпечення для приватних компаній та підприємств призводить до неоднакової якості управління в окремих організаціях і нерівномірного розвитку даної сфери в межах країни. Ефективність управління фінансово-економічною безпекою залежить насамперед від ініціатив і практики самих організацій, особливо якщо вони працюють на міжнародному ринку, будь то велика компанія або мале підприємство. У тексті навчального посібника під терміном "організація" слід розуміти всі види суб'єктів господарювання незалежно від форми власності.

Недоліки в площині вирішення практичних проблем є ознакою недостатньої розробленості теоретичних і методичних питань з організації й управління системи фінансово-економічної безпеки. Підтвердженням цього є відсутність широкого спектру навчальних посібників і методичної літератури з цієї теми. Саме цей факт став підґрунтям написання даного навчального посібника.

Основна мета навчального посібника – систематизувати знання з управління фінансово-економічною безпекою та надати цілісне розуміння

щодо закономірностей та особливостей організації системи фінансово-економічної безпеки.

Назва навчального посібника відповідає однойменній дисципліні, яка викладається магістрам освітньої програми "Управління фінансово-економічною безпекою" спеціальності "Менеджмент". Дана дисципліна є основною за спеціальністю, оскільки охоплює перелік тем, які формують початкове уявлення про діяльність професіонала в сфері фінансово-економічної безпеки та цілісне розуміння системи фінансово-економічної безпеки, основ і закономірностей її організації та управління. Поглиблене вивчення окремих питань організації й управління системи фінансово-економічної безпеки знаходять продовження в таких дисциплінах, як обліково-аналітичне забезпечення економічної безпеки, наукове та методичне забезпечення діяльності фахівців з фінансово-економічної безпеки, правове забезпечення безпеки суб'єктів господарської діяльності в Україні, професійна психологія, конкурентний аналіз і конкурентна розвідка, які викладаються студентам магістерської програми "Управління фінансово-економічною безпекою" спеціальності "Менеджмент" у Харківському національному економічному університеті ім. С. Кузнеця.

Структурно навчальний посібник складається з шести розділів, комплексних практичних завдань, глосарію професіонала з фінансово-економічної безпеки, переліку рекомендованої літератури та додатків. До кожного розділу розроблено відповідні компетентності професіонала, організований понятійний апарат, розроблена практична частина та складена рекомендована література.

У першому розділі надається розширене визначення категорії "безпека" та базових термінів – таких, як "загроза", "вразливість", "ризик", розкривається змістовність фінансово-економічної безпеки та її особливості, спектр загроз, що обумовлюють актуальність даної теми, механізм їх реалізації та можливі способи захисту.

Другий розділ розкриває місце управління фінансово-економічною безпекою та підходи до формування такої системи в корпоративному управлінні, взаємоузгодженість компонентів системи фінансово-економічної безпеки організації, її функціональне наповнення.

У третьому розділі визначено й описано послідовність, принципи організації та управління фінансово-економічною безпекою, особливості вибору організаційної структури підрозділу фінансово-економічної безпеки та її підпорядкованості, види завдань для професіоналів з фінансово-економічної безпеки.

Четвертий розділ присвячено питанням координації та планування в системі фінансово-економічної безпеки організації – механізму управління в системі фінансово-економічної безпеки, стратегічним і тактичним аспектам планування діяльності професіоналів з фінансово-економічної безпеки. Особливу увагу приділено взаємодії підрозділу фінансово-економічної безпеки з іншими підрозділами організації та зовнішніми структурами щодо протидії загрозам.

У п'ятому розділі висвітлено важливі питання в системі фінансово-економічної безпеки, пов'язані з кадровою роботою, це: система мотивації та культура безпеки, профілактичні методи кадрової безпеки в системі фінансово-економічної безпеки, етична відповідальність професіоналів з безпеки.

У шостому розділі охоплено питання моніторингу фінансово-економічної безпеки організації, контролю й аналітичним інструментам управління фінансово-економічною безпекою.

Даний навчальний посібник розрахований на студентів магістратури за освітньою програмою "Управління фінансово-економічною безпекою" спеціальності "Менеджмент", професіоналів у сфері фінансово-економічної безпеки, керівників підрозділів економічної та корпоративної безпеки. У процесі підготовки посібника використано теоретичні знання побудови систем корпоративної й економічної безпеки вітчизняних авторів, практика організації систем фінансово-економічної безпеки вітчизняних і міжнародних компаній та підприємств, праці з корпоративної безпеки зарубіжних авторів, які є практиками в цій сфері.

Автори висловлюють подяку шановним рецензентам, професорам С. В. Філипповій, Н. Ю. Подольчаку й Є. О. Балацькому, колективу редакційно-видавничого відділу Харківського національного економічного університету ім. С. Кузнеця за допомогу та сприяння у підготовці та публікації навчального посібника.

Той, хто знаходиться в безпеці, не відчуває загрози.
Абрахам Маслоу

Розділ 1. Роль та місце фінансово-економічної безпеки в управлінні організацією

Після вивчення матеріалів теми ви повинні:

знати:

основні терміни та поняття фінансово-економічної безпеки (безпека, загроза, вразливість, ризик);

природу виникнення загроз фінансово-економічній безпеці організації й їх види;

складові механізму реалізації та способи захисту від загроз фінансово-економічній безпеці організації;

приклади здійснення економічних злочинів;

рівні виникнення загроз фінансово-економічній безпеці організації;

уміти:

користуватися базовою термінологією фінансово-економічної безпеки;

розпізнавати ознаки забезпечення фінансово-економічної безпеки організації;

визначати загрози фінансово-економічній безпеці організації, їх мотиви та наслідки;

описувати економічні злочини та засоби протидії;

описувати рівні виникнення й ідентифікувати загрози фінансово-економічній безпеці організації.

План теми

1.1. Поняття безпеки організації, загрози та ризику.

1.2. Визначення фінансово-економічної безпеки організації.

1.3. Загрози фінансово-економічній безпеці організації і їх види.

1.4. Механізми реалізації загроз і способи захисту фінансово-економічної безпеки організації.

1.5. Рівні загроз фінансово-економічній безпеці організації.

Ключові поняття та терміни: безпека організацій, фінансово-економічна безпека, загроза, вразливість, ризик, економічний злочин, способи захисту.

1.1. Поняття безпеки організації, загрози та ризику

Безпека є універсальною категорією природних, суспільних і біологічних систем. Стосовно підприємств, установ, організацій – соціальних систем різних рівнів – термін "безпека" застосовується у різних аспектах, описуючи широкий спектр загальноприйнятих уявлень про організацію.

Безпека як категорія трактується як "*захищений стан, в якому не загрожує небезпека чому-небудь*" [4, с. 65]. У сучасних енциклопедичних виданнях подані різні підходи до визначення поняття "безпека", які враховують захищеність, загрози, ризики, забезпечення самостійності суб'єкта. Поняття "безпека" (лат. "sine cura – securitas") означає стан, якому притаманне почуття визначеності або відсутність занепокоєння.

Визначення поняття безпеки важливе, оскільки саме воно закладене в основу побудови системи безпеки організації та структурування її функціональних елементів.

По-перше, в загальному вигляді ***безпеку*** *можна розглядати як умови існування суб'єкта, контрольовані ним*. У цьому сенсі "перебувати в безпеці" означає "перебувати в безпечних умовах" – тобто в таких, які суб'єкт в змозі контролювати в процесі своєї діяльності та самореалізації. Враховуючи специфічну сукупність умов діяльності організації, можна говорити про перебування кого-небудь або чого-небудь у безпечних умовах, як то: безпечні умови праці або життєдіяльності, тобто умови нешкідливі, здорові, комфортні.

По-друге, ***безпека*** *є безумовною потребою людини*. Потреба в безпеці є одним із базисних мотиваційних механізмів і першоджерелом активності людини і є кінцевою метою в усіх сферах її життєдіяльності. Еволюцію потреби в безпеці наочно демонструє піраміда Маслоу. Обґрунтована цією теорією ієрархія ставить потребу в безпеці на перше місце серед тих, що відрізняють людину від решти живого світу (рис. 1.1). "Так само, як сита людина не відчуває себе голодною, той, хто знаходиться в безпеці, не відчуває загрози. *Потреба в безпеці* розглядається як активний і основний мобілізаційний ресурс організму, фактор лише в дійсно надзвичайних обставинах – таких, як війна, хвороба, стихійні лиха, зростання злочинності, дезорганізація суспільства" [21].

Рис. 1.1. **Місце безпеки в ієрархії потреб Маслоу**

Усі інші потреби – потреби більш високого рівня – виникають тільки після задоволення потреби в безпеці та створюють безпеку матеріальну, духовну, суспільну. Це насамперед пов'язане з природою всіх економічних злочинів. Усі злочини та шахрайства здійснюються людьми та пояснюються їхніми цінностями або "антицінностями", інтересами та мотивами [26].

По-третє, демонстрація цінностей через усвідомлення потреб людини визначає ***безпеку*** *як ключову цінність – благо, умову, що дозволяє домагатися поставлених цілей і задовольняти потреби наступного рівня*. Безпека виступає як цінність духовна, емоційна та матеріальна, тобто як будь-яке матеріальне або ідеальне явище, яке має значення для людини (або організації в цілому), заради якого вона діє, витрачає сили, заради якого вона живе.

Безпека як об'єктивна потреба, цінність та умова реалізується у діяльності людей, суспільства, держави, світової спільноти з виявлення (вивчення), попередження, послаблення, усунення (ліквідації) та відображення небезпек і загроз, здатних погубити їх, позбавити фундаментальних матеріальних і духовних цінностей, завдати неприйнятну (неприпустиму об'єктивно та суб'єктивно) шкоду, закрити шлях для виживання та розвитку. У цьому полягає глибинний смисл забезпечення безпеки організації будь-якого рівня (суспільного чи корпоративного, державного, світового), виділяючи її в окрему функцію управління такими організаціями.

Отже, під **безпекою організації** слід розуміти *захищеність організації від негативного впливу зовнішніх і внутрішніх загроз, дестабілізаційних факторів, за умов чого досягається стале функціонування та розвиток організації*.

Для усвідомлення сутності безпеки треба розуміти, що загрози існують завжди, але не всі організації потерпають від негативного їх впливу. Існування загрози як такої ще не означає негативні наслідки для організації. Наскільки організація може протистояти або запобігти впливу загрози, настільки сильною є система захисту її ресурсів, збільшує або зменшує ризики небезпеки та появи негативних наслідків. Тому забезпечення безпеки організації потребує визначення і загроз, і ризиків.

Між загрозою та ризиком існує пряма залежність, яку умовно можна визначити через здатність організації прийняти цей ризик (вразливість). Загроза та вразливість організації породжують ризик і призводять до небажаних наслідків і втрат (рис. 1.2).

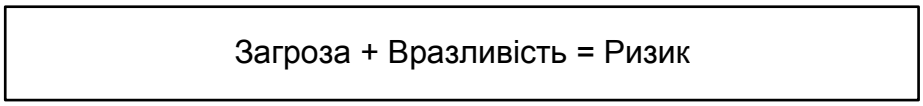

Рис. 1.2. **Основні дефініції безпеки**

Професіонал з безпеки має розуміти основні поняття, пов'язані із загрозами, і основні способи захисту від ризиків, які засновані на слабкостях і недоліках існуючої системи захисту організації.

Загроза – це перш за все небезпека, але більш точно – це:

декларація наміру заподіяти шкоду;

визначення чогось поганого, знак або небезпека, що щось небажане може статися;

хто-небудь або що-небудь, здатний принести шкоду або біль, наприклад: людина, тварина, який-небудь предмет.

Якщо не буде загроз, то й не буде потреби в будь-якому захисті. Загрози мають свої причини та можуть бути спровоковані певними суб'єктами. Тому професіонал з безпеки має розрізняти специфічні загрози для організації й їх причини. Такі причини загроз можуть критися у організаційному оточенні, організаційній культурі, продуктах і глобальному світогляді.

Завдання професіонала з безпеки – мати програму захисту ресурсів організації, яка [40, с. 28]:

мінімізує ймовірність успішної атаки агента загрози;

мінімізує втрати, якщо атака загрози відбувається;

проводить швидке відновлення організації у разі успішної атаки.

Вразливість – це слабкі місця в безпеці або процесі захисту організації. Зарубіжні експерти, автори навчально-методичних робіт з корпоративної безпеки, вразливість визначають таким чином [40, с. 36]:

"без належного захисту": відкритість до емоційної чи фізичної небезпеки або шкоди;

у військовому розумінні: відкритість до нападу та можливих пошкоджень;

крайня вразливість: легко переконати або піддатися спокусі;

фізична або психологічна слабкість: не в силах протистояти хворобі, слабкість або нездатність до опору;

схильність до підвищення ставок, відповідальність перед вищою мірою покарання.

Вразливість є характеристикою того, чи спроможна організація впоратися з загрозою та протистояти небезпеці, прийняти на себе ризик небажаного впливу існуючої загрози, відчути її. Прикладами таких вразливостей організації можуть бути відсутність або недоліки в:

системі охорони об'єктів організації (відеоспостереження, сигналізації, детекторів руху тощо) для попередження та реєстрації подій, що може призвести до розкрадання майна або заподіяння шкоди;

системі контролю й управління доступом до організаційних об'єктів і підрозділів, як то: через систему пропусків, охорони, використання біометрії;

процесі зберігання або видалення активів організації, як то: документів про майно, його транспортування;

системі безпеки, навчанні та розподілі обов'язків і відповідальності щодо захисту активів;

політиці безпеки, процедурах і процесах, які містять перелік заходів, указівки співробітникам у письмовій формі, через що складно притягнути співробітників до відповідальності за невиконання захисту організаційних активів;

системі інформаційної безпеки, організаційній мережі, своєчасного виявлення вторгнень з боку мережевих інтерфейсів всередині і за межами організації, що сприяє несанкціонованому доступу до організаційних мереж;

системі перевірки особових даних щодо довірених осіб;

системі перевірки співробітників перед найманням на роботу, особливо на відповідальні та важливі посади, що дозволяє найняти співробітників з історією зловживання службовими обов'язками, крадіжок та іншим кримінальним минулим.

Ризик визначається як:

шанс, що щось піде не так (небезпека травми, руйнування або втрати може статися);

можливість інвестиційних втрат, спекуляції;

статистичні коефіцієнти загрози, ймовірність загрози від чого-небудь, як то: невдачі інженерних систем.

За управління ризиками стосовно організацій відповідає ризик-менеджмент. Саме управління є загальним процесом визначення, контролю, елімінування, мінімізації небажаних подій, які можуть негативно вплинути на захист чого-небудь. Ризик-менеджмент включає оцінювання й аналіз ризику (включаючи аналіз витрат і доходів), реалізацію та тестування гарантій, загальні огляди.

Більшість організацій має в своїй структурі персонал з ризик-менеджменту, який охоплює різні аспекти управління бізнес-ризиками. Професіонал з безпеки повинен контактувати з цими фахівцями та координувати діяльність з управління ризиками щодо захисту структури та ресурсів організації.

1.2. Визначення фінансово-економічної безпеки організації

Розглядаючи безпеку суб'єктів господарювання, найчастіше дотримуються комплексного підходу, говорячи про корпоративну або безпеку бізнесу, економічну та фінансово-економічну безпеку. Терміни "корпоративна безпека" та "безпека бізнесу" вважаються синонімами.

Аналіз пошукових запитів за термінами безпеки організації (корпоративної, економічної, фінансово-економічної) за допомогою Google AdWords у всіх пошукових системах надав такі результати:

аналіз англомовних термінів щодо визначень безпеки організації говорить про високу їх затребуваність: на першому місті – фінансова безпека, на другому – корпоративна (кількість запитів постійно зростає), на третьому – економічна. Пропорційний розподіл оцінок між цими термінами вказує на їх узвичаєність, чітку визначеність і зростаючу актуальність;

за наявною кількістю запитів україномовних та російськомовних термінів можна говорити, що в українських і російських реаліях найбільш вживаним і розповсюдженим є термін "економічна безпека", який використовують і для опису безпеки корпоративної. Це підтверджує огляд наукової та методичної літератури з економічної безпеки українською та російською мовами;

аналіз запитів довів, що в іноземній практиці використовується термін "фінансова безпека", натомість у наших реаліях він стає найпопулярнішим, підкреслюючи актуальність питань цієї сфери.

Отже, доцільно розмежувати та надати визначення наведеним термінам, розкрити їх особливості (рис. 1.3).

Корпоративна безпека – це захист корпоративних активів – тобто тих, які підтримують і створюють здатність вести бізнес і приносити прибуток. Такими активами є люди, фізичні активи й інформація. Незважаючи на те, що корпоративна безпека спрямована насамперед на прибуткові корпорації, всі організації, включаючи неприбуткові (як, наприклад, уряд) потребують захисту активів. Тому корпорацією вважається група, визначена як особлива за законом і розглянута за законом як єдиний орган з власними правами та відповідальністю, окремими від тих, які притаманні її членам. Згідно з чинним законодавством, *корпорація* – це договірне об'єднання, створене на основі поєднання виробничих, наукових і комерційних інтересів, з делегуванням окремих повноважень централізованого регулювання діяльності кожного з учасників [1].

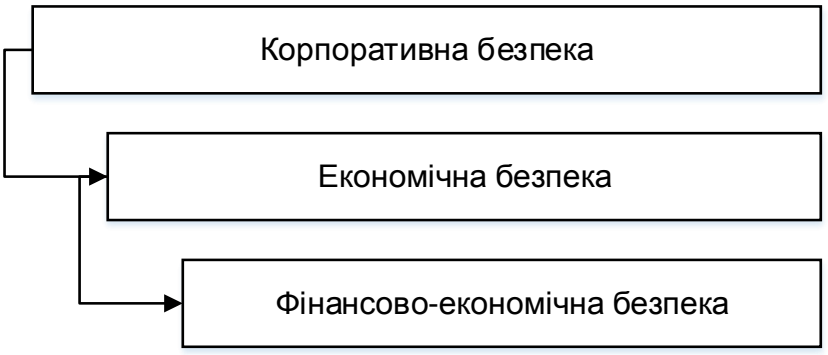

Рис. 1.3. **Співвіднесення понять безпеки організації**

Корпорації виконують багато функцій приватного бізнесу, уряду, освітніх структур, місцевого самоврядування тощо. Корпорація вважається найбільш досконалою формою організації підприємств, що існує переважно

у вигляді публічного акціонерного товариства, засновники якого формують акціонерний капітал шляхом об'єднання власних ресурсів через механізм випуску та продажу цінних паперів (передусім акцій), а співвласники несуть обмежену відповідальність. Під корпораціями розуміють компанії, які провадять більше одного виду діяльності, а їх бізнес-одиниці та підприємства знаходяться в різних країнах або містах. Такі компанії є суб'єктами як національного, так і міжнародного ринків.

Корпоративна безпека як найбільш ємне поняття складається з елементів, що відповідають за безпеку окремих ресурсів і видів її діяльності. Такими її елементами є: фінансово-економічна, інформаційна, кадрова, фізична, технічна, екологічна, техногенна безпека. Усі зазначені елементи мають значення, пріоритет визначається видом діяльності, характеристиками продукції або послуг, розміром, організаційним і географічним розташуванням тощо. Сутність того чи іншого виду визначається об'єктами забезпечення безпеки та джерелами загроз.

Об'єктами корпоративної безпеки виступають корпоративні активи та процеси управління ними: фінанси, персонал, інформація, матеріальні цінності, репутація, бізнес-процеси.

Стосовно окремих бізнес-одиниць і підприємств з метою комплексного забезпечення їх безпеки використовують термін "економічна безпека". Економіка підприємства будується на використанні всіх видів ресурсів (фінансових, матеріальних, трудових, інформаційних), а процеси, що протікають в сферах діяльності підприємства та засновані на використанні та відтворенні тих чи інших видів ресурсів, приводять до економічних результатів. Саме тому економічній безпеці приділяється більша увага в проблемах і темах з корпоративної безпеки. Найчастіше економічну безпеку розглядають самостійно, вважаючи, що саме вона є основною, а інші види безпеки стають функціональними завданнями відповідних підрозділів компанії:

інформаційна безпека – завданням ІТ-підрозділів;

кадрова – управління персоналом і відділу кадрів;

фізична – відділу охорони та режиму;

технічна – виробничих підрозділів;

екологічна та техногенна – служби охорони праці.

Безліч підходів, якими керуються для опису економічної безпеки, досить докладно висвітлено в роботах [15; 24]. Поєднуючи існуючи точки зору та погляди в наукових колах, визначимо **економічну безпеку** як систему

захисту бізнес-процесів і результатів господарської діяльності організації від небажаних змін. Усі бізнес-процеси розподіляють на основні (розроблення та виробництво продуктів або послуг; маркетинг; управління постачанням, збутом, доставкою; продаж та обслуговування клієнтів) і забезпечувальні (планування та стратегічний розвиток діяльності; управління корпоративними службами та приміщеннями; управління персоналом, фінансами, юридичними послугами, зовнішніми зв'язками, захистом зовнішньої середи; розроблення та супроводження систем і технологій). Структура об'єктів економічної безпеки організації показана на рис. 1.4.

Рис. 1.4. **Об'єкти економічної безпеки організації**

Для забезпечення захисту підприємству слід дотримуватися стратегії, що забезпечує достатній рівень і нарощування потенціалу, сталий розвиток бізнесу та підготовленість до можливих небажаних змін. Тому економічна безпека вважається обов'язковою умовою успіху в бізнесі для отримання прибутку та збереження цілісності організації та її структури.

Ознаками забезпечення економічної безпеки організації є:

протидія економічним злочинам;

стан ефективного використання ресурсів або потенціалу;

наявність конкурентних переваг;

захищеність від внутрішніх і зовнішніх загроз і забезпечення стабільного функціонування;

реалізація та захист економічних інтересів;

міцний корпоративний дух персоналу;

репутація та сила бренду.

В умовах ринкової економіки посилюються завдання щодо підвищення рентабельності, поточного контролю діяльності підприємств і управління ризиками. Багато підприємств потерпають від неефективності використання ресурсів – людських, фінансових, матеріальних, від нестачі необхідної для прийняття правильних рішень інформації, економічного шахрайства, ненавмисного або навмисного спотворення звітності з боку персоналу та керівників. Подібних проблем можна уникнути шляхом належної організації внутрішнього контролю та фінансово-економічної безпеки.

Фінансово-економічна безпека (ФЕБ) – це діяльність, здійснювана з метою надання об'єктивних гарантій і консультацій щодо створення та захисту стійкого та прибуткового функціонування, розвитку та вимогливого дотримання встановлених режимів (організаційних, юридичних, виробничих, фінансових тощо) організації, спрямована на вдосконалення її діяльності й є невід'ємною частиною контролю та підтримки управлінських рішень на підприємстві.

Ключова роль ФЕБ полягає у захисті сталого функціонування, а тому фінансово-економічну безпеку організації визначають як [7, с. 236]:

сукупність робіт із забезпечення максимально високого рівня платоспроможності та ліквідності оборотних коштів;

стан найбільш ефективного використання ресурсів, який проявляється в показниках прибутковості та рентабельності, а також в якості управління основними й оборотними засобами;

процес запобігання збиткам від негативних внутрішніх і зовнішніх впливів на економічну безпеку.

Під фінансово-економічною безпекою розуміють процеси, які спрямовані на гарантування достатньої впевненості в тому, що економічний суб'єкт забезпечує:

бізнес-процеси, які орієнтовані на ефективність і результативність організації, в тому числі досягнення фінансових і операційних показників, збереження активів, незалежність організації;

достовірність і своєчасність бухгалтерської (фінансової) й управлінської звітності;

дотримання застосовуваних положень нормативних документів, у тому числі під час здійснення фактів господарського життя та ведення управлінського та бухгалтерського обліку.

Важливо пам'ятати, що фінансово-економічна безпека не тільки сприяє реалізації економічним суб'єктом цілей своєї діяльності, а й гарантує їх досягнення, використовуючи систематизований і послідовний підхід до моніторингу різних загроз і підвищення ефективності бізнес-процесів, управління ризиками, внутрішнього контролю, корпоративного управління.

Цілями діяльності професіоналів з ФЕБ організації є запобігання:

збитку діяльності через розголошення, просочування інформації та несанкціонованого доступу до джерел конфіденційної інформації;

розкраданню фінансових і матеріально-технічних коштів, знищенню майна та цінностей;

порушенню роботи технічних засобів забезпечення виробничої діяльності, зокрема засобів інформатизації, а також запобігання збитку персоналу організації;

промисловому шпигунству, руйнуванню економічного потенціалу та конкурентоспроможності;

перевищенню повноважень і некваліфікованим діям з боку менеджменту організації, руйнуванню організаційної структури управління;

ущемлення комерційних інтересів власників і персоналу організації.

1.3. Загрози фінансово-економічній безпеці організації і їх види

Професіонал з безпеки повинен чітко уявляти загрози, рівні їх виникнення та природу, оскільки він повинен розуміти основні концепти, пов'язані з ризиками захисту активів, а також бачити слабкості та недоліки поточної системи захисту і поточних бізнес-процесів. Важливо розуміти загальні загрози, специфічні загрози для активів організації, а також те, що загрози мають причини, які можуть бути різноманітними.

Якщо не буде загроз, то не буде й потреби у захисті. Професіонал з безпеки повинен це розуміти, акцентувати увагу та зосереджуватися на предметі програми захисту господарської діяльності.

Безпосередні **загрози фінансово-економічній безпеці підприємництва** – це потенційні або реально можливі події, процеси, явища або дії фізичних та юридичних осіб, що порушують стан захищеності суб'єкта підприємницької діяльності, його сталість і розвиток і здатні призвести до припинення його діяльності або до фінансово-економічних втрат. Разом з цим, як зазначає В. В. Крутов, загрозою безпеці підприємництва не є автоматично

будь-яка дія, що має негативні наслідки. Так, не слід вважати загрозою фінансово-економічній безпеці підприємництва діяльність керівництва зі вкладення коштів у цінні папери, впровадження нових організаційних форм, організацію виробництва зовсім нового виду товару (хоча зазначені управлінські рішення є ризикованими та можуть мати негативні економічні наслідки). Такого роду рішення становлять невід'ємну частину самої підприємницької діяльності, що здійснюється на свій ризик і припускає певні втрати. У свою чергу, дії, які свідомо спрямовані на отримання будь-якої вигоди від економічної дестабілізації організації та заниження рівня її економічної безпеки, розцінюються як загрози. Діяльність керівництва організації, незважаючи на ризикований характер, у цілому відповідає чинному законодавству. Загрози, як правило, передбачають порушення законодавчих норм (тієї або іншої галузі права – цивільного, адміністративного, кримінального) та певну кількість відповідальних осіб, які їх здійснюють.

Таким чином, В. В. Крутов зазначає три ознаки, які є характерними для загроз економічній безпеці підприємницької діяльності [16, с. 319]:

свідомий і корисливий характер;

спрямованість дій на завдання збитків суб'єктові підприємництва;

протиправний характер.

Так, В. І. Ярочкін наводить експертні оцінки загроз підприємницької діяльності [37, С. 92].

1. Економічний тиск:

зрив угод;

паралізація діяльності фірм із використанням повноважень державних органів, засобів масової інформації;

компрометація діяльності фірми;

шантаж, компрометація керівників і окремих співробітників.

2. Фізичний тиск:

пограбування та розбійні напади на офіси, склади;

погрози фізичними розправами;

наймані вбивства.

3. Промислове шпигунство:

підкуп співробітників;

передання документів і розробок;

копіювання програм і даних;

проникнення в ПЕОМ;

підслуховування переговорів.

4. Здійснення фінансового впливу.

5. Здійснення психологічного впливу.

Загрози фінансово-економічній безпеці підприємницької діяльності можуть бути досить різноманітними. Але всі їх можна класифікувати на постійні та тимчасові, зовнішні та внутрішні.

Загрози можуть бути як *внутрішні,* так і *зовнішні*, які можуть призвести до зниження ефективності організації, втрати керованості, порушення стабільного функціонування. До зовнішніх для організації відносять загрози, обумовлені причинами, не пов'язаними безпосередньо з діяльністю самої організації – такі, як: розкрадання матеріальних коштів і цінностей третіми особами; незаконні дії конкурентів; вимагання з боку кримінальних структур.

Зовнішні загрози фінансово-економічній безпеці організації можна розподілити на сім груп, а саме:

економічні загрози в країні та світі;

політичні загрози в країні та світі;

загрози з боку державних органів (корупція тощо);

загрози у процесі здійснення цивільно-правових відносин з контрагентами;

загрози з боку конкурентів;

техногенні та природні загрози;

загрози, пов'язані з організованою злочинністю.

Економічні загрози повинні постійно діагностуватися й оцінюватися організацією, а професіонал з безпеки повинен володіти відповідною інформацію. Такі загрози можуть бути спричинені поточним і прогнозованим станом економіки, як то: темпи інфляції або дефляції, рівень зайнятості, міжнародний платіжний баланс, купівельна спроможність гривні, стабільність долара США за кордоном, податкова ставка тощо. Кожен з цих факторів може становити загрозу функціонуванню та розвитку організації. Водночас професіонал з безпеки має враховувати той факт, що для однієї організації стає економічною загрозою, інше сприймає як можливість. Під час спаду, наприклад, галузь з випуску запчастин для автомобілів процвітає, тому що за таких умов споживачі воліють ремонтувати свої автомашини, а не купувати нові.

Політичні загрози – це перш за все взаємовідносини бізнесу та держави. Активна участь лідерів бізнесу та підприємницьких структур у політичному процесі є чіткою вказівкою на важливість державної політики

для організацій. Керівництво організації повинно стежити за нормативними документами місцевих органів управління, урядовими кредитами на фінансування довгострокових вкладень, обмеженнями щодо найману робочої сили та можливості отримання позики, а також за угодами з тарифів і торгівлі, спрямованими проти інших країн або укладених з іншими країнами. Оскільки уряд постійно й активно бере участь у ділових питаннях, для організацій було б розумним уважно стежити за політичною діяльністю. Професіонал з ФЕБ має бути залучений до цього процесу.

Загрози з боку державних органів пов'язані з регулюванням і контролем виконання організацією інституційних вимог середовища, додержанням нормального перебігу виробничих та інших бізнес-процесів, контролем порушення норм, корупцією, недосконалістю законодавства, адміністративним ресурсом, політикою та ін.

Загрози у ході здійснення цивільно-правових відносин з контрагентами – це загрози прямого впливу на сталість функціонування та ФЕБ організації. Організація вступає у відносини з різноманітними контрагентами – постачальниками товарів (матеріальних ресурсів, послуг) і покупцями продукції, банками, іншими підприємствами. У процесі цих відносин у обох сторін виникають зобов'язання, згідно з якими вони повинні у визначений термін здійснити грошові платежі, поставити товар або виконати послугу на користь іншої особи. Загрози виникають у разі невиконання контрагентом таких зобов'язань, як порушення строків постачань та оплати, неякісне виконання послуг, пошкодження товару або через його сумнівну репутацію та неблагонадійність.

Основні загрози для фінансово-господарської діяльності організації з боку контрагентів пов'язані з можливістю різних шахрайських дій. З боку покупців це може бути порушення строків і порядку оплати, одностороння зміна узгоджених цін і обсягів закупівель та ін. З боку постачальників це може бути порушення строків поставок, номенклатури, якості, ціни, умов постачання тощо. Шахрайство з боку постачальників виражається в розкраданні грошових коштів покупців з використанням різних способів обману та маніпуляцій. У відносинах з сумнівним контрагентом для суб'єктів господарювання можуть виникати податкові ризики. Це загрожує платнику податків не тільки пенями та штрафами, а й репутацією. Такі контрагентські ризики можливі з різних причин, а саме: неспроможність (банкрутство) контрагента або наявність у нього ознак банкрутства; події політичного характеру; тривале зупинення виробництва у контрагента

внаслідок аварії, катастрофи, пожежі, стихійного лиха. Тому професіонал з ФЕБ має перевіряти контрагента та підтверджувати його благонадійність.

Загрози з боку конкурентів формують окрему групу загроз і ризиків. Жоден суб'єкт господарювання не може собі дозволити ігнорувати фактичні та можливі реакції своїх конкурентів. Шпигунство й інші прояви недобросовісної конкуренції на ринку обумовлюють пильну увагу професіоналів з безпеки. Професор Майкл Портер, проводячи аналіз конкурента, ставить такі питання: "Що рухає конкурентом?", "Що робить конкурент?" і "Що він може зробити?". Професіонал з ФЕБ має доводити факти протиправних дій з боку конкурентів і мати відповідну стратегію захисту.

Природні загрози не мають економічної природи, але можуть призводити до фінансового збитку – недоотримання прибутку, фінансових утрат, руйнування потенціалу. Їх називають "діяннями Бога" або "актами природи", це:

загрози стихійних явищ – пожежі, викликані блискавкою, повені внаслідок сильних дощів, землетруси, зсуви, грязьові потоки, селі, лавини, штормові вітри й екстремальні перепади температури тощо;

повсякденні природні небезпеки – кліматичні, ґрунтові та фактори водного середовища.

Найбільш надійний механізм захисту від природних загроз – це страхування. Але за ним виникають вже інші ризики – ненадійність страхової компанії, "ризик безвідповідальності" та ін.

Загрози впливу людського фактора (*техногенні*) – це всі ті загрози, які не обумовлені природними чинниками. Екологічні катастрофи, політична напруженість, міжкультурні розбіжності серйозно загострюють ризики сталого функціонування підприємств і компаній в усьому: від порушення ланцюжків постачань до втрати ділової репутації. Такі загрози вимагають заходів щодо їх мінімізування.

Загрози, пов'язані з організованою злочинністю, набули поширення. Вони є складними та небезпечними не тільки для господарської діяльності організацій, але й для особистої безпеки власників, директорів, співробітників. Це зобов'язує професіоналів з ФЕБ діяти у тісній співпраці з правоохоронними структурами.

До наведеної класифікації можна додати також *технологічні загрози* – це зміни в технологічному зовнішньому середовищі, які можуть поставити організацію в безнадійне, програшне конкурентне становище.

Аналізуючи технологічне зовнішнє середовище, доцільно враховувати зміни в технології виробництва, а отже, в забезпеченні тим самим фінансово-економічної безпеки, застосуванні інформаційних систем і технологій в проектуванні та наданні товарів і послуг. Не всі організації знаходяться під впливом швидкого науково-технічного прогресу. Однак керівництво повинно визначити, які фактори в технологічному зовнішньому середовищі можуть призвести до створення так званого "футурошока", що виступає як загроза руйнування організації. Цей термін, введений в обіг Е. Тоффлером у 70-х рр. XIX ст. [51], інтерпретують як "шок майбутнього", або руйнівний стрес і дезорієнтацію, що виникає через вплив на індивідуум занадто великих змін за дуже короткий час.

Більшість великих підприємств і тисячі дрібних діють на міжнародному ринку, тому *міжнародні фактори загроз* мають бути предметом уваги цих організацій і служб їх безпеки. Керівництво сьогодні повинно постійно контролювати й оцінювати зміни в цьому широкому середовищі. Загрози фінансово-економічній безпеці організації можуть виникнути в результаті легкого доступу до сировинних матеріалів, діяльності іноземних картелів (наприклад, ОПЕК), змін валютного курсу та політичних рішень у країнах, що виступають у ролі інвестиційних об'єктів або ринків.

Фактори загроз соціальної поведінки включають мінливі очікування, відносини та звичаї суспільства. Зміни, що впливають на соціум, формуючи його ставлення до майбутнього, створюють відповідні загрози. Вони знаходяться у тісній взаємодії із змінами технологічного середовища, політичними кризами, економічною ситуацією, екологічними катастрофами тощо. До важливих факторів сьогодні належать: соціальна нерівність і соціальна мобільність, роль жінок і національних меншин у суспільстві, зміна соціальних установок, рух на захист інтересів споживачів. Найчастіше саме соціальні фактори створюють найбільші загрози для організації. Щоб ефективно реагувати на їх зміну, організація має змінюватися, усвідомлено перетворюючись в установу, пристосовану до нового навколишнього середовища.

Ринкові фактори загроз – мінливе ринкове зовнішнє середовище, або ділове оточення, які є областю постійного занепокоєння для організацій. В аналіз ринкового зовнішнього середовища входять численні фактори загроз, а саме: рівень підприємницької активності в регіоні, стан споживчого ринку, життєві цикли різних виробів або послуг, легкість проникнення

на ринок, розподіл доходів населення та рівень конкуренції в галузі, взаємовідносини з постачальниками, посередниками, споживачами та конкурентами. У цілому аналіз ринкових факторів дає можливість професіоналу з безпеки уточнити стратегії захисту та зміцнити позицію організації щодо конкурентів і контрагентів. Корпоративна стратегія може концентруватися на проблемах захисту або розширенні компанії чи галузі. У світлі стратегії, обраної конкурентами, власна стратегія організації може бути спрямована на зміцнення внутрішнього ринку, пошук урядового захисту проти іноземних конкурентів або на розширення міжнародної активності з метою протидії стратегіям інших компаній.

Внутрішніми загрозами є такі, чия поява обумовлена або породжується діяльністю самої організації (його власників, керівників та іншого персоналу), а саме – розголошення власними співробітниками конфіденційної інформації, низька кваліфікація фахівців, які розробляють ділові документи (договори), неефективна робота служби економічної безпеки й осіб, відповідальних за перевірку контрагентів. Внутрішні загрози можна розподілити на такі:

загрози з боку персоналу організації;

загрози, пов'язані з неефективним управлінням і організацією бізнес-процесів.

Так, автори роботи [7] детально описують загрози економічній безпеці підприємства, що виникають на рівнях акціонерних відносин, вищого менеджменту, бізнес-процесів, обліку та контролю фінансово-господарської діяльності.

За ступенем важкості наслідків В. В. Крутов [16, с. 319] виділяє загрози з високою, значною, середньою та низькою вагою наслідків.

Висока вага означає, що зазначені загрози можуть призвести до різкого погіршення всіх фінансово-економічних показників діяльності суб'єкта підприємництва, що може викликати негайне припинення його діяльності. У цьому випадку, як правило, відбувається ліквідація суб'єкта господарювання.

Значний ступінь важкості наслідків реалізації загроз передбачає можливість нанесення суб'єкту підприємницької діяльності таких фінансових втрат, які негативно вплинуть на основні фінансово-економічні показники та на його діяльність у майбутньому.

Середній ступінь важкості означає, що подолання наслідків здійснення загроз вимагає витрат в обсязі поточних витрат суб'єктів господарювання, проте цей процес не є довготривалим.

Наслідки реалізації загроз із низьким ступенем наслідків не завдають будь-якого істотного впливу ні на стратегічні позиції суб'єкта господарювання, ні на його поточну діяльність.

В управлінні ФЕБ важливо розрізняти загрози *за об'єктами впливу*. Об'єктами впливу виступають насамперед ресурси: трудові (персонал), матеріальні, фінансові, інформаційні:

загрози персоналу – шантаж з метою отримання конфіденційної інформації, викрадення співробітників, вимагання тощо;

загрози матеріальним ресурсам – пошкодження будинків, приміщень, систем зв'язку, крадіжка устаткування;

загрози фінансовим ресурсам – шахрайство; фальсифікація фінансових документів, валюти, викрадення коштів;

загрози інформаційним ресурсам – несанкціоноване підключення до інформаційної мережі фірми, вилучення конфіденційних документів.

За суб'єктами загроз: загрози з боку кримінальних структур; конкурентів; контрагентів; власних співробітників; правоохоронних і контролюючих структур. В іноземній спеціальній літературі суб'єктів, які спроможні завдати збитку (шкоди) організації, називають агентами загроз.

За видом збитку – загрози, реалізація яких завдає прямих збитків, та загрози, що призводить до втрати вигоди.

Усі можливі фактори загроз безпеці організації можна розподілити на дві групи. До першої належать *передбачувані загрози*, тобто відомі з теорії безпеки або господарської практики та включені у відповідний список. *Непередбачувані загрози*, визначати які на стадії аналізу небезпечної ситуації або ризику організації неможливо. Одне з найважливіших завдань безпеки полягає в тому, щоб створити регулярну програму попередження та виявлення факторів загроз, звузити коло загроз другої групи.

Усі загрози, за винятком природних, мають соціальну природу та спровоковані суб'єктами (фізичними й юридичними). Тому розглядати загрози стосовно організації слід у тісному зв'язку та взаємодії чинників внутрішнього та зовнішнього середовищ. Метою професіоналів з ФЕБ є своєчасне виявлення та запобігання загрозам, забезпечення захищеності діяльності організації та досягнення нею цілей сталого функціонування та розвитку.

1.4. Механізми реалізації загроз і способи захисту фінансово-економічної безпеки організації

Отже, загроза – це подія або цілеспрямована дія, в результаті якої збільшується ймовірність порушення нормального функціонування організації та недосягнення нею своїх цілей, зокрема заподіяння організації якої-небудь шкоди. Низка негативних явищ в фінансово-господарській діяльності, які за своєю сутністю відповідають загрозам, мають комплексний характер. Більшість з них є типовими, їх класифікація розглянута в підрозділі 1.3.

Боротьбу із загрозою рекомендують проводити за такою послідовністю:

I етап – визначення загрози;

II етап – визначення варіанта реалізації загрози та формування моделі потенційного правопорушника;

III етап – визначення ймовірності настання події;

IV етап – визначення можливого збитку від загрози;

V етап – побудова системи захисту від загрози, включаючи превентивні, заходи з реагування під час виникнення загрози та заходи з ліквідації наслідків.

Реалізація загрози шляхом нанесення економічного збитку організації може супроводжуватися через отримання вигоди будь-яким суб'єктом (наприклад, привласнення активів, шахрайство). Проте загроза може бути реалізована з інших причин, наприклад, пожежею або випадковою помилкою в податковій декларації, яка призведе до штрафних санкцій. У будь-якому випадку предметом розгляду є загрози спричинені діяннями певних суб'єктів – агентів загроз, як їх визначають в спеціальній літературі з корпоративної безпеки [38; 40].

Механізми реалізації загрози – це мотиви, засоби та способи її здійснення. Будь-яка загроза реалізується через мотиви агентів загроз, застосовувані засоби та способи. Агентами загроз можуть виступати співробітники, контрагенти, конкуренти, державні органи, шахраї й організована злочинність, хакери, покупці, політичні активісти, терористи, зовнішні аудитори, консультанти, боржники, торговці наркотиками, економічні та промислові шпигуни тощо.

На рис. 1.5 подані оцінки типових видів економічних злочинів за даними міжнародної аудиторської компанії *Price Waterhouse Coopers* [56]. За її оцінками, більше однієї третини організацій є жертвами економічних злочинів.

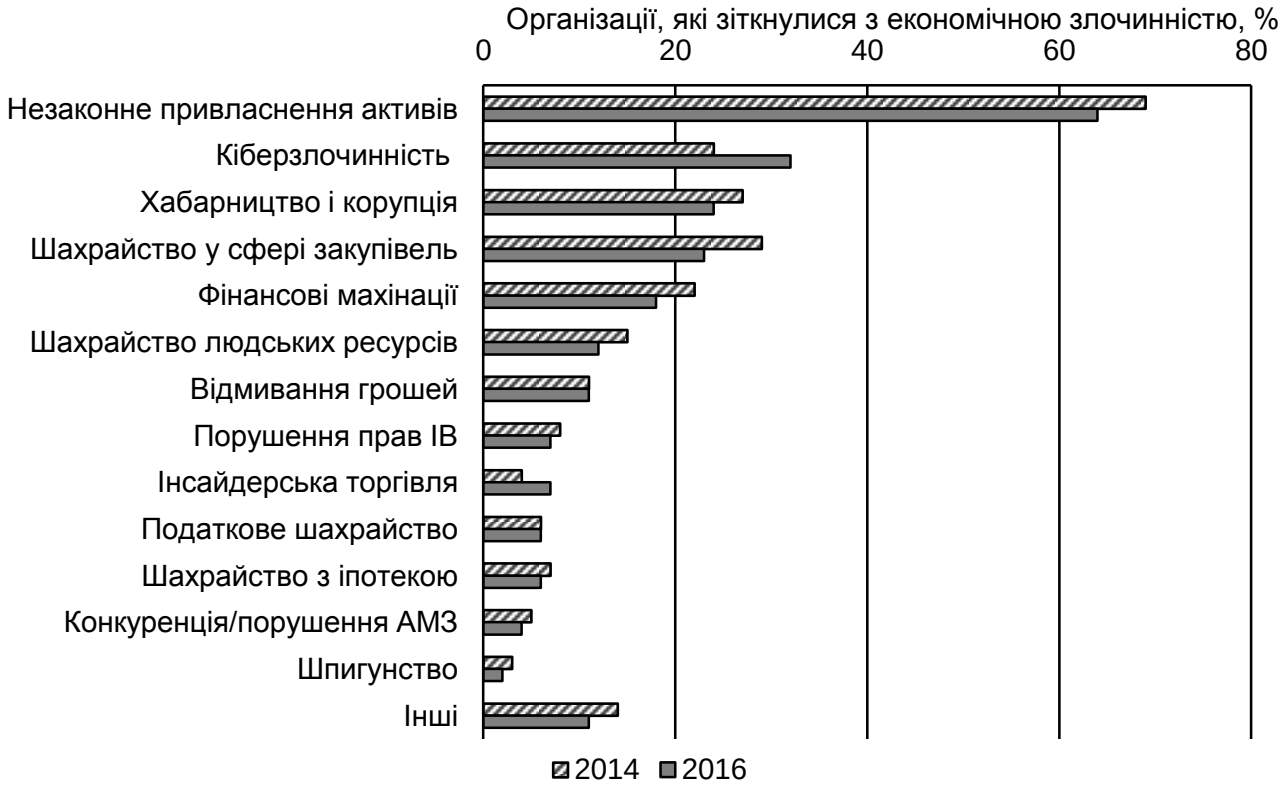

Рис. 1.5. **Оцінки типових видів економічних злочинів**
(за даними *PWC)*

Найбільш вразливою загрозою XXI ст. вважається кіберзлочинність (друге місце серед зареєстрованих економічних злочинів). Найбільша трудність у протистоянні економічній злочинності полягає в тому, що місцеві правоохоронні органи не володіють достатніми ресурсами, щоб розслідувати злочини, покладаючи відповідальність щодо боротьби з економічною злочинністю на організації. Фахівці *PWC* зазначають, що 82 % усіх розкритих злочинів здійснені працівниками відповідних організацій. А це означає, що агенти загроз організації знаходяться в їх корпоративному середовищі. Саме це призвело до поширення такої діяльності, як управління фінансово-економічною безпекою.

Усі дії з боку персоналу, спрямовані проти блага організації, або такі, що прямо чи опосередковано можуть завдати шкоди, (обман, недбалість, недогляд, приховування, брехня, кримінал, корупція, хабарництво, маніпуляція, викривлення, злодійство), об'єднуються єдиним визначенням – шахрайство.

Шахрайство має широкий спектр визначень, а саме:

це кримінальний обман; людина або річ, які не є тим, за що себе видають (Оксфордський словник);

використання свого становища з метою особистого збагачення шляхом навмисного неефективного використання ресурсів або активів організації, яка наймає на роботу (Асоціації сертифікованих фахівців з розслідування шахрайства – ACFE);

обман, нечесні дії з корисливою метою ("Тлумачний словник" С. І. Ожегова);

навмисні дії одної або більше осіб серед керівництва, управлінського персоналу, працівників або третіх осіб, що полягають у використанні обману для отримання неправомірної або незаконної вигоди (Міжнародні стандарти аудиту ISA 240).

За даними дослідження Ernst & Young:

рівень зафіксованого в Україні корпоративного шахрайства трохи вищий за середній у розвинених країнах (13 %), але кращий за показник країн, що розвиваються (20 %);

у середньому один з тисячі співробітників обманює компанію один раз на рік;

у середньому лише чотири з десяти осіб чесні з оточуючими;

середній термін, протягом якого здійснюється шахрайство, – 18 місяців з моменту початку шахрайських дій до моменту їх виявлення.

Згідно зі світовими дослідженнями, XXI ст. визнане століттям шахрайства, оскільки цей вид злочину не є особливо тяжким (не вбивство та не пограбування), тому строго не карається, але є дуже прибутковим і зазвичай важко доведеним. Шахрайство у сфері закупівель і бухгалтерського обліку відбувається внаслідок зростання кількості внутрішніх шахрайських операцій, злочинів на рівні вищого керівництва та відповідального персоналу організацій, відсутності системи покарання за економічні злочини.

Найбільш типовими та традиційними видами економічних злочинів вважаються: привласнення активів, кіберзлочинність, хабарництво та корупція, шахрайство у сфері закупівель і бухгалтерського обліку [56; 57].

Незаконне привласнення активів історично вважається самим простим для виявлення шахрайством, оскільки його досить легко виявити та передбачити. Основні використовувані методи з попередження привласнення активів – це посилення організаційного контролю, аналітичні процедури внутрішнього аудиту.

Кіберзлочинність набуває поширення з низки причин: розповсюдження використання інформаційних технологій: трансформація на цій платформі таких видів загроз, як шахрайство з активами або в бухгалтер-

ському обліку; складність виявлення загроз; відсутність і недоліки превентивних заходів. Як приклад можна навести фінансові злочини, здійснювані організованими групами осіб, які добре фінансуються та займаються викраденням коштів та інших активів за допомогою сучасних технологій [57].

Корупція та хабарництво є достатньо розповсюдженою загрозою в усьому світі. Вони здійснюються насамперед у країнах з низьким рівнем розвитку державних інститутів.

Найбільша кількість економічних злочинів відбувається у фінансовому та державному секторах, транспортуванні та логістиці, у сфері роздрібної торгівлі та споживчих товарів, комунікацій, аерокосмічній і оборонній галузях, страхуванні, енергетиці, комунальному господарстві та гірничодобувній промисловості.

Причини розповсюдження економічної злочинності криються як у мотивації агентів загроз, так і у змінюваному оточенні.

Ділове середовище й умови функціонування організацій значно змінилися. Так, у минулому була розповсюджена модель довготривалих трудових відносин між компанією (або підприємством) і співробітниками. Організації демонстрували свою лояльність до співробітників, співробітники були лояльними до них. На одному підприємстві працювали майже сім'ями – від батька до сина, аж до виходу на пенсію. Ситуація змінилась, організації прагнуть зберегти продуктивність, не бажаючи зазнавати фінансових витрат. Тому за умови фінансових складнощів суб'єктів господарювання під скорочення підпадають насамперед витрати на персонал шляхом звільнення персоналу й урізання соціальних виплат.

Отже, економічна злочинність і шахрайство в фінансово-господарській діяльності організації підвищує її вразливість, ризики фінансово-економічних втрат, знижуючи тим самим рівень фінансово-економічної безпеки. Це питання стратегічного характеру, які вирішуються на самому високому рівні – власниками та керівником суб'єкта господарювання.

Спектр можливостей здійснення злочинних вчинків щодо фінансово-господарської діяльності достатньо широкий: від засобів, що належать самій організації, до залучення агентів і ресурсів із зовні. Ступінь необхідного захисту залежить від безлічі факторів, які називають "драйверами безпеки". *Драйвери безпеки* – це ті засоби, способи та прийоми, які формують певний рівень безпеки в певний час. Для того щоб знизити ризик або запобігти можливості здійснення злочинного вчинку, заходи безпеки мають бути застосовані до конкретних ресурсів організації, виходячи

з потрібної суми грошей, людей необхідної кваліфікації, часу й інших чинників, які необхідні для забезпечення адекватного захисту ресурсів.

Найбільш популярні методи виявлення шахрайства не змінилися за останні декілька років. За оцінками тієї ж аудиторської компанії, список, як і раніше, очолює корпоративна служба безпеки, і лише 6 % зловживань виявляє служба внутрішнього аудиту (глобально – у 14 % випадків). Більше половини учасників опитування (54 %) не використовують систему анонімного оповіщення. Однак 82 % респондентів, які використовують таку систему, вважають її ефективною. Також варто зазначити, що 27 % респондентів в Україні не знали про методи виявлення шахрайства у порівнянні з 10 % респондентів у світі. Наведені факти є доказовою основою необхідності організації підрозділів корпоративної, зокрема фінансово-економічної, безпеки організацій.

1.5. Рівні загроз фінансово-економічній безпеці організації

Можна виділити такі *напрями криміналізації діяльності організацій* [8, с. 77]:

здійснення заборонених законом видів діяльності (торгівля зброєю, виробництво та торгівля наркотиками, проституція, торгівля людьми, фальшивомонетництво, контрабанда та ін.);

здійснення неліцензованих видів діяльності. Сюди можна віднести передусім "чорну" банківську діяльність, виробництво контрафактної продукції, проведення будівельних робіт без відповідної ліцензії, використання несертифікованих матеріалів тощо;

здійснення діяльності, яка не потрапляє в офіційну звітність суб'єкта господарювання. Це виробництво не врахованих на підприємстві робіт, продукції, виконуваних силами підприємства, але оформлених на підставну фірму, контрольовану керівництвом підприємства. Для роздрібних торгових організацій такими є традиційні операції зі зменшення виручки шляхом викривлення інформації;

використання незаконних методів діяльності – від недобросовісної конкуренції до комерційного підкупу, хабарів, шантажу тощо;

здійснення незаборонених операцій, кінцевою або справжньою метою яких є отримання тієї чи іншої вигоди, що інакше було б неможливо, у тому числі з використанням удаваних угод. Зазвичай це використання лазівок у законодавстві, а також побудова фінансових схем з метою зменшення податкового чи іншого тягаря. Сюди можна віднести страхові й інші

схеми виплати заробітної плати, збільшення собівартості робіт, продукції підприємства шляхом укладання фіктивних субпідрядних контрактів з підставними фірмами, махінації з ПДВ у експорті, "осадження" прибутку на торгівельних посередниках і багато іншого.

Рівень загроз і фінансово-економічних наслідків, які вони провокують, залежить від того, на якому рівні управління компанією загрози виникають і хто виступає агентом цих загроз. Так, відносини всередині організації можна розбити на такі рівні (рис. 1.6): між власниками; між власниками та вищим керівництвом; між вищим керівництвом і менеджерами середньої ланки; між власниками та трудовим колективом; між третіми сторонами та власниками; між третіми сторонами та організацією.

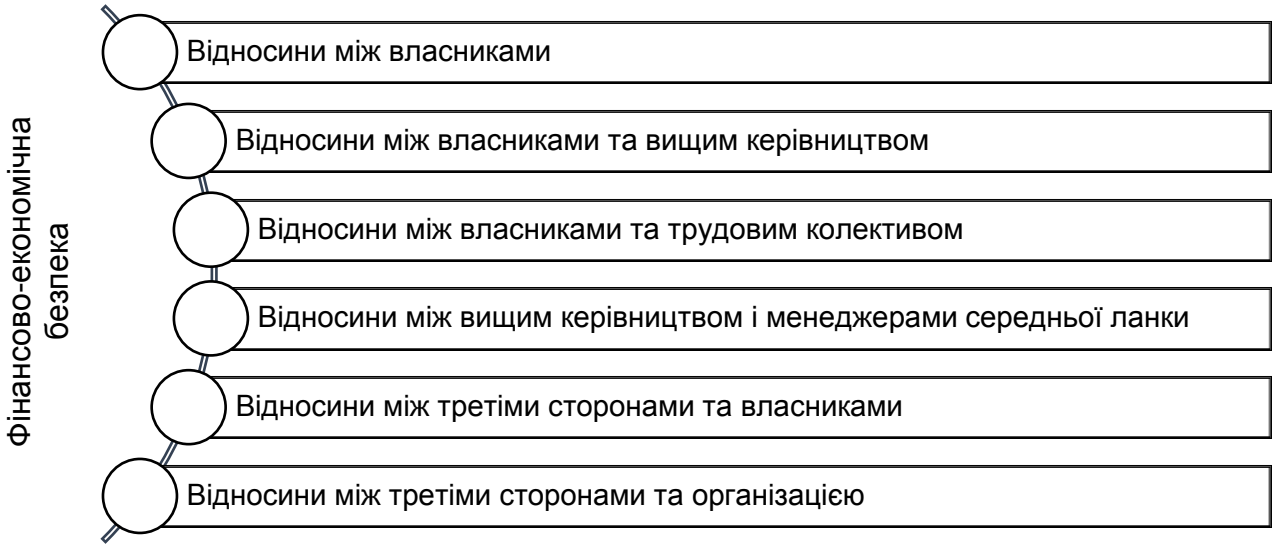

Рис. 1.6. **Рівні загроз фінансово-економічній безпеці організації**

Описані відносини можуть бути настільки переплетені між собою, що аналізувати їх окремо немає сенсу. Так, загрози, які спричинені діями власників і вищого керівництва, мають найбільш негативні наслідки щодо фінансово-господарської діяльності суб'єкта господарювання, їх слід розглядати сукупно. Третьою стороною можуть бути сторонні фізичні особи, юридичні особи, уповноважені органи державної влади.

Найбільш мотивовані в забезпеченні фінансово-економічної безпеки акціонери. Основними загрозами для власників можуть бути:

перехід права власності до сторонніх третіх осіб (наприклад, унаслідок недружнього поглинання);

економічно невигідний для власника продаж суб'єкта господарювання;

перехід права власності до вищого керівництва організації;

утрата контролю над бізнесом як таким, перехід контролю до сторонніх осіб;

утрата контролю над бізнесом як таким, перехід контролю до вищого керівництва суб'єкта господарювання;

ліквідація суб'єкта господарювання;

функціонування організації всупереч інтересам власників.

Треті особи можуть бути зацікавлені в організації, як правило, у таких випадках:

контрагенти підприємства (постачальники чи покупці) бажають вертикальної інтеграції;

контрагенти конкурентів підприємства також бажають вертикальної інтеграції, але знаходять дане підприємство більш доцільним для поглинання в силу яких-небудь причин, ніж конкурента;

конкуренти підприємства по горизонталі, бажають зайняти більш міцне положення на ринку шляхом розширення ніші;

дії професійних спекулянтів підприємствами;

під впливом інтересів інших сторонніх організацій.

З точки зору внутрішніх ризиків, основним джерелом загроз для суб'єктів господарювання вважаються дії менеджменту середньої ланки.

Потенційні способи реалізації загроз криються в здійснюваних бізнес-процесах, які умовно можна сформулювати таким чином [8]:

придбання товарно-матеріальних цінностей, робіт, послуг, а також їх обіг всередині підприємства;

розрахунки з оплати праці;

розрахунки за податками та податкова оптимізація;

фінансові операції (кредити, позики, цінні папери, інші операції);

реалізація та розрахунки з постачальниками та покупцями товарно-матеріальних цінностей та послуг.

Прикладами шахрайських дій та нанесення збитку суб'єкту господарювання з боку персоналу можуть бути:

1) придбання товарно-матеріальних цінностей:

- закупівля ресурсів (у завищеному обсязі, за ціною вище ринкової чи реальної відпускної ціни постачальника, неналежної якості), отримуючи вигоду від постачальника;
- лобіювання умов і приховування порушень поставки, розрахунків на користь постачальника з метою отримання вигоди від постачальника;

• оформлення надходження (оприбуткування) товарно-матеріальних цінностей у меншій або більшій кількості у порівнянні з реальною в корисливих цілях;

2) збереження та переміщення товарно-матеріальних цінностей всередині підприємства:

• розкрадання зі складу, завищення норм втрат і подальше привласнення надлишків;

• підміна аналогічними товарно-матеріальними цінностями більш низької якості або вартості, списання з різних причин;

• невідповідність товарно-матеріальних цінностей за кількістю й якістю за документами з підміною, розкраданням товарно-матеріальних цінностей або використанням неврахованих товарно-матеріальних цінностей в корисливих цілях;

3) використання товарно-матеріальних цінностей в виробничому процесі:

• накопичення надлишкових резервів товарно-матеріальних цінностей, використання необлікованих або "зекономлених" товарно-матеріальних цінностей в корисливих цілях;

• створення невідповідності між реальним виробничим процесом і технологічною картою (проектною документацією тощо) з використанням "зекономлених" відмінностей в корисливих цілях;

• завищення нормативів з подальшим використанням "зекономлених" товарно-матеріальних цінностей;

• реальне фактичне заниження витрачання товарно-матеріальних цінностей у виробництві, з відображенням у документах більшого порівняно з фактичним; нормативне витрачання товарно-матеріальних цінностей з подальшим використанням "зекономлених" товарно-матеріальних цінностей в корисливих цілях;

4) випуск готової продукції, робіт, послуг:

• ресурси підприємства використовуються на інших об'єктах;

• виконання понаднормових робіт (випуск продукції) й їх документальне невідображення;

• виконання робіт (випуск продукції) не повністю відображується документально;

• створення надмірних запасів готової продукції у виробничих підрозділах у корисливих цілях шляхом списання або уцінки "залежалої" продукції;

- приховування браку, списання без його знищення і його подальше використання в корисливих цілях;
- завищення нормативів браку та списання нормативної продукції в брак з її подальшим використанням у корисливих цілях;

5) реалізація готової продукції (матеріалів, сировини, напівфабрикатів, інших ресурсів, здача готових об'єктів):

- співробітник підприємства ініціює договір підряду, реалізацію (договір поставки продукції) на умовах, не вигідних підприємству, або у завищеному обсязі, отримуючи вигоду від покупця;
- співробітник підприємства здійснює (сприяє укладенню) угоду з обраним замовником (покупцем) за ціною нижче ринкової або реальної закупівельної ціни покупця, отримуючи вигоду від замовника (покупця);
- співробітник підприємства лобіює умови договору підряду (поставки), які вигідні більше замовнику (покупцеві), ніж підприємству, отримуючи вигоду від замовника (покупця);
- співробітник підприємства лобіює умови розрахунків, які вигідні більше замовнику (покупцеві), ніж підприємству, отримуючи вигоду від замовника (покупця);
- співробітник підприємства "не помічає" порушень з боку замовника (покупця) в частині поставки та розрахунків або виконує дії, спрямовані на приховування цих порушень, отримуючи вигоду від покупця;
- умови контракту (відвантаження продукції) оформлені у меншій або більшій порівняно з реальною кількістю,з подальшим використанням надлишків продукції або фактичною недопоставкою в корисливих цілях. Це дуже характерно для реалізації необлікованих надлишків продукції, використання ресурсів підприємства (електроенергія, вода, пар, орендна плата) орендарями;

6) розрахунки з контрагентами ведуться на умовах, невигідних для підприємства, або використовуються для розкрадання товарно-матеріальних цінностей, грошових коштів, інших активів;

7) розрахунки з оплати праці й їх оптимізація;

8) оптимізація витрат на оподаткування.

Цей перелік є типовим, фактично шахрайських дій з боку персоналу може бути набагато більше.

Рекомендована література: [1; 4; 7; 8; 16; 17; 21; 23; 27; 37; 38; 40; 51; 56; 57].

Практична частина

Контрольні запитання

1. Надайте розширене визначення категорії "безпека". Визначте основні концепти безпеки організації. Доведіть зв'язок між ними.

2. Наведіть визначення "загроз" безпеки. Розкрийте, в чому можуть критися причини загроз та яка роль професіонала з безпеки у боротьбі з загрозами.

3. Розкрийте значення "вразливості". Наведіть приклади вразливостей організації.

4. Надайте визначення "ризику". Розгляньте та прокоментуйте організаційну функцію ризик-менеджменту.

5. Наведіть найбільш вживані терміни, які використовують для визначення безпеки організації. З'ясуйте різницю між ними. Дайте визначення й охарактеризуйте сутність корпоративної безпеки.

6. Дайте визначення економічної безпеки суб'єкта господарювання, розгляньте її об'єкти та види. Які ознаки безпечного стану суб'єкта господарювання?

7. Розкрийте зміст фінансово-економічної безпеки, які гарантії діяльності економічного суб'єкта забезпечує фінансово-економічна безпека?

8. Розгляньте та прокоментуйте, на що спрямована діяльність професіоналів з ФЕБ.

9. Розкрийте загрози фінансово-економічній безпеці підприємництва. Які ознаки є для них характерними?

10. Розкрийте зовнішні загрози фінансово-економічній безпеці організації за такими ознаками: економічні загрози в країні та світі; політичні загрози в країні та світі; загрози з боку державних органів (корупція тощо); загрози у ході здійснення цивільно-правових відносин з контрагентами; загрози з боку конкурентів; техногенні та природні загрози; загрози, пов'язані з організованою злочинністю.

11. Визначте внутрішні загрози фінансово-економічній безпеці організації за такими ознаками: за ступенем важкості наслідків, за об'єктами впливу, за суб'єктами загроз, за видом збитку, за передбачуваністю.

12. Охарактеризуйте механізм реалізації загрози, розкрийте сутність найбільш розповсюджених економічних злочинів.

13. Наведіть рівні загроз фінансово-економічній безпеці організації. Які основні загрози можуть бути для власників організації, спричинені діями менеджменту? Які загрози виходять від третіх осіб?

14. Розкрийте можливі загрози фінансово-економічній безпеці організації з боку персоналу, які мають місце в процесі придбання й обігу товарно-матеріальних цінностей.

15. Розкрийте можливі загрози фінансово-економічній безпеці суб'єкта господарювання з боку персоналу, які мають місце під час здійснення розрахунків з оплати праці.

Тестові завдання

1. Категорія "безпека" трактується як:

а) відкритість до фізичної шкоди;

б) захищений стан, в якому не загрожує небезпека чому-небудь;

в) ймовірність загрози від чого-небудь;

г) належний нагляд за активами.

2. Декларація наміру заподіяти шкоду – це:

а) загроза;

б) вразливість;

в) ризик;

г) шкода.

3. Безпека організації має на меті:

а) не допустити руйнування організації в ризикованих умовах функціонування;

б) протистояти можливій шкоді для фізичних активів організації;

в) захистити стан організації на всіх стадіях її розвитку від зовнішніх і внутрішніх загроз;

г) не допустити інвестиційні втрати та спекуляції.

4. Під вразливістю організації розуміють:

а) слабкі місця в процесі захисту організації;

б) фізичну або психологічну слабкість персоналу органів безпеки;

в) шанс, що щось піде не так (небезпека травми, руйнування або втрати);

г) стійка мотивація агентів загроз.

5. Яке з наведених визначень більш чітко визначає ризик:

а) шанс або ймовірність, що щось піде не так (небезпека травми, руйнування або втрата);

б) існування загроз фінансово-господарській діяльності підприємства;

в) вразливість підприємства до загроз, пов'язаних з організованою злочинністю;

г) інструмент контролю управлінських рішень у системі безпеки підприємства?

6. Корпоративна безпека – це:

а) контроль за виконанням контрагентами своїх зобов'язань;

б) виключно протидія недобросовісній конкуренції – до комерційного підкупу, хабарів, шантажу;

в) здатність компанії відновлювати свої ресурси;

г) захист корпоративних активів, які підтримують і створюють здатність вести бізнес і приносити прибуток.

7. Що з наведеного не є ознакою забезпечення економічної безпеки підприємства:

а) стан ефективного використання ресурсів або потенціалу;

б) зростання випадків шахрайства;

в) міцний корпоративний дух персоналу;

г) правильної відповіді немає?

8. Фінансово-економічна безпека – це:

а) діяльність із надання об'єктивних гарантій і консультацій у створенні та захисті сталого та прибуткового функціонування та вимогливого дотримання встановлених режимів (організаційних, юридичних, виробничих, фінансових тощо) організації;

б) удосконалення фінансово-господарської діяльності підприємства через управління ліквідністю, ділову активність, інвестиційну привабливість, кредитоспроможність;

в) здатність відновлювати ліквідність і платоспроможність оборотних коштів підприємства;

г) спрямування на вдосконалення діяльності – невід'ємна частина аудиторського контролю на підприємстві.

9. Фінансово-економічна безпека підприємства не гарантує:

а) що бізнес-процеси, які орієнтовані на ефективність і результативність організації, забезпечують досягнення фінансових і операційних показників, збереження активів, незалежність організації;

б) достовірність і своєчасність бухгалтерської (фінансової) й управлінської звітності;

в) зниження ризикованості операцій фінансової діяльності підприємства через коливання валютних курсів і нестабільну суспільно-політичну ситуацію в країні;

г) дотримання застосовуваних положень нормативних документів, у тому числі під час здійснення фактів господарського життя та ведення управлінського та бухгалтерського обліку.

10. Діяльність професіонала з фінансово-економічної безпеки не спрямована на запобігання:

а) розкраданню фінансових і матеріально-технічних коштів, знищенню майна та цінностей;

б) інформаційній атаці агентів загроз і розповсюдженню комп'ютерних вірусів;

в) промисловому шпигунству та руйнуванню конкурентоспроможності економічного потенціалу;

г) перевищенню повноважень і некваліфікованим діям з боку менеджменту, руйнуванню організаційної структури управління.

11. Загрози фінансово-економічній безпеці підприємництва – це:

а) припинення діяльності підприємства, його фінансово-економічні втрати;

б) реально можливі події, процеси, явища або дії фізичних та юридичних осіб, що порушують стан захищеності суб'єкта підприємницької діяльності, його сталість і розвиток;

в) певні втрати внаслідок вкладання коштів у фінансову діяльність;

г) будь-яка дія, що має негативні наслідки (наприклад. виробництво нового продукту).

12. Що з наведеного слід вважати загрозою фінансово-економічній безпеці підприємництва:

а) вкладення коштів у цінні папери;

б) упровадження нових організаційних форм;

в) організацію виробництва зовсім нового виду товару;

г) правильної відповіді немає?

13. Причини контрагентських ризиків – це:

а) неспроможність (банкрутство) контрагента;

б) події політичного характеру;

в) тривале зупинення виробництва у контрагента внаслідок аварії, катастрофи, пожежі, стихійного лиха;

г) усі відповіді правильні.

14. Екологічні катастрофи, політична напруженість, міжкультурні розбіжності – це загрози:

а) природні;

б) технологічні;

в) техногенні;

г) правильної відповіді немає.

15. Використання свого становища з метою особистого збагачення шляхом навмисного неефективного використання ресурсів або активів організації – це:

а) шахрайство;

б) фальсифікація;

в) підкуп;

г) шкода.

16. Вид злочину, який передбачає викрадення активів суб'єкта господарювання у відносно невеликих і несуттєвих розмірах – це:

а) незаконне привласнення активів;

б) шахрайство людських ресурсів;

в) фінансові махінації;

г) шахрайство у сфері закупівель.

17. Шахрайство, фальсифікація звітності та валюти, крадіжка коштів – це загрози:

а) персоналу;

б) матеріальним ресурсам;

в) фінансовим ресурсам;

г) інформаційним ресурсам.

18. Пошкодження будинків, приміщень, систем зв'язку, крадіжка устаткування – це загрози:

а) персоналу;

б) матеріальним ресурсам;

в) фінансовим ресурсам;

г) інформаційним ресурсам.

19. *Стан підприємства, за якого значне місце займає діяльність зі збільшення та привласнення доходів, отриманих злочинним шляхом, привласнення активів, здійснення заборонених законом видів діяльності тощо, характеризується як:*

а) криміналізація;

б) децентралізація;

в) корупція;

г) усі відповіді правильні.

Слово "криза", написане китайською, складається з двох ієрогліфів: один означає "небезпека", інший – "сприятлива можливість.

Джон Кеннеді

Розділ 2. Система фінансово-економічної безпеки організації

Після вивчення матеріалів теми ви повинні:

знати:

роль УФЕБ у системі корпоративного управління;

сутність СФЕБ, підходи до її формування;

компоненти СФЕБ (концепція, політика, програма) й їх визначення;

відділи корпоративного середовища СФЕБ організацій;

функції СФЕБ організацій, їх відмінності;

склад контролюючих органів в сфері ФЕБ організацій та їх функції;

уміти:

ідентифікувати інтереси суб'єктів корпоративного управління й осіб, зацікавлених у діяльності компанії;

обґрунтувати доцільність формування СФЕБ, об'єктів і суб'єктів ФЕБ організації;

описувати концепцію, політику ФЕБ організації;

описувати зв'язки відділів корпоративного середовища щодо забезпечення ФЕБ;

визначати й описувати функції СФЕБ організацій;

описувати стратегію дій керівника та професіоналів з ФЕБ під час планової або позапланової перевірки організації.

План теми

2.1. Управління фінансово-економічною безпекою та корпоративне управління.

2.2. Підходи до формування системи фінансово-економічної безпеки організації.

2.3. Компоненти системи фінансово-економічної безпеки організації і їх взаємоузгодженість з безпекою зовнішнього середовища.

2.4. Функції системи фінансово-економічної безпеки організації.

2.5. Контролюючі органи фінансово-економічної безпеки організацій і їх функції.

Ключові поняття та терміни: корпоративне управління, система фінансово-економічної безпеки, підхід, концепція, політика.

2.1. Управління фінансово-економічною безпекою та корпоративне управління

Одна з визначних проблем, з якою стикаються професіонали з безпеки й яка спричиняє значні фінансово-економічні втрати та руйнування активів організацій, є те, що керівники суб'єкта господарювання або члени корпоративного управління не усвідомлюють необхідність забезпечення кращого захисту активів своїх підприємств. Це призводить до того, що в критичній ситуації потрібні заходи з безпеки здійснюються частково або не здійснюються взагалі, а відповідальність за скоєні злочини ключові особи несуть не повній мірі.

На підтвердження цього можна навести такі цікаві факти щодо економічної злочинності в Україні за оцінками *PwC* [56]:

третина організацій не проводить оцінювання ризиків шахрайства;

більшість вітчизняних респондентів, які зафіксували випадки шахрайства, оцінюють збитки до 5 млн дол. США;

кожна п'ята організація, що постраждала від економічних злочинів, не вживала відповідних заходів стосовно співробітників, які скоїли їх.

Важливу роль у забезпеченні фінансово-економічної безпеки відіграють знання внутрішнього середовища організації як з боку органів управління, так і з боку персоналу. Один з п'яти опитаних респондентів не знають про існування формальної етики та комлаєнс-програми; багато помиляється щодо того, хто ними володіє, кому підпорядковується. Майже половина інцидентів серйозних економічних злочинів учинена в межах організації. Основні причини – моральний стан працівників і репутаційна шкода. Тому сьогодні об'єктивна потреба організацій в елементах управління безпекою має вбудовуватись у корпоративне управління й організаційну культуру й описану Кодексом корпоративну етику. "Люди та культура – ваша перша лінія оборони", – так визначають фахівці *PWC* [56].

Будь-яка організація складається з людей. І саме культура, спільні колективні цінності, моральний дух, бізнес-відносини, відносини з регулятором створюють потужну організацію та формують систему захисту. Професіонали з корпоративного управління й аудиту організацію сприймають як бізнес – зсередини та ззовні. Це підкреслює ключову роль, яку відіграють цінності безпеки в успішній бізнес-стратегії.

Персональну відповідальність за моральний дух і корпоративну етику, бізнес-ризики та стратегії, стан захищеності ресурсів і дії щодо запобігання ризикам, організацію всієї системи захисту несе керівник організації.

У межах своїх обов'язків виконавче керівництво організації виступає уповноваженим корпоративних власників для прийняття рішень щодо бізнес-ризиків, які пов'язані з купівлею або продажем частини компанії, виробленням продукції, ринками тощо. Вони також мають приймати рішення щодо ресурсів, які витрачаються на захист організації та побудову бізнес-процесів. Це включає в себе кількість грошей, людей та інших ресурсів, які виділяються на це. Професіонал з ФЕБ виступає в цьому випадку спеціалістом із захисту активів, власним консультантом для управлінських структур. Рішення, що стосуються того, який ризик прийняти в частині захисту активів, делегується професіоналу з ФЕБ.

Професіонал з ФЕБ має розуміти, що організаційні ресурси належать власникам. Тому рішення про те, скільки ресурсів має бути виділено для захисту різних активів, як правило, ґрунтуються на таких операціях, як повернення інвестицій, аналіз рентабельності й інших факторах.

Управління ФЕБ знаходиться у тісній взаємодії з радою директорів і менеджментом організації, бере участь у вдосконаленні систем управління сталим функціонуванням, протидії ризикам, контролі та корпоративному управлінні з метою забезпечення:

ефективності діяльності та процесу управління ризиками;

надійності й ефективності системи внутрішнього контролю;

повноти та достовірності фінансової й управлінської інформації;

дотримання законодавства;

збереження активів організації та захисту її персоналу.

Вибір методів і технологій ФЕБ визначається цілями та видами діяльності, набором специфічних для даної організації ризиків, станом навколишнього середовища. Інформатизація, поява Інтернету докорінно змінюють бізнес-середовище, виявляючи необхідність структурної перебудови традиційної системи корпоративного управління та безпеки.

У системі корпоративного управління підпорядкованість підрозділу ФЕБ має важливе значення, бо саме відповіді на запитання: "Перед ким звітує керівник ФЕБ та кому підпорядковується?" – визначають ефективність безпекової системи.

Розподіл повноважень визначається організаційно-правовою формою організації. В умовах малого підприємництва власники бізнесу є й управлінцями. З розвитком організації бізнесу власники відіграють помітно меншу роль у щоденному управлінні бізнесом. Зростання корпорації та кількості власників (акціонерів) приводить до передання управлінської функції найманим менеджерам.

Відокремлення функцій володіння й управління призводить до виникнення конфлікту інтересів між акціонерами та менеджерами, оскільки цілі ведення бізнесу в цих сторін різні. Саме для захисту інтересів акціонерів створена система корпоративного управління.

Корпоративне управління – це сукупність процесів і організаційних структур, створюваних Радою для інформування, управління та моніторингу діяльності організації з метою досягнення поставлених цілей.

Рада – це вищий орган управління організації, відповідальний за управління та/або нагляд за діяльністю та виконавчим керівництвом організації. Як правило, це незалежна група директорів (тобто рада директорів, наглядова рада або рада управлінців або повірених). Якщо такої групи немає, термін "рада" може означати керівника організації. Термін "рада" може означати раду з безпеки, якому орган управління делегує певні функції

Для більшості інвесторів – потенційних акціонерів якість корпоративного управління відіграє важливу роль у питанні "вкладати чи не вкладати?", а для компанії іноді можливість залучити ресурси є питанням життя чи смерті. Іноді "правильна" поведінка Ради директорів відіграє не менш важливу роль, ніж фінансові показники.

Після розподілу функцій володіння й управління взаємини між акціонерами (принципалами) та найманими менеджерами (агентами) отримали назву агентських відносин. Розподіл агентських відносин показано на рис. 2.1.

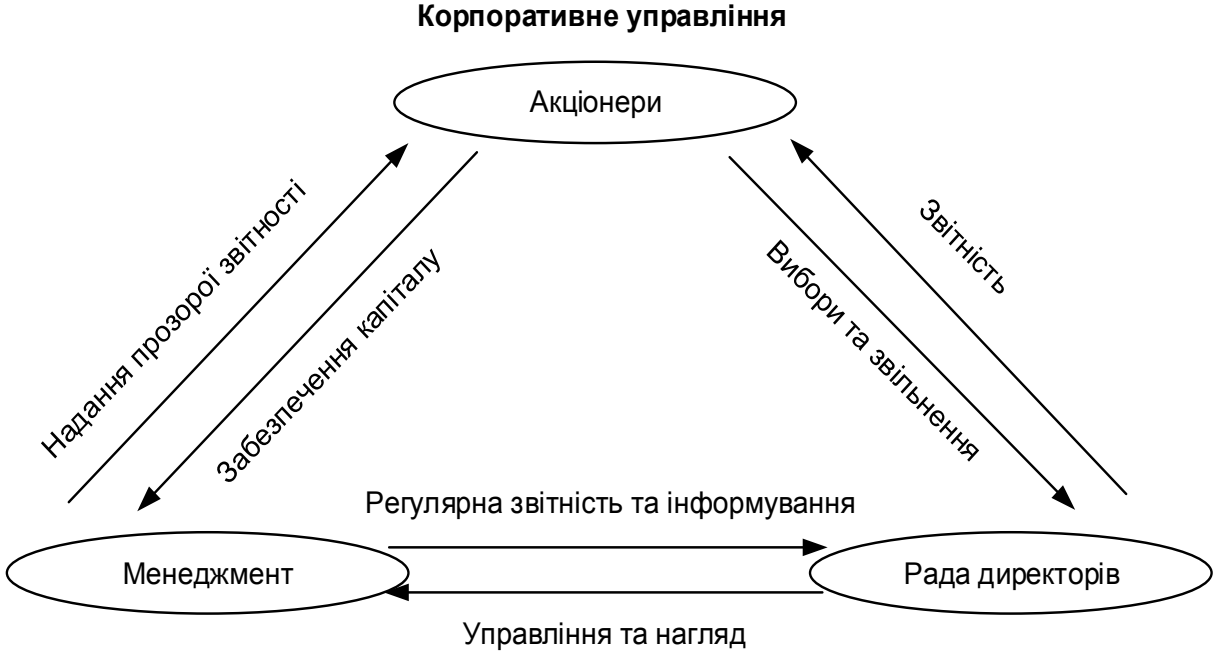

Рис. 2.1. **Розподіл повноважень у системі корпоративного управління**

Принципали (власники) наймають агента (керівництво) для керування від його імені. Агент стає довіреною особою принципала. Водночас у принципала виникають так звані "агентські" витрати, для того щоб контролювати дії агента в силу відсутності абсолютної довіри. Приймаючи на себе зобов'язання виконувати певні завдання, агент стає повністю підзвітний принципалу. Однак цілі агента (такі, як більш висока заробітна плата й інші винагороди) відрізняються від цілей принципала, який бажає збільшити своє майно. Така проблема – розбіжність цілей агента та принципала отримала назву "агентської проблеми".

Агентська проблема – конфлікт інтересів акціонерів, власників облігацій і менеджерів. Вона проявляється у суперечці інтересів менеджерів і постачальників капіталу з причини відсутності у менеджерів прагнення до збільшення доходів на інвестований капітал (рис. 2.2).

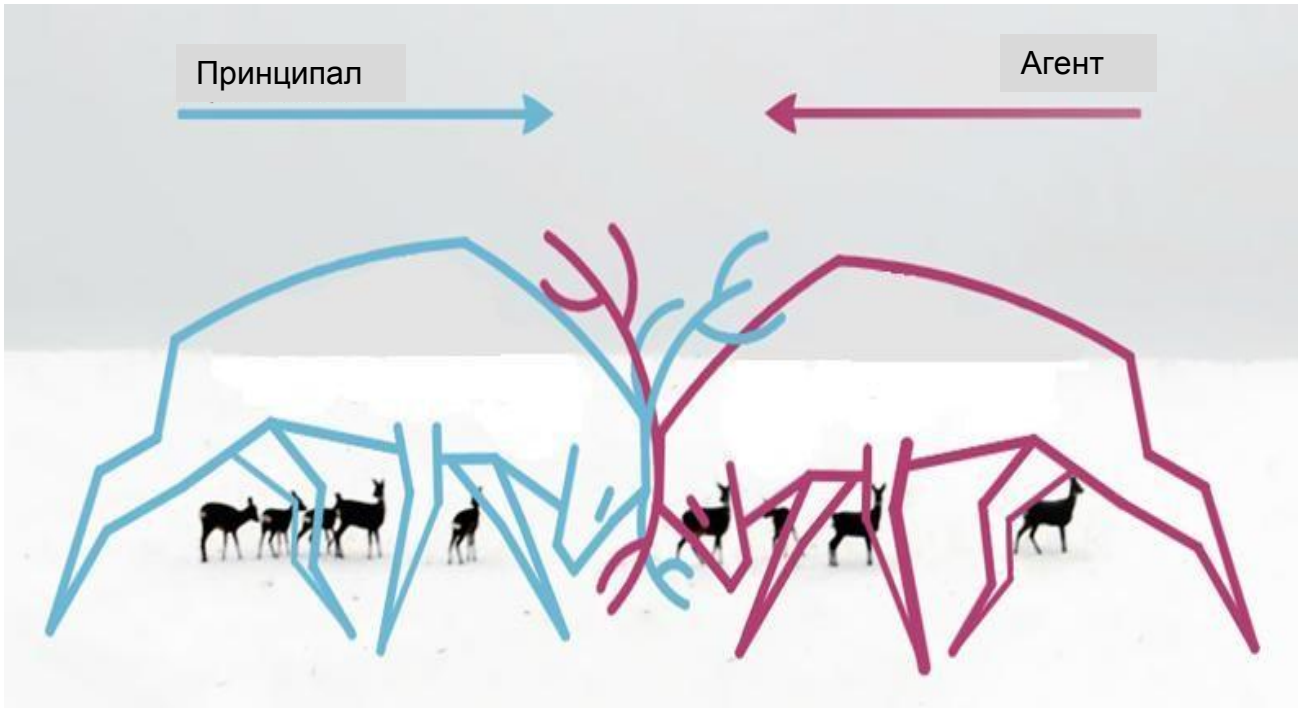

Рис. 2.2. **Зіткнення інтересів учасників корпоративного управління**

У сучасній теорії менеджменту поняття "агентської проблеми" багаторазово розширилося й ускладнилося, оскільки в агентських відносинах бере участь набагато більше сторін, окрім акціонерів і менеджерів. Ця теорія отримала назву "теорії стейкхолдерів". Усі зацікавлені сторони й їх очікування схематично подані на рис. 2.3.

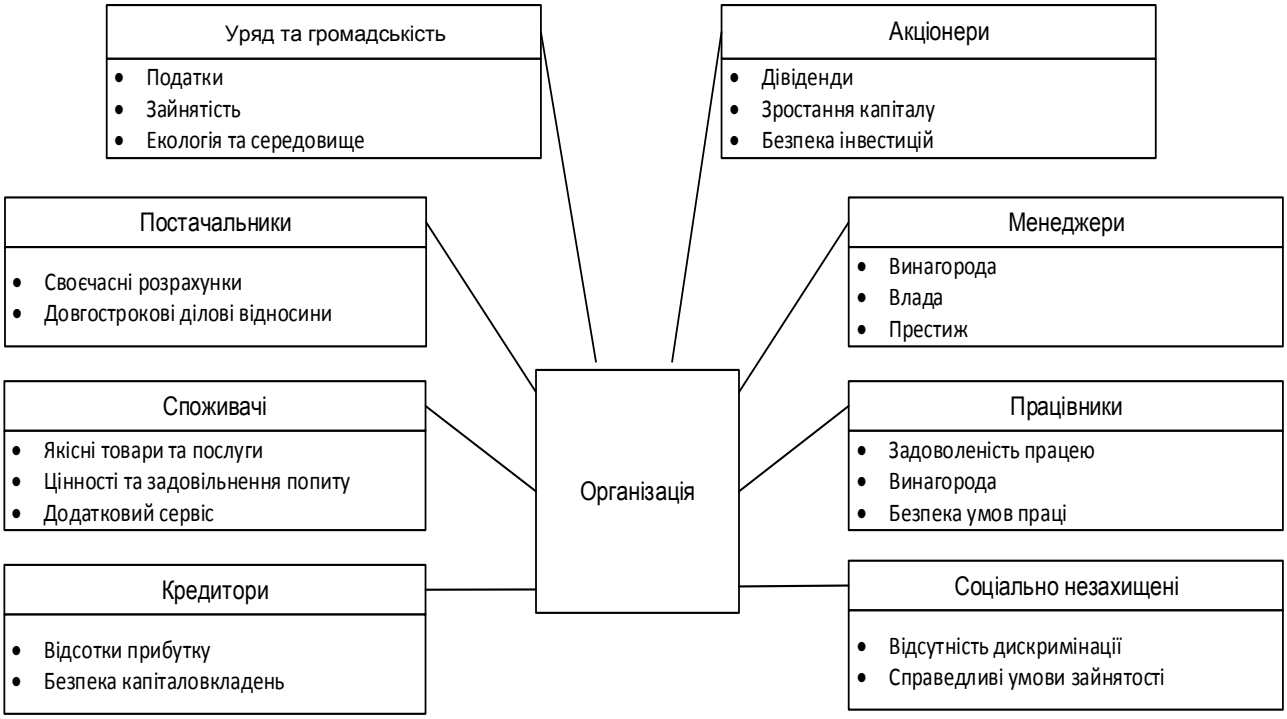

Рис. 2.3. **Групи зацікавлених в діяльності організації сторін і їх очікування**

Зрозуміло, що чим більше зацікавлених груп – тим більше та глибше конфлікт інтересів. Завдання ефективного корпоративного управління – врахувати та збалансувати інтереси всіх стейкхолдерів. Але у менеджменту теж є свої інтереси, а оскільки менеджери теж люди, велика ймовірність того, що вони будуть дотримуватися насамперед своїх інтересів. Перед акціонерами постає необхідність якимось чином змусити менеджерів діяти в інтересах компанії й її акціонерів.

У зв'язку із цим виникають *агентські витрати* – це та величина втрат інвесторів, яка пов'язана з розподілом права власності та контролю. Агентські витрати включають три категорії витрат:

витрати на здійснення контролю над діяльністю менеджерів (перевірки);

витрати на створення організаційної структури, що гальмує небажану поведінку менеджерів (введення в органи управління зовнішніх інвесторів);

альтернативні витрати, які виникають у випадках, коли умови, встановлені акціонерами, обмежують дії менеджерів, що суперечать основній меті – збільшенню багатства.

Крім контролю є й інші механізми, які спонукають менеджерів діяти в інтересах акціонерів:

системи стимулювання на основі показників діяльності компанії;

безпосереднє втручання акціонерів;

загроза звільнення.

Спроби вирішити агентську проблему шляхом збігу інтересів менеджерів і акціонерів призвели до того, що винагорода директорів стала включати великі соціальні пакети та бонуси, які залежать від показників діяльності компанії (наприклад, можливість придбати акції за пільговими цінами або отримувати премії, які безпосередньо залежать від величини чистого прибутку). У свою чергу, це спричинило збільшення ризику шахрайства з боку вищого управлінського персоналу через можливість "правильно" вплинути на показники фінансової звітності, щоб забезпечити відповідний показник чистого прибутку та курс акцій. Виникає "замкнене коло", і необхідно вибудувати чітку систему корпоративного управління, базовану на етичних цінностях, щоб його розірвати.

2.2. Підходи до формування системи фінансово-економічної безпеки організації

Система фінансово-економічної безпеки є невід'ємною складовою корпоративного управління. Формування системи фінансово-економічної безпеки (СФЕБ) – це перш за все створення відповідальних структур, наділених повноваженнями виконувати основний перелік функцій та координування управління фінансово-економічної безпеки (УФЕБ), нести за них відповідальність.

СФЕБ є сукупністю елементів, функціонування яких забезпечує ефективну діяльність у сфері захисту активів організації, здійснення бізнес-процесів і захисту результатів фінансово-господарської діяльності. Ці заходи спрямовані на досягнення мети, тобто планованого результату забезпечення ФЕБ. Управлінські відносини, які виникають у здійсненні таких процесів, – це взаємозв'язки та взаємозалежності елементів даної системи. Зв'язок цих компонентів механізму управління очевидний. СФЕБ відображує структуру УФЕБ, а управлінські відносини встановлюють порядок взаємозв'язків між окремими ланками цієї структури. Таким чином, СФЕБ і управлінські відносини як компоненти механізму УФЕБ є взаємодоповнювальними.

Практики дотримуються різних підходів до побудови СФЕБ, як то: виокремлення незалежного спеціального органу, що розділяє повноваження зі службами внутрішнього аудиту, ризик-менеджменту, юридичною службою, структурою управління персоналом тощо або діє як структура, що об'єднує в єдиний ланцюжок зазначені відділи. Це визначається рядом особливостей – таких, як організаційно-правова форма та розмір організації, інтереси та зацікавленість власників, стратегічні плани, присутність організації на міжнародних ринках, вразливість до факторів зовнішнього середовища.

За підходом до формування СФЕБ організації можна розподілити на такі групи:

організації, в структурі управління яких виділено спеціальні підрозділи (департамент, управління, служба, відділ), яким делеговані функції забезпечення фінансово-економічної безпеки;

організації, в штатній структурі яких є співробітник (професіонал, аналітик, фахівець з фінансово-економічної безпеки), який виконує актуальні для організації функції з фінансово-економічної безпеки; загальне керівництво здійснює директор організації;

організації, в яких функції забезпечення фінансово-економічної безпеки закріплені між департаментами та функціональними підрозділами; відповідальність за їх виконання покладено на керівників відповідних служб;

організації, які не ставлять перед собою спеціальні завдання із забезпечення фінансово-економічної безпеки, а її стан забезпечується рівнем виконання завдань та обов'язків керівників і співробітників.

Організація й управління ФЕБ можуть здійснюватися або самостійно організацією, або незалежним консультантом (найманим професіоналом з ФЕБ). Для самостійного забезпечення ФЕБ організація може створити спеціальний підрозділ.

Практика показує, що малі підприємства найчастіше залучають зовнішні спеціалізовані організації (консалтингові, інформаційні, охоронні тощо), які надають їм інформацію щодо ділового оточення, бізнес-партнерів, проводять на замовлення маркетингове дослідження, здійснюють послуги щодо підбору та навчання персоналу.

Середні підприємства зазвичай використовують комбінований підхід до вирішення завдань УФЕБ: якщо необхідно – замовляють послуги сторонніх організацій, з іншого боку – спираються на можливості власних служб (фінансової, юридичної, маркетингової, аудиту, управління персоналом,

охорони тощо). Але з метою забезпечення ефективності діяльної підрозділів організації доцільне створення власного координаційного підрозділу та призначення керівника, який відповідатиме за ФЕБ.

Для великих компаній створення окремих підрозділів, які відповідають за корпоративну та фінансово-економічну безпеку, і доцільне, і необхідне. А для розроблення пропозицій та виконання консультативних функцій навіть може створюватися Рада з безпеки.

Світові ринки, унікальність продукту, наявність мережі бізнес-одиниць, диверсифікація робочої сили, клієнтів, а також мінливі технологічне та ділове середовища роблять завдання забезпечення безпеки більш складними. Розуміння того, як працює бізнес, є необхідним, але недостатнім для забезпечення належного рівня захисту активів. Це навіть більше, ніж просто усвідомлення необхідності розроблення та реалізації успішної програми захисту активів. Перш за все це розуміння фундаментальних принципів безпеки. Саме тому фахівці з безпеки повинні виконувати завдання із забезпечення захисту активів для будь-якої компанії. А директори компаній не повинні легковажно ставитися до ролі безпеки, оскільки це може загрожувати фінансово-економічними втратами.

Існує багато думок щодо відповідальності СФЕБ за корпоративну безпеку та про те, яким чином вона вписується в корпоративну структуру та корпоративне середовище. Дехто припускає, що, оскільки безпека є функцією комплаєнсу, вона повинна бути частиною більш великої організації комплаєнс-контролю – такої, як аудит або юридичний відділ. Інші доводять, що роль безпеки тісно пов'язана з людьми, і тому безпека повинна стати невід'ємною частиною організації управління персоналом. Хтось вважає, що забезпечення безпеки є невід'ємною складовою операційної діяльності суб'єкта господарювання та має стати частиною його організації та безперервності бізнесу. Усе це вказує на те, що універсального підходу до організації СФЕБ немає. Необхідно знайти ефективні аргументи, щоб закріпити безпеку за будь-якою з наведених функцій або низкою інших.

Так, наприклад, у системі управління ризиками та внутрішнього контролю безпеці відведена роль другої лінії захисту суб'єкта господарювання (рис. 2.4).

Системний внутрішній контроль дозволяє своєчасно виявляти відхилення в роботі бізнес-процесів організації від положень регламентуючих документів. Установлюючи ці відхилення та виявляючи причини їх виникнення, внутрішній контроль сприяє своєчасному розробленню керівниками бізнес-процесів заходів, спрямованих на раціоналізацію їх діяльності.

Рис. 2.4. **Модель трьох ліній оборони суб'єкта господарювання**

Ідея моделі "трьох ліній оборони" полягає в тому, що система внутрішнього контролю суб'єкта господарювання може бути організована порізному – залежно від стадії його розвитку. В Україні модель трьох ліній оборони тільки отримує поширення, належної уваги до організації служби внутрішнього контролю, управління безпекою, ризиками та комплаєнсу не приділяється. Служба внутрішнього контролю асоціюється переважно із внутрішнім аудитом, з перевіркою наявності та використанням активів, ліквідацією заборгованості, з перевіркою якості бухгалтерської (фінансової) звітності й оптимізацією податків і зборів. Очевидно, що цей підхід потребує перегляду. А створення СФЕБ – це можливість об'єднати всі функції управління, спрямовані на забезпечення безпеки й управління ризиками діяльності в єдиний організаційний механізм.

Порядок організації ФЕБ, у тому числі обов'язки та повноваження підрозділів і персоналу організації, залежать від характеру та масштабів діяльності організації, особливостей системи управління. Тому потрібно виходити з таких принципів:

УФЕБ повинна здійснюватися на всіх рівнях управління організацією, у всіх його підрозділах;

у здійсненні УФЕБ повинен брати участь весь персонал організації відповідно до його повноважень і функцій;

корисність УФЕБ повинна бути порівняння з витратами на його організацію та здійснення.

Міжнародний інститут внутрішніх аудиторів сформулював вісімнадцять ключових управлінських принципів, одночасне виконання яких гарантує забезпечення ФЕБ:

1) Органи управління, які правильно організовані та функціонують (Рада директорів і комітети), з потрібною кількістю виконавчих і незалежних директорів, з чітко встановленою процедурою ведення протоколів зустрічей;

2) члени Ради та комітетів, які мають відповідну кваліфікацію та досвід з чітким усвідомленням своєї ролі в управлінні та розумінням бізнесу компанії, а також володіють незалежними й об'єктивними судженнями;

3) Рада з належними повноваженнями, фінансуванням і ресурсами для проведення незалежних запитів;

4) усвідомлення членами Ради необхідності прозорого ведення бізнесу;

5) організаційна структура, що дозволяє вимірювати досягнення організації в цілому та окремих її співробітників;

6) організаційна структура, що сприяє виконанню стратегічних цілей;

7) наявність управлінської політики для операцій з ключової діяльності;

8) чіткі межі відповідальності та підзвітності;

9) ефективна взаємодія між Радою, комітетами, виконавчим керівництвом, внутрішніми та зовнішніми аудиторами й іншими провайдерами гарантій;

10) належний нагляд з боку керівництва над встановленням і підтриманням строгих контролів;

11) компенсаційні пакети вищого керівництва відповідають етичним цінностям, цілям, стратегії та контрольному середовищу організації, а також сприяють належній діяльності керівництва;

12) інформування та підтримка етики, цінностей організації, а також відповідний тон керівництва в організації, включаючи створення атмосфери, в якій працівники без остраху звільнення можуть виражати зворотний зв'язок керівництва, відстежувати та досліджувати потенційні конфлікти інтересів;

13) ефективне використання внутрішніх аудиторів, засноване на їх незалежності, адекватності їх ресурсів обсягу робіт, а також ефективності діяльності;

14) чітке визначення ділянок відповідальності; застосування політики управління ризиками та процесами;

15) ефективне використання зовнішніх аудиторів, засноване на їх незалежності, адекватності їх ресурсів обсягу робіт;

16) прозоре розкриття ключової інформації для зацікавлених учасників організації;

17) розкриття управлінських процесів, порівняння їх із загальноприйнятими національними кодексами чи найкращою практикою;

18) нагляд за операціями з пов'язаними сторонами та конфліктом інтересів.

Для виконання цих принципів необхідна чітко вибудована система контролю в організації, елементом якої є СФЕБ.

СФЕБ має відповідати основним характеристикам, притаманним системам управління такого рівня, а саме: цілісності, органічній внутрішній єдності; наявності інтегральних властивостей, які не утворюють систему елементів; здатності до саморегуляції.

Об'єктом ФЕБ виступає корпоративне середовище – все те, на що спрямовані зусилля щодо забезпечення ФЕБ. До таких *об'єктів* слід віднести:

різні види діяльності та бізнес-процеси (виробничі, комерційні, постачальницькі, управлінські та ін.);

майно та ресурси (фінансові, товарно-матеріальні цінності, техніко-технологічні, інформаційні, людські та ін.);

акціонерів і їх економічні інтереси;

відносини на різних рівнях (мікро- та макрорівень, ринковий або ділового середовища, регіональний та галузевий) з діловими партнерами, контрагентами, споживачами, регіональними та галузевими структурами, контролюючими та фіскальними службами, представниками органів влади.

Суб'єктами ФЕБ організації є ті особи, підрозділи, служби, органи, відомства, установи, які безпосередньо виконують функції зі забезпечення та підтримки безпечного стану її діяльності. Як правило, до *суб'єктів ФЕБ* відносять структури, які можна класифікувати за різними ознаками залежно від:

приналежності: суб'єкти внутрішні, які займаються цією діяльністю безпосередньо в організації, і зовнішні суб'єкти (рис. 2.5);

безпосередньої участі: спеціальні суб'єкти та весь інший персонал;

впливу на об'єкт безпеки: суб'єкти прямого та непрямого призначення;

легітимності: офіційні органи та кримінальні структури;

підпорядкованості: державні та недержавні органи.

Рис. 2.5. **Суб'єкти СФЕБ організації** [26]

До *внутрішніх суб'єктів* належать ті, які входять у структуру самого організації та вирішують завдання щодо забезпечення її безпеки. До складу цієї групи входять спеціальні суб'єкти (підрозділи ФЕБ, внутрішнього аудиту, комплаєнсу та ризик-менеджменту, охорона тощо), а також весь інший персонал, який дбає про ФЕБ своєї організації.

До *зовнішніх суб'єктів* належать ті суб'єкти, які знаходяться за межами організації та не підпорядковуються її керівництву. Це насамперед державні органи, які створюють умови для забезпечення безпеки суб'єктів господарювання.

До них відносять:

законодавчі органи – приймають закони, що створюють правову основу діяльності щодо забезпечення безпеки на рівні держави, регіону, організації й особистості;

виконавчі органи влади – проводять політику, деталізують механізми безпеки;

судові органи – забезпечують додержання законних прав організації та її співробітників;

державні інститути – здійснюють охорону кордонів, митний, валютно-експортний, податковий контроль і т. п.;

правоохоронні органи – ведуть боротьбу з правопорушеннями та злочинами;

систему науково-дослідних установ – реалізує завдання наукового дослідження проблем безпеки та підготовки кадрів.

З початком ринкових реформ паралельно з державними стали утворюватися недержавні організації, агентства, установи. Це різні приватні охоронні та детективні організації, аналітичні центри, інформаційні служби, навчальні, наукові та консультаційні організації і т. і. Вони, як правило, за плату надають послуги з охорони та захисту об'єктів, що забезпечують захист інформації, комерційної таємниці, накопичують і подають інформацію про конкурентів, ненадійних партнерів і т. і.

Графічно систему безпеки організації представляють як тривимірну модель. Доповнюючи та розкриваючи зміст УФЕБ, така модель матиме вигляд (рис. 2.6).

Як будь-яка система управління, СФЕБ має охоплювати сукупність всіх елементів, підсистем і комунікацій між ними, а також процесів, які забезпечують цілеспрямоване забезпечення ФЕБ компанії.

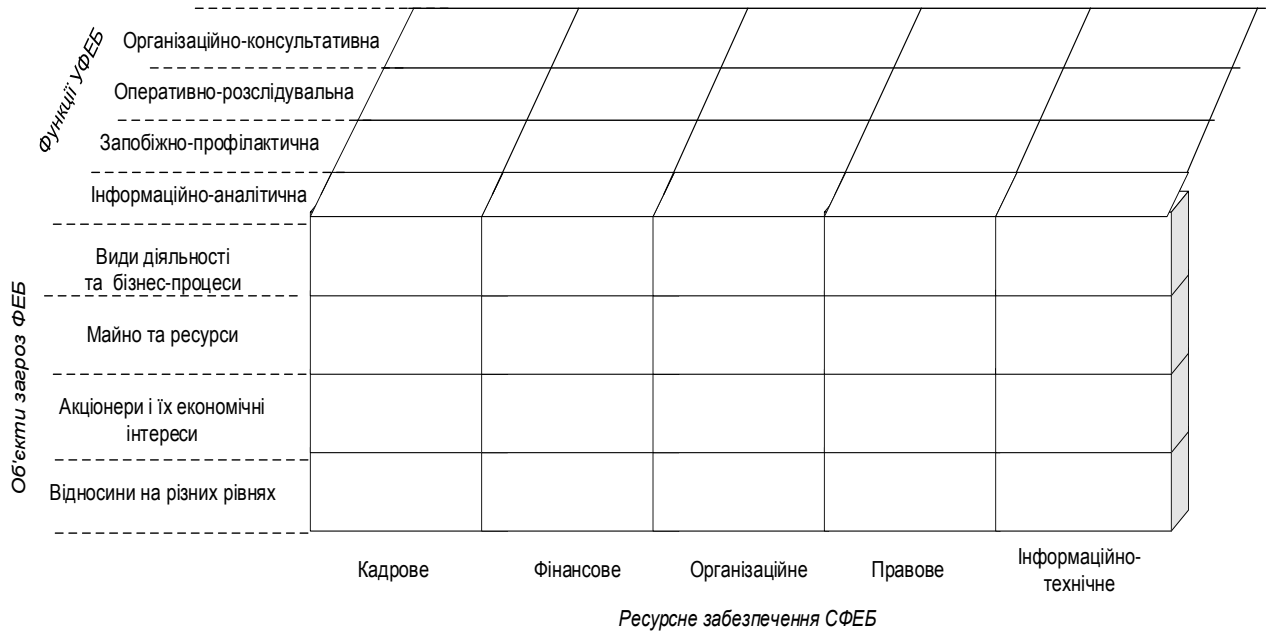

Рис. 2.6. **Тривимірна модель СФЕБ організації**

Така система управління базується на трьох основних складових: інформаційній підтримці процесів розроблення та реалізації рішень; наборі типових бізнес-процесів для вирішення поставленого завдання; системі активізації персоналу.

2.3. Компоненти системи фінансово-економічної безпеки організації і їх взаємоузгодженість з безпекою зовнішнього середовища

Отже, **СФЕБ** – це комплекс професійних засобів і методів у сукупності з органами, до компетенції яких входить забезпечення ФЕБ організації (бізнесу, підприємства, компанії). СФЕБ створює необхідні умови для ефективного ведення бізнесу, підтримує та сприяє стратегічному розвитку, дозволяє своєчасно реагувати на виявлені або потенційні загрози в роботі бізнес-процесів, мінімізувати їх вплив, попереджати можливі злочини та противоправні дії щодо активів організації, запобігати можливим фінансово-економічним втратам.

Компоненти системи фінансово-економічної безпеки організації – це ті її елементи, блоки й одиниці, які виконують певні самостійні функції, а в поєднанні забезпечують виконання повного циклу функцій з УФЕБ. Такі елементи ув'язують організаційні елементи в єдиний механізм і наділяють СФЕБ єдиними цілями та цінностями.

Ураховуючи значущість і місце СФЕБ в управлінні організацією, формування СФЕБ відповідно до системних і комплексних підходів має відбуватися таким чином:

такі компоненти СФЕБ, як концепція, політика, програма, розроблюються на базі наукової теорії управління безпекою одночасно з розробленням основноутворювальних для організації положень (бачення, місії, кредо, статут тощо) в цілому та не суперечать їм;

згідно з цими документами створюються спеціальні органи СФЕБ, ядром якої є підрозділ ФЕБ. У діяльності підрозділу ФЕБ істотна увага приділяється взаємодії з іншими підрозділами, організації їх діяльності таким чином, щоб найбільш ефективно та гарантовано забезпечити фінансово-економічну безпеку;

згідно з тими ж документами виробляються та враховуються вимоги фінансово-економічної безпеки до оргструктури та фінансово-господарської діяльності, формується оргструктура підрозділу, регламентується діяльність організації.

СФЕБ є невід'ємною складовою механізму управління організацією, а тому має бути підпорядкована виконанню стратегічних цілей та місії організації, втілювати її цінності. Бачення, місія та кредо організації мають ув'язувати всі рівні управління й організаційні функції.

Бачення можна віднести до демонстрації стратегічної мети, напряму діяльності, світогляду, цінностей співробітників і насамперед – керівника організації. Це ідеальна картина майбутнього, в якій організація могла б діяти за найсприятливіших умов й орієнтири, які організація не розраховує досягти в найближчому періоді, але допускає наближення до них. Визначення бачення – це стислий вислів, який має бути:

простим, чітким, щирим, лаконічним, зрозумілим для працівників і надихати їх;

заслуговувати довіри, ототожнювати етичні цінності з поведінкою;

слугувати орієнтиром, якого компанія прагне досягти в довгостроковій перспективі.

Місія організації – це соціально значуща мета. Це набір концептуальних положень, що в узагальненій формі розкривають те, чому вирішила присвятити себе організація. Місія є об'єднавчим початком різноманітних цілей організації, оскільки її змістовність знаходить прояв у цінності, віруванні та принципи (філософії), розкриваючи призначення та сенс існування організації, показує визначеність і передбачуваність організаційної поведінки в динамічно мінливому середовищі. У процесі розроблення місії враховуються інтереси засновників, власників, працівників, клієнтів (покупців), партнерів, держави та групові інтереси.

У лаконічному формулюванні поняття "місії" акцент ставиться на таких компонентах:

цінності, які відрізняють дану організацію від інших і які визначають цільові орієнтири;

основні продукти (послуги), що пропонуються організацією;

відмінні можливості та способи здійснення діяльності (технології, з допомогою яких організація гарантує досягнення цілей і виживання в довгостроковій перспективі).

Кредо (філософія, переконання) – це публічна заява про місію та цілі, про найдорожчі цінності для організації. Формулювання кредо не претендує на повноту подання цільових орієнтирів, але містить послання до тих, хто пов'язаний з організацією, інформує про ключові цінності. Кредо – це те, що додає цінності продукції та послугам організації. Це те, що внутрішні та зовнішні клієнти організації очікують від неї.

Прописані бачення, місія та переконання знаходять своє відображення та продовження в стратегічних, тактичних і річних бізнес-планах організації й є основою побудови програми захисту її активів. Вони також є базовими для розроблення та складання концепції та політики у сфері ФЕБ.

Концепція та політика в сфері корпоративної безпеки, зокрема ФЕБ, розробляються з урахуванням наукової теорії безпеки одночасно з розробленням основних положень для організації (таких, як стратегічне бачення, місія, статут) і не суперечать їм. На основі концепції та політики корпоративної безпеки створюється підрозділ ФЕБ, що є ядром СФЕБ, виробляються і враховуються режими безпеки, вимоги до оргструктури та фінансово-господарської діяльності.

Концепція фінансово-економічної безпеки організації – це офіційний документ, який надає повне уявлення про систему сервісу та підтримки розвитку організації, захисту активів, місце УФЕБ, її обґрунтованість. Концепція ФЕБ організації може прописуватися окремо або бути частиною концепції корпоративної безпеки**.** Вона не має чітко визначеного змісту; її складають, як правило, у великих компаніях, підприємствах і організаціях. Найчастіше додержуються такої *структури концепції безпеки*.

1. Загальні положення. У цьому розділі доцільно розкрити понятійний апарат, дати визначення основних термінів, визначити місце ФЕБ.

2. Цілі та завдання. Особливу увагу слід звертати на ув'язування цілей і завдань УФЕБ зі стратегічними планами організації.

3. Принципи й основоположні елементи. У розділі розкриваються основні принципи організації та функціонування корпоративної безпеки; визначаються чіткі елементи СФЕБ, які надалі є основою розподілу відповідальності та формування організаційної структури УФЕБ.

4. Характеристика основних видів загроз, ризиків організації, її сталого розвитку. У розділі окреслюються реальні та потенційні загрози, ризики для діяльності організації.

5. Основні об'єкти захисту. У розділі визначаються всі об'єкти організації, які підлягають захисту в СФЕБ від реальних і потенційних загроз, ризиків і протиправних посягань.

6. Правові основи організації та діяльності системи забезпечення безпеки. Правові основи УФЕБ визначаються відповідними положеннями Конституції України, законами держави й іншими нормативними актами.

7. Інженерно-технічні засоби забезпечення безпеки. У розділі розкриваються підходи до використання у СФЕБ організації сучасних інженерно-технічних засобів захисту від протиправних дій, інформаційних ресурсів, матеріальних цінностей, персоналу, території, будівель і споруд, транспортних засобів.

8. Управління безпекою. У розділі розкриваються основні принципи, суб'єкти та механізми УФЕБ, а також організація та проведення постійного контролю над СФЕБ з боку керівника (власника) організації.

9. Напрями та механізми взаємодії у процесі забезпечення безпеки. У розділі визначаються основи такої організації взаємодії в УФЕБ.

10. Фінансування організації та функціонування системи безпеки. У розділі визначаються основні принципи та порядок фінансування організації УФЕБ. Дається фінансово-економічне обґрунтування реалізації концепції, визначається бюджет, який витрачається на забезпечення безпеки.

11. Програма створення системи безпеки. Програма створення СФЕБ повинна передбачати пріоритети реалізації найбільш важливих і актуальних напрямів забезпечення безпеки з урахуванням реальних загроз і ризиків, а також виділених фінансових ресурсів. Визначається, що і в якій послідовності буде реалізовуватися у сфері безпеки, який фінансово-економічний та соціальний ефект планується отримати на кожному етапі реалізації концепції.

Політика фінансово-економічної безпеки організації містить опис загальних дій і орієнтирів прийняття рішень, які спрямовані на досягнення цілей УФЕБ і визначають відношення з людьми. Як і концепція безпеки, політика – це офіційний документ, який не має чітко визначеної структури. Як окремий документ політика безпеки, розробляється за відсутності концепції безпеки, і в такому випадку рекомендується додержуватися такої її структури.

1. Загальні положення, що розкривають базові елементи цього документу. Основне призначення політики безпеки – надати уявлення про принципи, які є в основі дій щодо забезпечення безпеки, розподіл відповідальності за дотримання політики безпеки між структурними підрозділами організації й особами, які відповідають за виконання політики безпеки та прийняття рішень з УФЕБ.

2. Принципи політики безпеки, зокрема ФЕБ. Це основні правила, яких слід додержуватися на всіх рівнях управління організацією для забезпечення виконання цілей та заходів з безпеки, а саме:

неприпустимість корупції та зловживань у ході здійснення, виробничої та будь-якої іншої діяльності;

безумовне дотримання вимог чинного законодавства, внутрішніх організаційно-розпорядчих і виробничих документів усіма суб'єктами забезпечення ФЕБ, незалежно від займаної посади, стажу роботи, статусу й інших взаємовідносин з організацією;

заходи з реагування та відповідальність, передбачені чинним законодавством, а також внутрішніми організаційно-розпорядчими та виробничими документами суб'єкта господарювання;

інформація щодо осіб, притягнутих до відповідальності за вчинення правопорушень і зловживань, пов'язаних з корупцією чи перевищенням службового становища.

3. Основоположні елементи політики. Це основні напрями забезпечення ФЕБ: взаємовідносини із працівниками, з контрагентами, з зовнішніми сторонами, зокрема державними контролюючими органами, громадськістю та конкурентами; дотримання конфіденційності, ведення управлінського та бухгалтерського обліку; оцінювання ризиків у рамках реалізації політики безпеки.

4. Ресурси та методи (прийоми та способи дії) забезпечення безпеки. Надається повне уявлення про фінансове забезпечення, формування кадрових і організаційних засобів, систему правових засобів, залучення технічних, інформаційних та інтелектуальних засобів. Наведемо короткий конкретний перелік цих методів [17]:

технічні – спостереження, контроль, ідентифікація;

організаційні – створення зон безпеки, режим, розслідування, пости, патрулі;

інформаційні – складання детективами характеристик на працівників, аналітичні матеріали й обліки конфіденційного характеру;

фінансові – матеріальне стимулювання співробітників, які мають досягнення у забезпеченні безпеки, грошове заохочення інформаторів;

правові – судовий захист законних прав та інтересів, сприяння правоохоронним органам;

кадрові – підбір, розстановка та навчання кадрів, які забезпечують безпеку організації, їх виховання;

інтелектуальні – патентування, ноу-хау.

5. Розподіл відповідальності між структурними підрозділами за дотримання принципів безпеки. У діяльності підрозділу ФЕБ істотна увага приділяється взаємодії з іншими підрозділами, організації їх діяльності таким чином, щоб найбільш ефективно та гарантовано забезпечити фінансово-економічну безпеку організації.

УФЕБ – це здійснення сервісу та підтримки функціонування та розвитку організації, її фінансово-господарської діяльності: відповідно, всі підрозділи організації й її співробітники важливі для УФЕБ. У структурі

великих організацій є декілька відділів, з якими УФЕБ повинно працювати в тісному контакті, взаємодіяти та спиратися на інформацію цих відділів, щоб успішно виконувати свої функції щодо забезпечення ФЕБ усієї організації. Ці відділи є невід'ємними елементами СФЕБ, їх діяльність спрямована на забезпечення гарантій того, що програмні заходи щодо забезпечення ФЕБ будуть реалізовані успішно. У великих компаніях такими відділами є (рис. 2.7).

Рис. 2.7. **Відділи корпоративного середовища СФЕБ**

1. *Управління з етики* (департамент, відділ) – підрозділ, який підпорядковується генеральному директору й управляється відповідним директором. Цей підрозділ відповідає за роботу, навчання та забезпечення підготовки працівників з питань етики. До його компетенції може входити управління питаннями на гарячій лінії. Гаряча лінія з питань етики створюється для прийому скарг (як правило, анонімних) і проведення розслідувань у зв'язку з інформацією про зловживання з боку працівників або інших осіб, які можуть бути пов'язані з організацією. Якщо абоненти залишають свої імена, то ця інформація зберігається в закритому вигляді в відділі етики. Якщо прийнята інформація потребує більш детального розслідування (в тому числі збирання доказів, проведення співбесід і допитів),

директор з питань етики надає цю інформацію в службу безпеки, у відділ розслідувань або оперативний відділ. Служба безпеки здійснює запити, повертає результати директорові з питань етики, який є внутрішнім замовником. Директор з питань етики проводить щомісячні збори з питань етики з представниками підрозділів безпеки, юридичного, управління персоналом і кадрами, внутрішнього аудиту.

2. *Відділ внутрішнього аудиту*. Робота внутрішнього аудиту спрямована на те, щоб гарантувати, що компанія працює, а її працівники виконують свої обов'язки відповідно до чинного національного та місцевого законодавства, корпоративних політик і процедур. Підрозділи внутрішнього аудиту та ФЕБ обмінюються інформацією, що представляє взаємний інтерес.

3. *Юридичний відділ*. Цей відділ відповідає за виконання всіх стандартних обов'язків, пов'язаних з наданням консультацій та допомоги професіоналів ФЕБ на вимогу або за необхідності.

4. *Управління персоналом і відділ кадрів*. Як випливає з назви підрозділів, вони займаються питаннями співробітників (такими, як професійна відповідність, скарги співробітників на своїх менеджерів) і надають указівки керівникам про дисципліну працівників, організують їх перепідготовку, навчання, атестацію тощо.

Більшість компаній мають подібні структури, які формують їх корпоративне середовище. Корпоративне середовище націлене на стратегічні орієнтири й управління загальною ефективністю бізнесу. Основні зусилля спрямовані на стратегічні напрями розвитку – зробити компанію прибутковою та збільшити акціонерну вартість. Підрозділи корпоративного середовища не розроблюють продукт компанії, але приймають участь у поточній діяльності суб'єкта господарювання та його бізнес-одиниць. Функції цих підрозділів – розробляти політику, забезпечувати виконання та контроль дотримання та виконання довірених їм зобов'язань перед Радою директорів та акціонерами.

У свою чергу, корпоративне управління, як правило, не приймає участь у повсякденній діяльності підприємства, але в разі потреби, (як-то: недостатньо ефективна робота підрозділів корпоративного середовища) будуть втручатися в їх роботу.

Не менш важливе місце в СФЕБ організації займає *корпоративна культура*. ФЕБ є віддзеркаленням її культури, тих етичних норм і правил, які є значущими для організації. Будь-яка організація, незалежно від

розмірів, має свою особливу культуру. Так, для одних суб'єктів господарювання нормальною практикою є сприяння та заохочення конкуренції між окремими бізнес-одиницями та підрозділами. За такої моделі суперництво, а також агресивна поведінка заохочуються та винагороджуються. В інших організаціях робота в команді є пріоритетом. Як вказують соціологи, культура організації побудована на поведінкових нормах, які визначаються як набір очікувань щодо того, як людина поведе себе в тій чи іншій ситуації. Культура в межах організації може відрізнятися між корпоративним та операційним середовищем так само, як і між компаніями. Субкультури малої організації можуть істотно відрізнятися від такої у великій. Розуміння культури організації має важливе значення для досягнення успіху.

2.4. Функції системи фінансово-економічної безпеки організації

Функціонально СФЕБ спрямована на: забезпечення успішної діяльності організації в умовах нестабільності (як внутрішньої, так і зовнішньої); своєчасне розпізнавання та запобігання потенційним загрозам; захист усіма законними способами економічних інтересів акціонерів, директорів і менеджменту, співробітників, клієнтів і контрагентів від загроз і ризиків; поширення концепції безпеки та сприяння сталому функціонуванню та розвитку організації. Налагоджена СФЕБ дозволяє припиняти різного роду зловживання (наприклад, розкрадання грошових коштів або товарно-матеріальних цінностей та ін.), запобігати псуванню чи знищенню активів суб'єкта господарювання, витоку конфіденційної інформації, а також спробам нанесення шкоди або отримання секретних відомостей за допомогою IT-технологій.

СФЕБ як така виконує **чотири основні функції**.

1. *Запобіжно-профілактичну функцію* – це робота на попередження прояву загроз, основними заходами безпеки є:

вивчення структури та функцій підрозділів організації з метою ідентифікації ризиків, що виникають під час їх здійснення, та відповідної розстановки сил і засобів безпеки;

здійснення організаційно-правового впливу на діяльність персоналу та клієнтів суб'єкта господарювання через розроблення та впровадження стандартів безпеки;

підбір, перевірка та контроль роботи персоналу, розроблення відповідної кадрової політики та програм стимулювання персоналу;

охорона організації: об'єктів, грошей, матеріальних цінностей, комунікацій, обладнання, вантажів, персоналу;

запобігання розкраданню фінансових і матеріально-технічних коштів, знищенню майна та цінностей;

атестація приміщень, спеціального обладнання окремих із них, облік носіїв інформації обмеженого доступу, захист засобів зв'язку, організація службового та спеціального діловодства;

виявлення негативних тенденцій, причин та умов напруженості, попередження та локалізація конфліктів, інструктаж персоналу з питань безпеки, формування почуття відповідальності за дотримання встановленого режиму;

запобігання порушенню роботи технічних засобів забезпечення виробничої діяльності, зокрема засобів інформатизації, а також запобігання збитку персоналу організації;

запобігання розголошенню, просочуванню інформації та несанкціонованому доступу до джерел конфіденційної інформації;

контроль дотримання персоналом організації режимних вимог, виявлення їх порушень і вжиття заходів до порушників;

упровадження технічних засобів контролю доступу, візуального контролю, охоронної та пожежоохоронної сигналізації, апаратних і програмних засобів забезпечення збереження конфіденційної інформації;

формування позитивного іміджу;

розроблення заходів відповідальності за порушення встановлених правил забезпечення ФЕБ.

2. *Інформаційно-аналітичну функцію* – через проведення спеціальних аналітичних процедур, збирання й обробку інформації, а саме:

організацію та проведення конкурентної розвідки, формування інформаційних ресурсів і баз даних;

інформаційно-аналітичні дослідження клієнтів і контрагентів суб'єкта господарювання;

фіксування та систематизацію даних про внутрішні та зовнішні загрози ФЕБ;

аналіз стану безпеки, прогнозування тенденцій її розвитку та планування заходів щодо її вдосконалення;

підготовку аналітичних звітів щодо стану ФЕБ, підтримку прийняття управлінських рішень.

3. *Оперативно-розслідувальну функцію* – через виконання спеціальних заходів, а саме:

взаємодію із контролюючими та правоохоронними органами з питань запобігання протиправним посяганням на власність, персонал та імідж організації та припинення їх;

протидію недобросовісній конкуренції, зокрема промисловому шпигунству;

проведення службових розслідувань за фактами протиправних дій персоналу, шахрайства, зловживання службовим положенням, порушення встановлених правил з безпеки в роботі;

проведення заходів щодо дезінформації конкурентів, впливу на недобросовісних клієнтів, боржників і зловмисників з метою відшкодування організації втрат, які понесені через вину цих сторін.

4. *Організаційно-консультативну функцію* – через надання експертно-консультативної допомоги на всіх рівнях управління організацією щодо:

удосконалення системи управління організацією;

визначення оптимальних для забезпечення безпеки сил і засобів, а також їх фінансового забезпечення;

уточнення нормативної та методичної бази;

установлення та підтримку системи заходів безпеки, визначення повноважень і відповідальності, розподілу обов'язків посадових осіб щодо забезпечення ФЕБ;

удосконалення операційної та комерційної діяльності;

поширення концепції безпеки серед керівного складу та персоналу суб'єкта господарювання.

Кожна з виділених функцій (запобіжно-профілактична, інформаційно-аналітична, оперативно-розслідувальна й організаційно-консультативна) є значущою. У комплексі вони формують єдиний механізм забезпечення захищеності організації від дестабілізаційних факторів, створюють умови для ефективної реалізації основних інтересів та цілей статутної діяльності.

2.5. Контролюючі органи фінансово-економічної безпеки організацій і їх функції

Перелік органів, які контролюють діяльність суб'єктів господарювання, досить широкий. Федерація роботодавців України склала реєстр із сімдесяти держорганів, які можуть проводити перевірки організацій [53].

Слід зазначити, що проведення перевірок суб'єктів господарювання в Україні має під собою доволі складне правове підґрунтя. За словами експертів [54], застарілість, неузгодженість і велика кількість нормативних документів, що регулюють проведення перевірок контролюючими органами, є чинником, що призводить до суперечок між господарюючими суб'єктами та контролюючими органами. Така ситуація викликає численні скарги на дії контролюючих органів від суб'єктів господарювання до органів влади всіх рівнів.

Стаття 19 Господарського кодексу України передбачає, що органи державної влади та посадові особи, уповноважені здійснювати державний контроль і державний нагляд за господарською діяльністю, їх статус, загальні умови та порядок здійснення контролю та нагляду визначаються законами.

Загальні правила проведення перевірок суб'єктів господарювання органами державного нагляду (контролю) регулюються Законом України "Про основні засади державного нагляду (контролю) у сфері господарської діяльності" [50]. Цим Законом регулюється діяльність уповноважених законом центральних органів виконавчої влади, їх територіальних органів, державних колегіальних органів, органів місцевого самоврядування в межах законних повноважень щодо виявлення та запобігання порушенням вимог законодавства суб'єктами господарювання та забезпечення інтересів суспільства (зокрема належної якості продукції, робіт і послуг, прийнятного рівня безпеки для населення, сприятливого навколишнього природного середовища).

Контроль за діяльністю, яка не підпадає під дію Закону, регламентується профільним законодавством. Закон не поширюється на відносини, що виникають під час здійснення заходів щодо: контролю органами державної фіскальної служби; валютного контролю; державного експортного контролю; контролю за дотриманням бюджетного законодавства; банківського нагляду; державного контролю за дотриманням законодавства про захист економічної конкуренції; державного нагляду за дотриманням вимог ядерної безпеки; державного нагляду (контролю) в галузі цивільної авіації; проведення оперативно-розшукової діяльності, дізнання, прокурорського нагляду, досудового слідства та правосуддя; державного архітектурно-будівельного контролю (нагляду); державного нагляду та контролю за додержанням законодавства про працю та зайнятість населення.

Законом визначено два типи заходів державного нагляду (контролю) – плановий та позаплановий, які можуть відрізнятися за видами (перевірка, ревізія, обстеження, огляд тощо). Водночас Законом встановлені єдині граничні терміни тривалості проведення планових і позапланових заходів.

Одним із головних надбань Закону є те, що державний нагляд (контроль) у сфері господарської діяльності має здійснюватися залежно від ступеня її ризику, тобто ймовірності виникнення внаслідок діяльності суб'єкта господарювання негативних наслідків для здоров'я громадян і безпеки навколишнього середовища.

Відповідно до положень Закону з метою оптимального розподілу та використання ресурсів органів державного нагляду (контролю) та запобігання порушенню вимог законодавства орган державного нагляду (контролю) повинен визначити критерії віднесення суб'єктів господарювання до трьох груп ризику з огляду на його ступінь: високий, середній чи незначний.

Законом запроваджено прозорий порядок здійснення державного нагляду (контролю), відповідно до якого плановий або позаплановий захід може бути здійснений за умови видання органом державного нагляду (контролю) належних, визначених Законом розпорядчих документів, а саме: наказу на проведення заходу й оформленого відповідним чином посвідчення (направлення), в якому зазначаються, зокрема, номер і дата наказу, на виконання якого проводиться захід; дати початку та закінчення заходу; перелік посадових осіб, які беруть участь у заході тощо.

Ще одним надзвичайно значущим досягненням Закону, яке неможливо залишити поза увагою, є те, що в ньому регламентовані не лише права й обов'язки органів, що уповноважені державою на здійснення заходів нагляду (контролю). Значну увагу у Законі приділено захисту прав суб'єктів господарювання, господарська діяльність яких перевіряється. Метою такого захисту є недопущення незаконного втручання та перешкоджання господарській діяльності з боку органів державної влади, їх посадових осіб під час здійснення ними державного нагляду (контролю).

Так, суб'єкт господарювання може відмовити представникові перевіряючого органу у здійсненні планового або позапланового заходу в тому разі, якщо керівнику суб'єкта господарювання або уповноваженій ним особі не пред'явлено належним чином оформленого посвідчення та службового посвідчення, що засвідчує посадову особу органу державного нагляду (контролю).

Також з метою захисту своїх прав суб'єкти господарювання, діяльність яких перевіряється, мають право фіксувати процес здійснення планового або позапланового заходу чи кожну окрему дію засобами аудіо-, відеотехніки та залучати в ході здійснення заходів державного нагляду (контролю) третіх осіб – як юридичних, так і фізичних (адвокатів, аудиторів, членів громадських організацій тощо). Причому встановлено, що присутність керівника чи заступника керівника або уповноваженої особи суб'єкта господарювання під час здійснення органом державного нагляду (контролю) планового або позапланового заходу обов'язкова.

До того ж Законом передбачено: якщо норма закону чи іншого нормативно-правового акту, виданого відповідно до закону, або норми різних законів чи нормативно-правових актів допускають неоднозначне множинне трактування прав та обов'язків суб'єктів господарювання або органів державного нагляду (контролю) й їх посадових осіб, що дозволяє приймати рішення як на користь суб'єкта господарювання, так і на користь органу державного нагляду (контролю), то рішення повинно прийматися на користь суб'єкта господарювання.

До органів, що позиціонують себе як такі, на які не поширюється дія Закону "Про основні засади державного нагляду (контролю) у сфері господарської діяльності" [50], але які є **контролюючими органами,** належать:

органи Державної фіскальної служби України – забезпечують формування єдиної державної податкової, державної митної політики в частині адміністрування податків і зборів, митних платежів і реалізації єдиної державної податкової, державної митної політики; проводять формування та реалізацію державної політики з адміністрування єдиного внеску на загальнообов'язкове державне соціальне страхування та політику у сфері боротьби з правопорушеннями у процесі застосування податкового та митного законодавства, а також законодавства з питань сплати єдиного внеску;

Державна санітарно-епідеміологічна служба Міністерства охорони здоров'я України – забезпечує реалізацію державної політики у сфері санітарного й епідемічного благополуччя населення;

Пенсійний фонд України – забезпечує реалізацію державної політики з питань пенсійного забезпечення та ведення персоніфікованого обліку надходжень від сплати єдиного внеску на загальнообов'язкове державне соціальне страхування;

Фонд соціального страхування з тимчасової втрати працездатності є самоврядною некомерційною установою, яка здійснює керівництво

й управління загальнообов'язковим державним соціальним страхуванням у зв'язку з тимчасовою втратою працездатності та витратами, зумовленими похованням;

Фонд соціального страхування від нещасних випадків на виробництві та професійних захворювань України – некомерційна самоврядна установа, яка забезпечує реалізацію законодавства в сфері загальнообов'язкового державного соціального страхування від нещасних випадків на виробництві та професійних захворювань;

органи Державної служби зайнятості України – забезпечують реалізацію державної політики у сфері зайнятості населення та трудової міграції;

Фонд соціального захисту інвалідів є бюджетною установою, яка в межах своєї компетенції забезпечує реалізацію заходів щодо забезпечення зайнятості та працевлаштування інвалідів, виконання програм щодо соціального захисту інвалідів;

Антимонопольний комітет України – забезпечує державний захист конкуренції у підприємницькій діяльності;

Державна фінансова інспекція України – забезпечує реалізацію державної політики у сфері державного фінансового контролю;

органи Міністерства внутрішніх справ України, яке є головним у системі центральних органів виконавчої влади у формуванні та реалізації державної політики у сфері захисту прав і свобод людини та громадянина, власності, інтересів суспільства та держави від злочинних посягань, у боротьбі зі злочинністю, розкритті та розслідуванні злочинів, охороні громадського порядку, забезпеченні громадської безпеки, безпеки дорожнього руху, а також з питань формування державної політики у сферах міграції (імміграції й еміграції), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів.

Особливе місце в системі контролюючих органів ФЕБ суб'єктів господарювання відіграє Державна служба фінансового моніторингу України (Держфінмоніторинг України), яка є центральним органом виконавчої влади зі спеціальним статусом щодо питань фінансового моніторингу. У своїй діяльності Держфінмоніторинг України керується Законом України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом" [49] і використовує міжнародні стандарти, які спрямовані на протидію легалізації (відмиванню) доходів, отриманих злочинним шляхом, і фінансуванню тероризму. Відповідно до міжнародних

стандартів Державна служба фінансового моніторингу України не є правоохоронним або контролюючим органом, а функціонує у взаємодії із фінансовим сектором і правоохоронними органами.

Середня кількість перевірок на рік у одного суб'єкта господарювання може досягати 78, середня кількість документів, які необхідно підготувати для перевірки контролюючим органам, – 68. Найпоширеніші для суб'єктів господарювання є перевірки органами фіскальної служби та внутрішніх справ, санітарно-епідеміологічної служби та протипожежного нагляду. Саме з представниками цих державних органів найчастіше доводиться стикатися керівникам і службам безпеки українських підприємств.

Найбільш частими порушеннями з боку перевіряючих органів є:

використання службового становища в особистих інтересах;

трактування законодавства виключно на користь перевіряючих;

примушення підприємців до перерахування коштів у різні фонди й організації;

нав'язування підприємцю різних комп'ютерних програм;

перевірки суб'єктів підприємницької діяльності без відповідних дозволів, за власною ініціативою;

перевищення допустимої частоти перевірок.

Перевірки контролюючих органів можуть бути як планові, так і позапланові. *Плановою виїзною перевіркою* вважається перевірка фінансово-господарської діяльності суб'єкта підприємницької діяльності, яка передбачена у плані роботи контролюючого органу та проводиться за місцезнаходженням такого суб'єкта чи за місцем розташування об'єкта власності, стосовно якого здійснюється така планова виїзна перевірка. Планова виїзна перевірка здійснюється за сукупними показниками фінансово-господарської діяльності суб'єкта підприємницької діяльності на підставі письмового рішення керівника відповідного контролюючого органу не частіше одного разу на календарний рік у межах компетенції відповідного контролюючого органу.

Забороняється проведення планових виїзних перевірок за окремими видами зобов'язань перед бюджетами, крім зобов'язань за тими позиками та кредитами, що гарантовані бюджетними коштами.

Право на проведення планової виїзної перевірки суб'єкта підприємницької діяльності надається, коли не пізніше ніж за десять календарних днів до дня проведення зазначеної перевірки надіслано письмове повідомлення з зазначенням дати її проведення.

Позаплановою виїзною перевіркою вважається перевірка, яка не передбачена в планах роботи контролюючого органу. Її проводять за наявності хоча б однієї з таких обставин:

а) за наслідками зустрічних перевірок виявлено факти, які свідчать про порушення суб'єктом підприємницької діяльності норм законодавства;

б) суб'єктом підприємницької діяльності в установлений строк не подано документи обов'язкової звітності;

в) виявлено недостовірність даних, заявлених у документах обов'язкової звітності;

г) суб'єкт підприємницької діяльності подав у встановленому порядку скаргу про порушення законодавства посадовими особами контролюючого органу під час проведення планової чи позапланової виїзної перевірки;

д) у разі виникнення потреби у перевірці відомостей, отриманих від особи, яка мала правові відносини з суб'єктом підприємницької діяльності, якщо суб'єкт підприємницької діяльності не надасть пояснення й їх документальні підтвердження на обов'язковий письмовий запит контролюючого органу протягом трьох робочих днів з дня отримання запиту;

е) проводиться реорганізація (ліквідація) суб'єкта господарювання.

Позапланові виїзні перевірки з підстави, визначеної у пункті "е", проводяться лише органами державної фіскальної служби й органами контрольно-ревізійної служби в межах їх повноважень. Позапланова виїзна перевірка може здійснюватися на підставі рішення Кабінету Міністрів України. Здійснення планових і позапланових виїзних перевірок із зазначених питань іншими державними органами забороняється.

Так, наприклад, право на проведення документальної податкової перевірки суб'єкта господарювання надається на підставі посвідчення, що оформляється на бланку фіскального органу, завіряється гербовою печаткою та підписується:

на планову перевірку – керівником органу або його заступником, якому підпорядкований підрозділ, що очолює перевірку;

на позапланову перевірку – тільки керівником податкового органу (особою, яка виконує його обов'язки).

Посвідчення на перевірку видається на кожного працівника, який приймає участь у перевірці. Таким чином, керівництво організації має право допускати до перевірки лише тих посадових осіб податкового органу, які мають посвідчення на перевірку, та не допускати тих, у кого відсутнє зазначене посвідчення. Крім цього, у разі сумнівів щодо осіб, які прийшли

на перевірку, можна порекомендувати бухгалтеру зателефонувати до податкового органу й отримати інформацію про кожного перевірювача.

Проведення кожної перевірки суб'єкт господарської діяльності має фіксувати в спеціальному Журналі перевірок із зазначенням дати, офіційного документу, уповноваженої особи, котра проводить перевірку.

Керівник підрозділу ФЕБ має контролювати весь процес перевірки з моменту надходження офіційного документа: наявність офіційного документа та правильність його оформлення, посвідчення уповноваженої особи, відображення мети та перебігу перевірки в організаційно-розпорядчих документах суб'єкта господарювання, дії відповідальних осіб і відповідність компетентностей співробітників господарюючого суб'єкта у взаємодії з контролюючими органами.

Керівник підрозділу ФЕБ повинен мати на увазі, що під час проведення перевірок розрахунок представників контролюючих (правоохоронних) органів, як правило, робиться на:

раптовість появи (стан стресу);

психологічний пресинг (підтримання в стресовому стані);

неграмотність (правову необізнаність) посадових осіб підприємства.

Основні завдання перевірювачів з органів фіскальної служби та внутрішніх справ такі:

отримати доступ до документів;

отримати пояснювальні документи від співробітників;

заволодіти максимумом інформації за мінімум часу;

змусити видати документи та ТМЦ добровільно, власноруч.

Тактичні прийоми (як правило, працівників правоохоронних органів):

насадження комплексу провини;

застосування різного виду погроз;

заборона телефонних дзвінків і переміщення офісом;

спроби проводити перевірки до глибокої ночі.

Типові помилки підприємців і співробітників підприємств:

сліпе підпорядкування особам, які прийшли на підприємство;

відсутність критичного підходу до дій та вимог працівників контролюючих (правоохоронних) органів;

нехтування попереджувальними (превентивними) заходами на випадок появи представників контролюючих (правоохоронних) органів – у стресовій ситуації людина, як правило, забуває все, що знала раніше та про що її інструктували усно;

не заведено Журнал реєстрації відвідувань тощо;

відсутність аналізу можливих загроз, виходячи з особливостей видів діяльності;

невіра в закон і невіра в свої сили. Як наслідок – незнання елементарних правил правомірної поведінки під час перевірок.

Ураховуючи зазначене, керівник підрозділу ФЕБ суб'єкта господарювання повинен пам'ятати про своє основне завдання та докласти максимум зусиль, щоб уникнути типових помилок підприємців у ході перевірки контролюючими (правоохоронними) органами.

Основне завдання керівника підрозділу ФЕБ – не дозволяти виходити за рамки правового поля, за змогою – не видати документи негайно на першу ж вимогу. Приймати будь-які рішення слід виважено та розсудливо.

Рекомендована література: [18; 46; 49; 50; 53; 56].

Практична частина

Контрольні запитання

1. Опишіть розподіл повноважень у системі корпоративного управління між акціонерами, Радою директорів і менеджерами компанії.
2. Визначте інтереси учасників корпоративного управління. Які причини виникнення агентської проблеми?
3. Охарактеризуйте роль УФЕБ у системі корпоративного управління.
4. Визначте стейкхолдерів компанії й їх очікування. Які можуть виходити загрози з боку зацікавлених осіб?
5. Охарактеризуйте найбільш розповсюджені підходи до формування СФЕБ організації. Які чинники у цьому процесі є визначальними?
6. Визначте об'єкти та суб'єкти ФЕБ організації. Розмежуйте внутрішні та зовнішні суб'єкти.
7. Надайте визначення СФЕБ. Розкрийте її компоненти.
8. Визначте бачення, місію та кредо організації. Яке місце займають ці концепти управління в формуванні СФЕБ?
9. Опишіть концепцію та політику в сфері ФЕБ організації.
10. З якими відділами корпоративного середовища має співпрацювати УФЕБ у тісному контакті та взаємодіяти щодо забезпечення гарантій заходів з ФЕБ? Охарактеризуйте їх функції.
11. Розкрийте запобіжно-профілактичну й інформаційно-аналітичну функції СФЕБ. Наведіть приклади здійснюваних заходів.

12. Розкрийте оперативно-розслідувальну й організаційно-консультативну функції СФЕБ. Наведіть приклади здійснюваних заходів.

13. Яким нормативно-правовим документом регламентуються загальні правила проведення перевірок суб'єктів господарювання органами державного нагляду (контролю)? Які основні положення процедури контролю?

14. Перелічіть основні контролюючі органи господарської діяльності організацій та їх контрольні функції.

15. Охарактеризуйте, які завдання постають перед керівником підрозділу ФЕБ під час планової або позапланової перевірки? Розкрийте типові помилки, недопущення яких необхідно попередити.

Тестові завдання

1. Сукупність процесів і організаційних структур, створюваних Радою управління організації для інформування, управління та моніторингу діяльності організації з метою досягнення поставлених цілей, – це:

а) корпоративне управління;

б) стратегічне управління;

в) надання прозорої звітності;

г) усі відповіді правильні.

2. В агентських відносинах акціонери виступають:

а) принципалами;

б) агентами;

в) робітниками;

г) підрядниками.

3. В агентських відносинах найманий менеджер виступає:

а) принципалом;

б) агентом;

в) робітником;

г) підрядником.

4. Суперечності інтересів менеджерів і акціонерів з причини відсутності у менеджерів прагнення до збільшення доходів на інвестований капітал називають:

а) громадянським конфліктом;

б) корпоративним конфліктом;

в) агентською проблемою;

г) усі відповіді правильні.

5. До суб'єктів ФЕБ безпеки організації відносять:

а) спеціальні служби, що забезпечують безпеку, та персонал організації;

б) органи, що займаються забезпеченням безпеки підприємництва: судові органи й органи прокуратури;

в) Національний банк України, Службу безпеки України, Державне казначейство та Митну службу;

г) усі відповіді правильні.

6. До внутрішніх суб'єктів СФЕБ організації не належать:

а) підрозділ ФЕБ, внутрішнього аудиту, комплаєнсу та ризик-менеджменту, охорона тощо;

б) персонал господарюючого суб'єкта, який дбає про ФЕБ свої організації в рамках своїх функціональних обов'язків і корпоративної етики;

в) приватні охоронні та детективні організації, аналітичні центри, інформаційні служби, навчальні, наукові та консультаційні організації;

г) правильної відповіді немає.

7. Об'єктом ФЕБ виступають:

а) бізнес-процеси (виробничі, комерційні, постачальницькі, управлінські та ін.);

б) фінансові, товарно-матеріальні цінності, техніко-технологічні, інформаційні, людські ресурси;

в) акціонери й їх економічні інтереси;

г) усі відповіді правильні.

8. Які з наведених відносин є об'єктом ФЕБ організації:

а) з діловими партнерами та контрагентами;

б) зі споживачами;

в) з регіональними та галузевими структурами, контролюючими та фіскальними службами, представниками органів влади;

г) усі відповіді правильні?

9. Демонстрація стратегічної мети, напряму діяльності, світогляду, цінностей співробітників, керівника організації – це:

а) бачення;

б) місія;

в) кредо;

г) культура.

10. Документ, який надає повне уявлення про систему сервісу та підтримки розвитку організації, захисту активів, місце УФЕБ, її обґрунтованість, – це:

а) концепція;

б) політика;

в) стратегія;

г) план.

11. Документ, який надає опис загальних дій і орієнтирів прийняття рішень в сфері ФЕБ – це:

а) концепція;

б) політика;

в) стратегія;

г) план.

12. Який з відділів співпрацює разом зі службою безпеки у проведенні розслідувань у зв'язку з інформацією про зловживання з боку працівників або інших осіб, які можуть бути пов'язані з організацією:

а) управління етики;

б) відділ внутрішнього аудиту;

в) юридичний відділ;

г) управління персоналом?

13. Робота якого з відділів разом зі службою безпеки спрямована на гарантування того, що компанія працює, а її працівники виконують свої обов'язки відповідно до чинного національного та місцевого законодавства, корпоративних політик і процедур:

а) управління етики;

б) відділ внутрішнього аудиту;

в) юридичний відділ;

г) управління персоналом?

14. Функціями якої групи заходів СФЕБ є підбір, перевірка та контроль роботи персоналу, розроблення відповідної кадрової політики та програм стимулювання персоналу:

а) запобіжно-профілактичної;

б) інформаційно-аналітичної;

в) оперативно-розслідувальної;

г) організаційно-консультативної?

15. Функціями якої групи заходів СФЕБ є виявлення негативних тенденцій, причин та умов напруженості, попередження та локалізація конфліктів, інструктаж персоналу з питань безпеки, формування почуття відповідальності за дотримання порядку:

а) запобіжно-профілактичної;

б) інформаційно-аналітичної;

в) оперативно-розслідувальної;

г) організаційно-консультативної?

16. Функціями якої групи заходів СФЕБ є запобігання розголошенню, просочуванню інформації та несанкціонованому доступу до джерел конфіденційної інформації:

а) запобіжно-профілактичної;

б) інформаційно-аналітичної;

в) оперативно-розслідувальної;

г) організаційно-консультативної?

17. Функціями якої групи заходів СФЕБ є організація та ведення конкурентної розвідки, формування інформаційних баз даних, перевірка клієнтів і контрагентів суб'єкта господарювання:

а) запобіжно-профілактичної;

б) інформаційно-аналітичної;

в) оперативно-розслідувальної;

г) організаційно-консультативної?

18. Функціями якої групи заходів СФЕБ є взаємодія із контролюючими та правоохоронними органами з питань запобігання протиправним посяганням на власність, персонал та імідж організації та припинення їх:

а) запобіжно-профілактичної;

б) інформаційно-аналітичної;

в) оперативно-розслідувальної;

г) організаційно-консультативної?

19. Функціями якої групи заходів СФЕБ є проведення заходів щодо дезінформації конкурентів, впливу на недобросовісних клієнтів, боржників і зловмисників з метою відшкодування суб'єкту господарювання втрат, які понесені через вину цих сторін:

а) запобіжно-профілактичної;

б) інформаційно-аналітичної;

в) оперативно-розслідувальної;

г) організаційно-консультативної?

20. Функціями якої групи заходів СФЕБ є установлення та підтримка системи заходів безпеки, визначення повноважень і відповідальності, розподіл обов'язків посадових осіб з метою забезпечення ФЕБ:

а) запобіжно-профілактичної;

б) інформаційно-аналітичної;

в) оперативно-розслідувальної;

г) організаційно-консультативної?

Не слід відвертатися від загрозливої небезпеки або намагатися втекти від неї. Якщо ви зробите це, ви опинитесь у подвійній небезпеці. Але якщо ви зустрінете її оперативно та не здригнувшись, ви скоротите її наполовину.
Уїнстон Черчілль

Розділ 3. Організація управління фінансово-економічною безпекою організації

Після вивчення матеріалів теми ви повинні:

знати:

послідовність організації й управління ФЕБ;

принципи управління ФЕБ організації;

варіанти організації управління ФЕБ;

завдання та функції підрозділів організації з УФЕБ, місце підрозділу ФЕБ в організаційній структурі управління;

правові та нормативно-методичні засади управління ФЕБ;

уміти:

запроваджувати принципи управління ФЕБ в організації;

визначати порядок організації УФЕБ;

визначати місце підрозділу ФЕБ в організаційній структурі управління, його функції;

проектувати організаційну структуру підрозділу ФЕБ організації;

демонструвати знання нормативно-методичного забезпечення роботи підрозділу ФЕБ;

розробляти документи, що регламентують діяльність підрозділу ФЕБ організації та його персоналу;

визначати обов'язки та відповідальність підрозділу ФЕБ.

План теми

3.1. Послідовність, принципи організації та управління фінансово-економічною безпекою.

3.2. Вибір організаційної структури підрозділу фінансово-економічної безпеки.

3.3. Підпорядкованість підрозділу фінансово-економічної безпеки, його повноваження.

3.4. Правові та нормативно-методичні засади управління фінансово-економічної безпеки.

3.5. Види завдань підрозділу фінансово-економічної безпеки.

Ключові поняття та терміни: організація, принципи управління, підрозділ фінансово-економічної безпеки, організаційна структура, підпорядкованість, нормативно-методичне забезпечення.

3.1. Послідовність, принципи організації та управління фінансово-економічною безпекою

Організація управління ФЕБ організації – перш за все це створення потрібної структури, яка буде наділена спеціальними повноваженнями та необхідними для її функціонування ресурсами. Серед навчально-методичних видань, які розкривають питання організації служб з безпеки, визначними є роботи таких авторів, як: В. П. Мак-Мак [17], Л. В. Гнилицька, О. І. Захарок, П. Я. Пригунов [9], В. Ф. Гапоненко [7], Н. Ю. Подольчак [27], І. П. Мойсеєнко й О. М. Марченко [21], робота під редакцією Ортинського В. Л. [13] та ін.

Підрозділ ФЕБ – це штатна структурна одиниця організації (компанії, акціонерного товариства, холдингу, корпорації, підприємства) з самостійними функціями, завданнями та відповідальністю. Залежно від форми власності організації, її організаційно-правової форми підрозділ ФЕБ може підпорядковуватися власникові, безпосередньо першому керівнику, органам державного управління організацією.

Підрозділ ФЕБ має на меті виконання функцій планування, організації, координації, вдосконалення та здійснення заходів щодо попередження, зниження рівня та протидії загрозам і ризикам поточної діяльності, сталого функціонування та розвитку організації. Особливість полягає в тому, що цей процес охоплює без винятку весь персонал організації, кожен із співробітників має усвідомлювати свою причетність до забезпечення фінансово-економічної безпеки організації.

Створювати такий підрозділ доцільно у випадках, коли:

завдання й обсяг діяльності з управління ФЕБ є такими, що економічно доцільно покласти виконання цієї функції на підрозділ, який здійснює зазначену діяльність на постійній основі;

у силу специфіки діяльності організації для забезпечення ефективності ФЕБ потрібне накопичення, збереження та передання спеціальних знань, навичок і досвіду;

ризики діяльності організації настільки високі, що забезпечення ефективності управління вимагає діяльності спеціального підрозділу ФЕБ на постійній основі;

існують вимоги законодавства або регулятора ринку щодо створення економічним суб'єктом спеціального підрозділу з контролю діяльності та забезпечення фінансово-економічної безпеки.

Підрозділ ФЕБ може включати різні підрозділи (відділи, групи). До найбільш значущих слід віднести: інформаційно-аналітичний, оперативного реагування, розвідки та контррозвідки, роботи з персоналом та інші.

Безпекові підрозділи, підпорядковані керівнику з безпеки корпоративного рівня, створюються з урахуванням кожного конкретного суб'єкта господарювання. Вони можуть формуватися за лінійним принципом (наприклад, "організація роботи щодо запобігання розкрадань на об'єктах компанії") або за об'єктовим ("комплекс заходів із забезпечення безпеки закупівель"). Якщо бізнес компанії має специфічні особливості, можна використовувати змішаний принцип.

На більшості підприємств підрозділи корпоративної безпеки формуються за такими напрямами: фінансово-економічна безпека, інформаційна безпека, охорона та безпека (фізична та майнова). Ці ж напрями закладені в основу професійно-кваліфікаційного забезпечення кадрами сфери корпоративної безпеки (Класифікатора професій [48] і Довідника кваліфікаційних характеристик професій працівників "Безпека господарської діяльності підприємств, установ, організацій" [44]).

Розуміння СФЕБ пояснюється тим, що поряд з виконанням своїх прямих посадових обов'язків керівник підрозділу ФЕБ опосередковано впливає на дії персоналу компанії, використовуючи затверджені генеральним директором нормативні документи компанії (накази, вказівки, інструкції тощо). Керівник підрозділу ФЕБ приймає участь у їх підготовці та вписує в регламентаційні документи завдання з безпеки або їх певну частину.

Загальна схема організації й управління ФЕБ компанії містить десять етапів (рис. 3.1), починаючи від діагностики та закінчуючи встановленням нових завдань і удосконаленням процесу забезпечення ФЕБ.

Рис. 3.1. **Етапи організації й управління ФЕБ організації**

Така послідовність забезпечує планомірне управління та контроль ефективності функціонування системи ФЕБ.

Для того щоб СФЕБ організації запрацювала ефективно, вона має відповідати певним **принципам управління ФЕБ**, які достатньо повно висвітлено в роботах [17; 20; 26].

1. Пріоритет заходів попередження, профілактика можливих загроз. Змістовність цього принципу передбачає завчасне виявлення потенційних загроз, аналіз причин виникнення загроз і наслідків тих, що вже наступили; спостереження за тенденціями, що сприяють розвитку загроз, та вироблення на цій основі відповідних профілактичних заходів.

2. Законність. Усі заходи, спрямовані на здійснення ФЕБ, повинні розроблятися на основі чинного законодавства та реалізовуватися в рамках актуальних нормативно-правових документів.

3. Комплексне використання сил і засобів. Для забезпечення безпеки використовуються всі наявні у розпорядженні організації ресурси. Кожен співробітник повинен у межах своєї компетенції брати участь у забезпеченні безпеки організації. Організаційною формою комплексного використання сил і засобів є програма ФЕБ організації.

4. Координація та взаємодія всередині та поза організацією. Заходи протидії загрозам здійснюються на основі взаємодії та скоординованості зусиль усіх підрозділів, служб суб'єкта господарювання, а також установлення необхідних контактів із зовнішніми організаціями, здатними надати необхідне сприяння в забезпеченні безпеки суб'єкта господарювання. Організувати координацію та взаємодію всередині та поза організацією може комітет (рада, група тощо) безпеки суб'єкта господарювання.

5. Поєднання гласності з конфіденційністю. Доведення до відома персоналу та громадськості в допустимих межах заходів з безпеки відіграє найважливішу роль – запобігання потенційним і реальним загрозам. Така гласність, проте, неодмінно повинна доповнюватися у виправданих випадках заходами конспіративного характеру.

6. Компетентність. Працівники та групи співробітників повинні вирішувати питання забезпечення безпеки на професійному рівні, а в необхідних випадках – спеціалізуватися за основними його напрямами.

7. Економічна доцільність. Вартість фінансових витрат на забезпечення безпеки не повинна перевищувати того оптимального рівня, за якого втрачається економічний сенс їх застосування.

8. Планова основа діяльності. Забезпечення безпеки повинно будуватися на основі комплексної програми та підпрограм із забезпечення

безпеки суб'єкта господарювання за основними видами діяльності (економічна, науково-технічна, екологічна, технологічна тощо) і розроблюваних для їх виконання планів роботи підрозділів організації й окремих працівників.

9. Системність. Цей принцип припускає врахування всіх факторів впливу, залучення до її забезпечення співробітників підрозділів, використання в цій діяльності всіх сил і засобів.

3.2. Вибір організаційної структури підрозділу фінансово-економічної безпеки

Організація ефективного підрозділу ФЕБ потребує часу та вимагає вирішення багатьох важливих питань, основними з яких є:

проектування організаційної структури та ресурсного забезпечення підрозділу ФЕБ;

установлення підпорядкованості підрозділу ФЕБ організації;

розроблення нормативно-організаційних документів підрозділу ФЕБ;

установлення взаємодії підрозділу ФЕБ з іншими підрозділами організації.

Підрозділ ФЕБ може створюватися як окремий підрозділ або як структурна одиниця підрозділу корпоративної (або економічної) безпеки, якщо такий є. Функціональне навантаження, вибір організаційної структури, штат, ресурсне забезпечення (фінансове, кадрове, матеріально-технічне, інформаційне) підрозділу залежать від таких чинників, як:

розмір організації;

види діяльності та специфіка продукції (послуг);

прибутковість фінансово-господарської діяльності;

цілі та стратегія розвитку організації;

рівень конкуренції в галузі та на міжнародному ринку (якщо організація є суб'єктом міжнародного ринку);

розміщення структурних підрозділів і виробничих потужностей, складів і транспортних комунікацій;

рівень криміналізації сегмента ринку, де працює організація, корупції, недобросовісної конкуренції;

професійна якість персоналу;

адміністративний вплив органів державної влади й управління;

стратегічне бачення та позиції керівників (власників) організації щодо концепції економічної безпеки.

Важливим для проектування роботи підрозділу є визначення кількості потрібного персоналу. Розмір підрозділу з безпеки безпосередньо залежить від розміру організації. Тому доцільно спиратися на норми керованості, що дозволить упорядкувати роботу підрозділу та забезпечити раціональну роботу його персоналу (рис. 3.2):

департамент безпеки створюється з чисельністю працівників у штаті не менше п'ятнадцяти осіб (включаючи посаду керівника);

управління безпеки, або служба, створюються з чисельністю працівників у штаті не менше семи осіб (включаючи посаду керівника);

відділ безпеки створюється з чисельністю працівників у штаті не менше чотирьох осіб (включаючи посаду керівника);

сектор безпеки (бюро, група) створюється з чисельністю працівників у штаті не менше трьох осіб (включаючи посаду керівника);

призначення фізичної особи, яка відповідає в організації за безпеку.

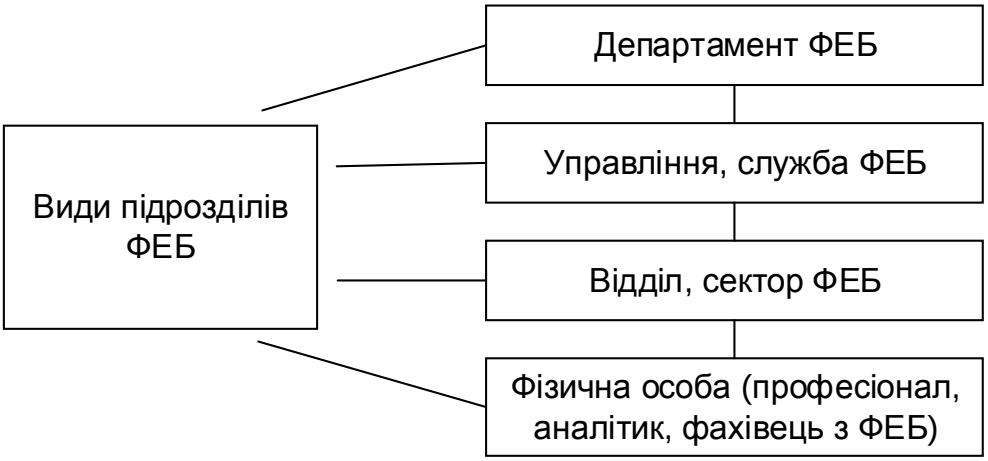

Рис. 3.2. **Типові види підрозділів, рекомендовані для організації підрозділів ФЕБ**

Найбільше поширення в організації систем економічної безпеки отримали дві організаційні структури: лінійна та лінійно-штабна. Лінійна структура – це найпростіша ієрархічна структура управління. Схематично вона складається з керівника підрозділу та кількох підлеглих (рис. 3.3).

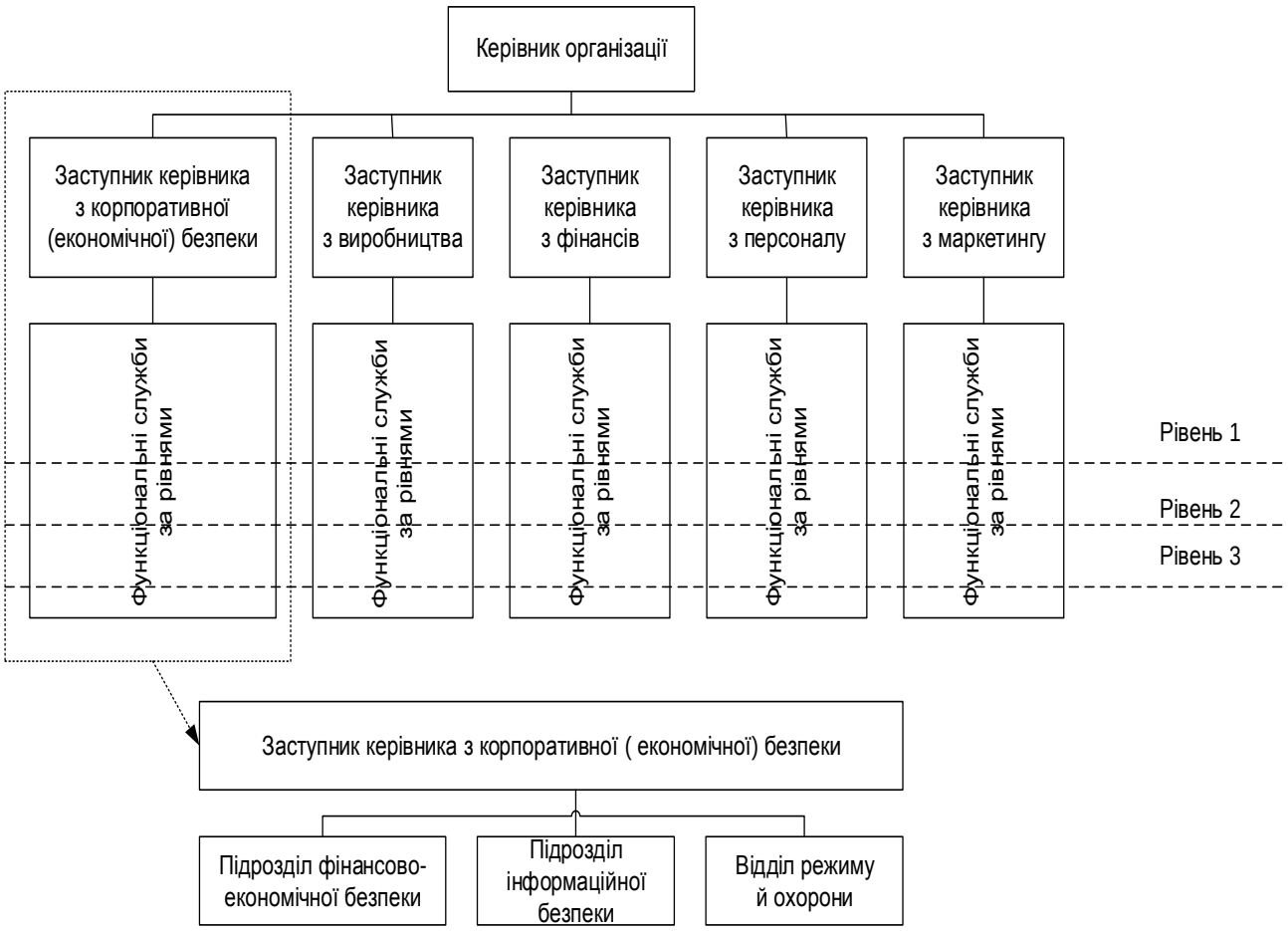

Рис. 3.3. **Місце підрозділу ФЕБ у лінійній структурі організації**

Великі підприємства можуть мати до чотирьох і навіть більше рівнів ієрархії. Якщо взяти за основу таку структуру, то її переваги можна сформулювати таким чином:

чітка підпорядкованість – кожен начальник, кожен працівник підпорядкований лише одній вищій особі;

чітка визначеність функцій та відповідальності;

швидка реакція виконавців на вирішення поставлених завдань;

чіткий розподіл і контроль витрат між підрозділами.

Серед недоліків (або питань, що потребують додаткової уваги та вирішення), доцільно навести:

відсутність ланок, що займаються питаннями стратегічного планування; у роботі керівників практично всіх рівнів оперативні проблеми домінують над стратегічними;

тенденція до тяганини та перекладання відповідальності щодо вирішення проблем безпеки, що потребують участі кількох підрозділів;

власникам організації інформація надається за вимогою або запитом самого власника, що є загрозою своєчасного попередження можливих небезпек;

незначна гнучкість персоналу та пристосовність їх до зміни ситуації;

критерії ефективності й якості роботи підрозділів і організації в цілому – різні;

тенденція до формалізації оцінки ефективності й якості роботи підрозділів зазвичай призводить до виникнення атмосфери страху та роз'єднаності;

перевантаження керівників верхнього рівня;

підвищена залежність результатів роботи організації від кваліфікації, особистих і ділових якостей вищих керівників.

З огляду на те, що недоліки структури переважують її переваги, більш ретельну увагу доцільно приділяти формальним основам роботи підрозділу ФЕБ (організаційній документації, контролю виконання завдань та їх оцінюванню) та роботі з персоналом. Типові приклади структур з безпеки лінійного типу наведені у табл. А.1 додатка А.

Лінійно-штабна структура включає спеціалізовані підрозділи (штаби), які не володіють правами прийняття рішень і управління нижчими підрозділами, а лише допомагають відповідному керівникові у виконанні окремих функцій, перш за все – функцій стратегічного планування, аналізу, контролю та безпеки. В іншому ця структура відповідає лінійній (рис. 3.4).

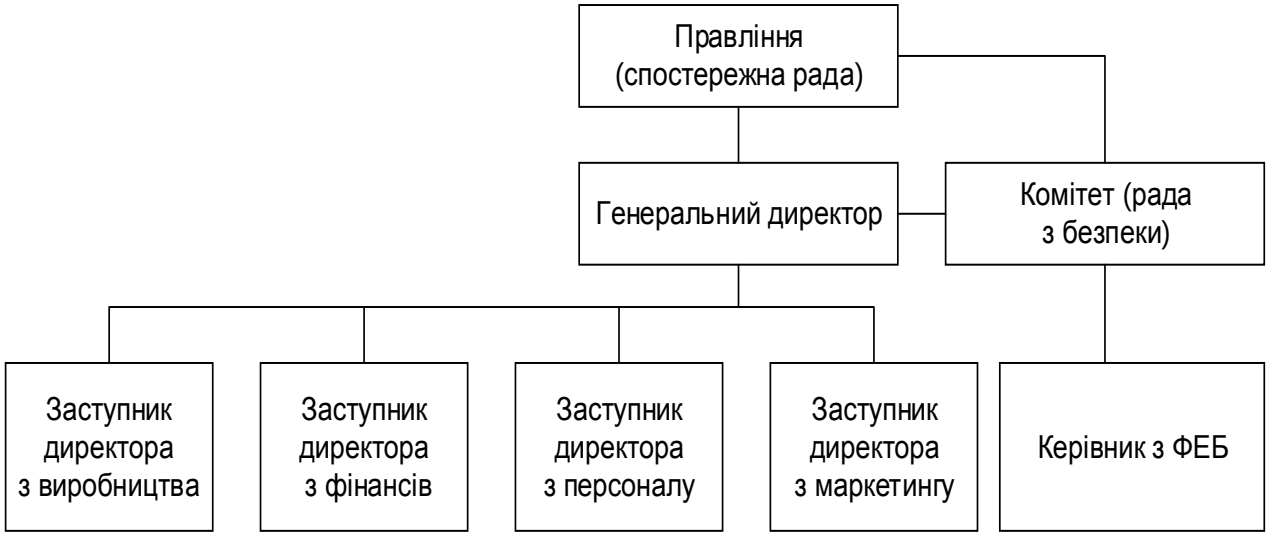

Рис. 3.4. **Лінійно-штабна структура компанії**

Переваги лінійно-штабної структури полягають у такому:

націленість на опрацювання стратегічних питань;

розвантаження вищого керівництва;

попередження загроз господарській діяльності з боку вищого керівництва та менеджменту (перевищення повноважень);

можливість залучення зовнішніх консультантів і експертів.

Разом з тим лінійно-масштабна структура має свої недоліки, наприклад, тенденції до надмірної централізації управління ФЕБ. Інші недоліки аналогічні лінійній структурі, але в ослабленому вигляді. Тому лінійно-штабна структура вважається більш ефективною.

Іншим варіантом може бути залучення незалежного консультанта для організації й оцінювання ФЕБ у таких випадках:

власні ресурси суб'єкта господарювання недостатні для виконання завдань з організації й (або) оцінювання ФЕБ;

витрати на створення й утримання спеціального підрозділу ФЕБ перевищують вартість залучення незалежного консультанта для виконання завдань з організації й (або) оцінювання ФЕБ;

є зацікавленість керівництва організації в незалежному оцінюванні ФЕБ;

використовуються стандартні, апробовані на практиці підходи до організації та (або) оцінювання ФЕБ.

Під час організації управління ФЕБ господарської діяльності малого підприємництва необхідно керуватися вимогою раціональності й економічної доцільності.

3.3. Підпорядкованість підрозділу фінансово-економічної безпеки, його повноваження

Питання підпорядкованості підрозділу ФЕБ виникають у тому випадку, коли є розбіжності інтересів між особами, які виконують функції органів управління суб'єкта господарювання, як то між власниками (акціонерами), Радою директорів і генеральним директором, директором і керівниками підрозділів (менеджерами). У цьому зв'язку постає питання, кому буде підпорядкований та підзвітний підрозділ з безпеки.

Рівень підпорядкованості визначає повноваження та роль підрозділу з безпеки в фінансово-господарській діяльності організації, а також впливає на якість і результативність виконання співробітниками ФЕБ своїх обов'язків. Зазвичай зустрічаються такі *організаційні моделі підпорядкованості підрозділів з безпеки*.

1. Підрозділ з безпеки підпорядкований генеральному директорові (директорові) та звітує перед ним (рис. 3.5 а). У даному випадку керівник з безпеки виконує рекомендаційну функцію для керівника суб'єкта господарювання та забезпечує контроль інших рівнів управління. Така схема управління ФЕБ є ефективною за умови співпадіння інтересів директора та керівника ФЕБ у цілях фінансово-господарської діяльності суб'єкта господарювання та чіткого розмежування повноважень і відповідальності між ними. Узгодження інтересів може бути досягнуте за умов прямої зацікавленості керівника ФЕБ в інтересах бізнесу через механізм мотивації та стимулювання чи дольову участь у підприємстві. Може також зустрічатися модель, коли керівник з безпеки підпорядкований одному з інших керівників організації у виконанні функції забезпечення інформацією керівництва й у деякому обсязі контрольних функцій інших рівнів управління.

2. Підрозділ з безпеки підпорядкований Раді директорів або комітету з безпеки (рис. 3.5б, в). У даному випадку керівник ФЕБ разом з керівником організації зобов'язані виконанням контрольних і рекомендаційних функцій.

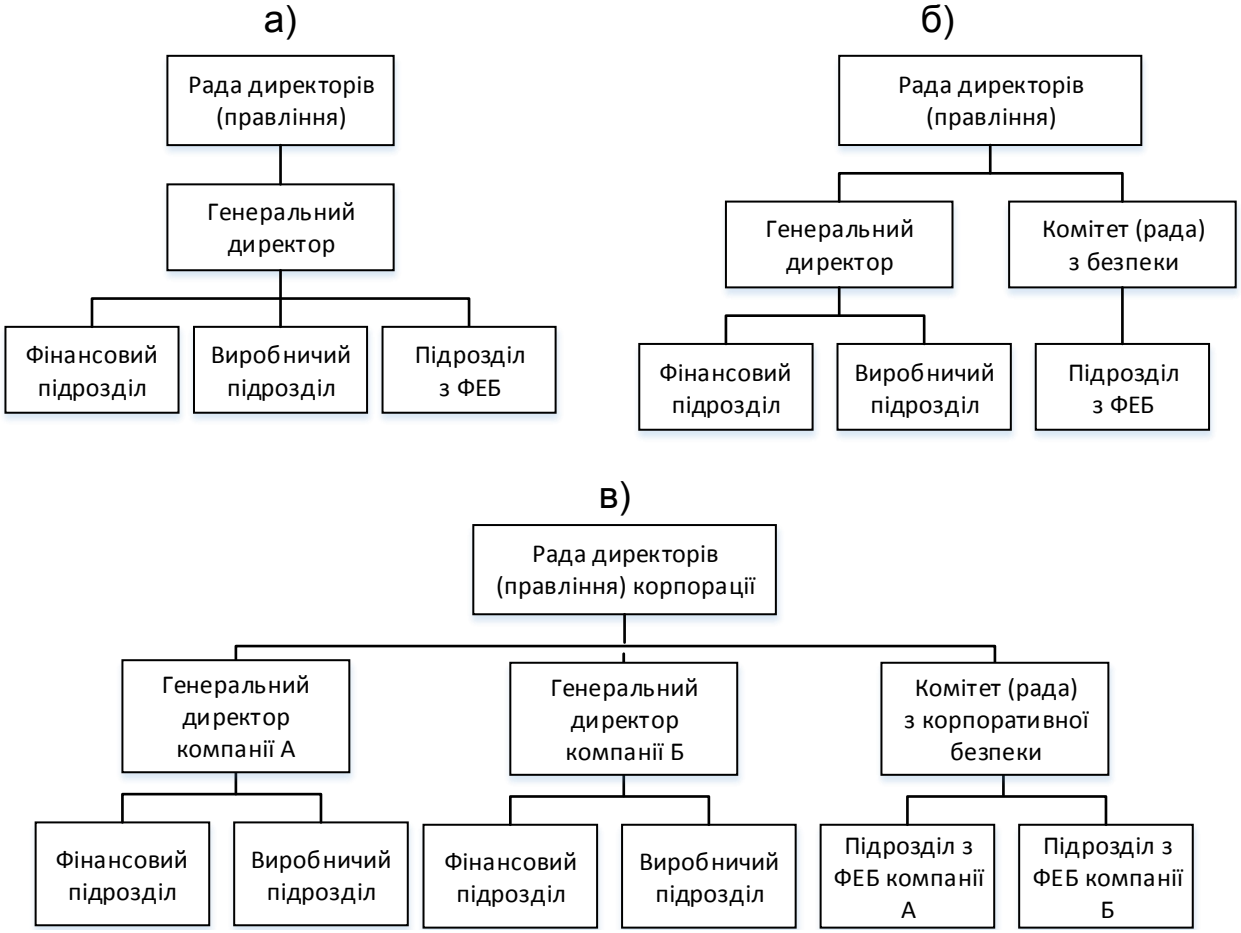

Рис. 3.5. **Організаційні моделі підпорядкованості підрозділів з ФЕБ** (початок)

г)

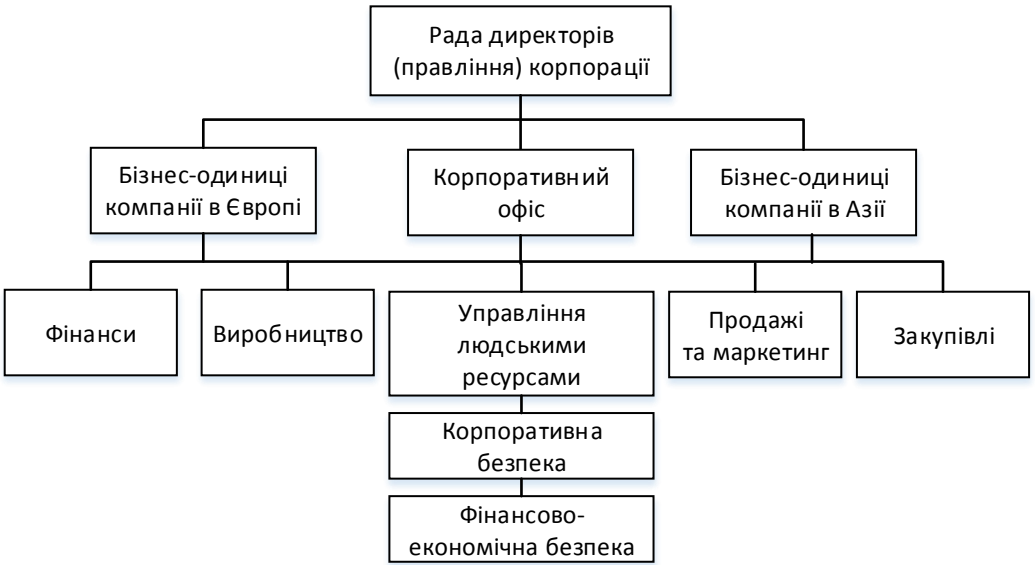

Рис. 3.5. **Організаційні моделі підпорядкованості підрозділів з ФЕБ** (закінчення)

Така модель є обґрунтованою для великих компаній та корпорацій (рис. 3.5в), які прагнуть до поширення єдиних стандартів з безпеки, гарантом виконання яких є директор, а система ФЕБ спрямована на контроль і забезпечення їх виконання на всіх рівнях управління компанією. У цьому зв'язку може виникнути конфлікт між генеральним директором компанії та керівником з безпеки, що також потребує чіткого розмежування повноважень і відповідальності між ними.

3. Підрозділ з безпеки підпорядкований підрозділу з управління людськими ресурсами (рис. 3.5г). За такої моделі керівник з безпеки має звітувати перед директором з управління людськими ресурсами, а останній напряму звітує генеральному директорові. Таке розміщення підрозділів з безпеки є логічним, як вважають консультанти та керівники іноземних компаній, оскільки безпека стосується безпосередньо персоналу та роботи з ним.

Деякі експерти та директори вважають за доцільне підпорядкування підрозділу з ФЕБ директорові з внутрішнього аудиту. Однак директори з аудиту зазначають, що їх відділи строго відповідають за дотриманням у діяльності компанії регіональних, національних і міжнародних законів, функцій комплаєнс-політики та процедур компанії. Більшість аудиторів не бажають перебирати на себе частину відповідальності за забезпечення безпеки, оскільки департамент безпеки часто бере на себе провину, коли щось йде не так. Також може виникнути конфлікт інтересів між департаментами безпеки й аудиту щодо створення корпоративних політик

і процедур безпеки. Водночас аудит визнає не тільки відповідність політики та процедур безпеки, але й їх адекватність.

У компаніях, діяльність яких пов'язана із інформацією та високими технологіями й активи яких автоматизовані, служба ФЕБ може бути включена до складу департаменту з інформаційних технологій (ІТ). Пояснюється така модель тим, що інформаційна система безпеки обслуговує ІТ, тобто має сенс розмістити всі функції безпеки під ІТ.

Також можна розглядати розміщення служби з ФЕБ у складі фінансового департаменту з підпорядкованістю генеральному директорові.

Місце підрозділу ФЕБ в організаційній структурі будь-якого виду зазначеними варіантами не вичерпується, можливі й інші варіанти.

Вважається, що якщо служба безпеки здатна чинити вплив на організаційну структуру організації, то вона зможе сформувати цілісну систему забезпечення корпоративної безпеки.

Оптимальною можна вважати структуру, за якої генеральний директор відповідає за створення та забезпечення функціонування підрозділу ФЕБ, сам підрозділ функціонально підпорядкований Раді з безпеки (штабу, комітету), а адміністративно – директорові суб'єкта господарювання. Це дає підрозділу ФЕБ необхідну незалежність, оскільки тільки в умовах незалежності вона може виконувати ті контрольні, моніторингові та розвідувальні функції, які на неї покладені. Якщо організаційна структура не передбачає створення Ради з безпеки, то служба ФЕБ має функціонально підкорятися Раді директорів.

Незалежність підрозділу ФЕБ передбачає свободу від умов, які створюють загрозу здатності підрозділу неупереджено виконувати свої обов'язки. Для того щоб досягти ступеня незалежності для ефективного виконання підрозділом своїх обов'язків керівник ФЕБ повинен мати прямий і вільний доступ до вищого виконавчого керівництва та Ради. Цього можна досягти шляхом установлення підзвітності двом сторонам. Проблеми незалежності необхідно вирішувати на рівнях індивідуальному, функціональному й організаційному.

Об'єктивність роботи підрозділу ФЕБ – це уявна настанова, яка дає змогу професіоналам і фахівцям з ФЕБ виконувати завдання неупереджено – таким чином, щоб вони самі відчували відповідальність і довіру до результатів своєї роботи та не допускали компромісів щодо її якості. Об'єктивність вимагає підтвердження результатів роботи об'єктивними фактами. Загрози об'єктивності також мають розглядатися на рівнях індивідуальному, функціональному й організаційному.

Організаційна незалежність досягається, коли керівник ФЕБ функціонально підзвітний Раді. Приклади функціональної підзвітності:

ухвалення Радою Положення (Концепції) про фінансово-економічну безпеку;

ухвалення Радою плану забезпечення ФЕБ;

ухвалення бюджету та ресурсного плану ФЕБ;

отримання Радою інформації від керівника ФЕБ про хід виконання плану ФЕБ і з інших питань;

ухвалення Радою рішень про призначення й усунення з посади керівника ФЕБ;

ухвалення винагороди керівника ФЕБ;

розгляд Радою відповідних запитів виконавчого директора та керівника ФЕБ про наявність неприйнятних обмежень в обсязі робіт або ресурсів.

Функції директора в організації роботи підрозділу ФЕБ полягають у такому:

ухвалення управлінських рішень щодо забезпечення керівництва ФЕБ інформацією;

адміністративне управління системою ФЕБ (ухвалення необхідних організаційно-розпорядчих документів);

створення режиму збереження комерційної таємниці;

надання допомоги та здійснення контролю за діяльністю функціональних підрозділів суб'єкта господарювання.

Розподіл повноважень і функцій з організації та здійснення ФЕБ компанії поданий у табл. 3.1.

Таблиця 3.1

Розподіл повноважень і функцій з організації й управління ФЕБ компанії

Органи управління	Функції та повноваження органів управління
1	2
Рада директорів (наглядова рада)	Установлює загальні принципи та вимоги ФЕБ, затверджує Концепцію безпеки компанії в цілому, приймає рішення щодо підвищення ефективності ФЕБ

Продовження табл. 3.1

1	2
Комітет з безпеки ради директорів (наглядової ради)	Установлює стандарти та методи здійснення безпеки; спостерігає за ефективністю ФЕБ, незалежністю спеціального підрозділу ФЕБ, процесом забезпечення ФЕБ і кодексом ділової поведінки (етики) її співробітників. Аналізує звіти про стан безпеки. Проводить регулярні зустрічі з керівником підрозділу ФЕБ, керівниками інших підрозділів для розгляду істотних ризиків, проблем забезпечення безпеки та відповідних планів. Аналізує результати й якість виконання розроблених керівниками підрозділів заходів (коригувальних кроків) щодо вдосконалення ФЕБ. Розглядає випадки та результати розслідувань зловживань і шахрайства, оцінює адекватність прийнятих керівником підрозділу ФЕБ заходів щодо попередження таких випадків
Генеральний директор	Відповідає за організацію та здійснення ФЕБ фактів господарського життя, ведення бухгалтерського обліку та складання бухгалтерської (фінансової) звітності в цілому, результати та досягнення цілей сталого функціонування
Фінансовий директор (головний бухгалтер)	Відповідає за організацію та здійснення внутрішнього контролю ведення бухгалтерського обліку та складання бухгалтерської (фінансової) звітності, взаємодію із третіми особами (контролюючими органами, кредиторами та інвесторами)
Керівники підрозділів і персонал	Проводять оцінювання загроз, ризиків і контроль бізнес-процесів; складають і оновлюють документацію щодо фінансових втрат, фактів шахрайства; відповідають за ефективність бізнес-процесів
Підрозділ ФЕБ	Здійснює організацію захисту законних прав та інтересів компанії. Здійснює збирання, аналіз і прогнозування інформації щодо зовнішніх і внутрішніх загроз компанії, в тому числі фінансовим, матеріальним, інформаційним та кадровим ресурсам. Здійснює виявлення та запобігання можливій протиправній діяльності з боку працівників компанії

Закінчення табл. 3.1

1	2
	Забезпечує гарантування безпеки спеціальними засобами та методами. Удосконалює заходи з безпеки, поширює Концепцію ФЕБ компанії. Здійснює отримання інформації, необхідної для подальшого прийняття найбільш оптимальних управлінських рішень з окремих питань стратегії та тактики компанії. Проводить виявлення й усунення негативних впливів на компанію з боку недобросовісних конкурентів, кримінальних структур та окремих осіб. Здійснює організацію заходів щодо формування серед населення та ділових партнерів позитивного реноме компанії, що сприяє реалізації планів економічного розвитку та статутних завдань. Здійснює контроль за ефективністю функціонування системи безпеки, вдосконалення її елементів. Проводить консультації керівників підрозділів і персоналу щодо дотримання вимог безпеки

Підрозділ ФЕБ повинен бути вільним від втручання третіх осіб у проведення робіт і звітування про результати. Керівник ФЕБ повинен підтримувати відносини з Радою та безпосередньо взаємодіяти з нею.

За допомогою підрозділу ФЕБ здійснюється контроль та координація заходів з ФЕБ у всіх сферах роботи компанії (фінанси, виробництво, маркетинг, реалізація, закупівлі, логістика, управління персоналом та ін.). Тому до забезпечення фінансово-економічної безпеки можуть бути залучені максимальна кількість структурних підрозділів і фахівців організації (планово-економічна служба, бухгалтерія, управління персоналом, юридична тощо).

3.4. Правові та нормативно-методичні засади управління фінансово-економічної безпеки

Будь-яка управлінська діяльність потребує упорядкування та має регламентуватися чинним законодавством, спиратися на визначені нормативно-правові документи, правила та процедури.

На жаль, сьогодні в Україні відсутні ключові закони, які б змогли ефективно регламентувати професійну діяльність в області економічної

безпеки, у тому числі закони про: службу безпеки, комерційну таємницю, охоронну діяльність, зброю, детективну діяльність та інших.

Незважаючи на відсутність низки важливих законів, організація та діяльність підрозділу ФЕБ повинна здійснюватися тільки у реально існуючому правовому полі. Усі проведені заходи з ФЕБ організації повинні бути строго регламентовані Конституцією України, законами держави, постановами Кабінету Міністрів, відомчими інструкціями, а також інструкціями, які розробляються безпосередньо в організації, затверджуються її першим керівником і детально регламентують усю діяльність системи й її безпеки.

Правові засади формують законодавчі акти, постанови, накази та інші правові документи органів управління. Нормативно-методичне забезпечення управління ФЕБ складають положення, інструкції, нормативи, методичні вказівки, рекомендації та роз'яснення (рис. 3.6).

Рис. 3.6. **Правове та нормативно-методичне забезпечення УФЕБ**

Отже, нормативно-правове забезпечення системи ФЕБ організації включає:

Конституцію України;

закони України;

накази та розпорядження Президента України;

постанови та розпорядження Кабінету Міністрів України;

міжнародні договори;

відомчі нормативні акти;

статут організації;

концепцію економічної безпеки організації;

накази та розпорядження керівника організації, що стосуються питань забезпечення економічної безпеки в усіх сферах (внутрішньої та зовнішньої) функціонування організації;

положення про підрозділ організації та посадові інструкції;

інструкції, що регламентують діяльність суб'єктів управління ФЕБ організації.

Основні положення щодо захисту господарської діяльності, ведення бізнесу та фінансово-економічної безпеки організації закріплені в Конституції та законах, які регламентують господарську діяльність, це:

Цивільний та Цивільно-процесуальний кодекси України;

Господарський та господарський процесуальний кодекси України;

Податковий кодекс України;

Кримінальний кодекс України;

Кодекс України "Про адміністративні правопорушення";

Кодекс законів про працю й інші кодексі України залежно від галузевих особливостей діяльності організації;

Закон України "Про акціонерні товариства";

Закон України "Про господарські товариства";

Закон України "Про захист від недобросовісної конкуренції";

Закон України "Про інформацію";

Закон України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом" та інші.

Правову основу створення та діяльності підрозділу з безпеки організації є Статут організації. Посилання на Статут є обов'язковою умовою організації підрозділу ФЕБ, управління та діяльності щодо протидії зовнішнім і внутрішнім загрозам.

Національне законодавство не містить будь-яких нормативно-правових актів прямої дії щодо організації корпоративної безпеки та СФЕБ організації або створення відповідного підрозділу, його прав та обов'язків. Тому правову основу для організації та діяльності підрозділів корпоративної безпеки будуть складати нормативні документи, які дають право на діяльність в основних напрямах захисту компанії.

Суб'єкт господарської діяльності має право створювати у своїй структурі підрозділи із захисту активів і персоналу, зокрема підрозділи корпоративної та фінансово-економічної безпеки, які мають відповідні обов'язки та відповідальність. Якщо таке рішення прийняте, в Статуті суб'єкта господарювання це має бути визначено.

Так, обов'язки та відповідальність підрозділу ФЕБ можуть бути визначені як:

розроблення методології та запровадження процесів оцінювання відповідності вимогам фінансово-економічної безпеки нових ділових пропозицій, контрактів, проектів;

розроблення та контроль реалізації довгострокового плану фінансово-економічної безпеки з урахуваннях ефективного й економічного використання ресурсів безпеки;

забезпечення загального напряму управління всіма видами діяльності зі забезпечення фінансово-економічної безпеки в компанії;

взаємодія з керівниками аудиторських, юридичних, екологічних, санітарних, технічних, медичних структур для вирішення питань, пов'язаних з безпекою активів компанії;

забезпечення відповідності процесів фінансово-економічної безпеки до встановлених вимог безпеки та договірних відносин з клієнтами;

контроль за здійсненням інформаційної безпеки в компанії та програми захисту корпоративної та клієнтської інформації;

контроль розроблення загальнокорпоративної програми антикризового управління;

контроль розроблення та запровадження системи вимірювання фінансово-економічної безпеки, що дозволяє оцінити ефективність програми фінансово-економічної безпеки та задоволеність клієнтів;

виконання стандартних управлінських обов'язків і завдань відповідно до встановлених корпоративних правил і режимів;

забезпечення безпечного середовища з метою захисту людей, матеріальних цінностей та інформації компанії;

безпосереднє розроблення та впровадження стандартів забезпечення фінансово-економічної безпеки, які відповідають нормативно-правовим вимогам;

забезпечення реалізації політики фінансово-економічної безпеки, намірів або застосування пов'язаних з безпекою законів і правил; забезпечення додаткової підтримки корпоративних елементів – у разі необхідності;

підтримання зв'язків з контролюючими та державними органами безпеки, участь у розробленні політики безпеки, представництві організації

у професійних і галузевих спілках з метою формування й інтерпретації безпекової політики;

взаємодія з державними та місцевими правоохоронними органами, слідчими та протипожежними органами;

розроблення, впровадження та підтримування системи оцінювання безпеки компанії, що дозволяє оцінювати ефективність програми безпеки кожного елементу компанії, компанії у цілому та бенчмаркінг програм з безпеки аналогічних компаній;

розроблення корпоративної політики безпеки для запровадження процесів і процедур з адміністративного захисту; кадрової, фізичної й інформаційної безпеки; навчання й освіти в сфері безпеки; розслідування, планування та визначення якості безпеки та контролю, протипожежного захисту та безпеки міжнародних операцій;

розроблення, узгодження, запровадження та підтримання економічно ефективної програми захисту активів і бізнес-процесів.

Описані обов'язки та відповідальність підрозділу ФЕБ створюють підґрунтя й узаконену основу для запровадження діяльності з фінансово-економічної безпеки в організації.

На основі Статуту організації розробляється Положення про підрозділ, який підтверджує й закріплює організаційно-структурний статус персоналу з ФЕБ. У Положенні про підрозділ з безпеки організації має бути визначено:

1) статус підрозділу з безпеки: він є самостійним структурним підрозділом;

2) умови створення та ліквідації підрозділу; який орган є компетентним за прийняття такого рішення (як правило, за рішенням і наказом Голови правління);

3) організаційно-структурна підпорядкованість підрозділу;

4) об'єкти, що входять у зону відповідальності співробітника Підрозділу з безпеки; який орган їх визначає та закріплює (як правило, визначає та закріплює генеральний директор за допомогою наказу);

5) структура та штатна чисельність підрозділу (затверджується генеральним директором);

6) перелік нормативної документації, яким керується персонал підрозділу й який регулює його роботу (законодавство України; Положення "Про підрозділ безпеки"; накази та розпорядження генерального директора);

7) зв'язки підрозділу безпеки з іншими відділами організації.

На основі Положення про підрозділ відповідно до вимог чинного законодавства України на підставі Довідника кваліфікаційних характеристик професій працівників у сфері безпеки [44] складаються Посадові інструкції штатних працівників підрозділу. У розробці посадових інструкцій ураховуються конкретні завдання та функції, права й обов'язки, відповідальність працівників підрозділу з безпеки.

Далі розробляються організаційно-розпорядчі документи, що регламентують порядок і правила роботи підрозділу ФЕБ: інструкції, вказівки та правила; порядок і спосіб здійснення завдань, поставлених перед працівниками підрозділу ФЕБ. Такі інструкції можна складати за різними ознаками, як то: вид виконуваних робіт; об'єкт, що потребує захисту; процедура дій з боку персоналу тощо. Метою складання інструкцій є:

організація режиму й охорони об'єктів захисту, включаючи вимоги щодо пропускного та внутрішньооб'єктного режиму;

збереження комерційної таємниці, включаючи перелік відомостей, які до неї належать;

організація роботи з конфіденційною інформацією, забезпечення захисту інформації, що обробляється та передається в автоматизованих системах і засобах зв'язку;

забезпечення перевірки та встановлення взаємовідносин із контрагентами;

облік і контроль фінансів, забезпечення їх збереження в процесі операцій, зберігання та транспортування;

перевірка кандидатів на роботу співробітниками служби безпеки, відбір, підбір та атестація персоналу організації;

порядок і правила проведення службових розслідувань.

Співробітники підрозділу безпеки зобов'язані чітко засвоїти зміст нормативних та організаційно-розпорядчих документів. Керівникам підрозділів слід періодично проводити перевірку засвоєння матеріалу шляхом інструктажу або прийняття заліків.

3.5. Види завдань підрозділу фінансово-економічної безпеки

Реалізація функції ФЕБ полягає в проведенні контрольних заходів, спрямованих на мінімізацію фінансово-економічних ризиків під час укладання та виконання договорів, здійснення операцій фінансово-господарської діяльності, а також інших напрямів діяльності.

1. *Мінімізація економічних ризиків пуд час укладання договорів*. До даної області входить перевірка майбутніх контрагентів – залежно від обсягів

запланованої співпраці. Для цього встановлюються: фінансовий та майновий стан контрагента; наявність у особи, яка буде укладати угоду, прав на її здійснення; наявність і дійсність ліцензії (якщо його діяльність ліцензована); відсутність щодо придбаного майна спору або прав на нього третіх осіб; визначення "справжніх" власників бізнесу.

У ході перевірки контрагентів (як діючих, так і майбутніх) з'ясовується благонадійність партнера, історія можливих судових рішень, позовів, визначаються взаємовідносини партнера як з державними органами, так і з іншими його контрагентами. Перевіряються наявність позовів, спрямованих на визнання договорів за участю контрагента нікчемними; судові рішення про стягнення боргів з контрагента, наявність яких визначає платоспроможність партнера; порушення справи про банкрутство контрагента.

Участь у тендерних (конкурсних) процедурах передбачає:

контроль за коректністю розкриття тендерних (конкурсних) пропозицій за допомогою членства в тендерному комітеті ;

узгодження договірної документації та перевірка контрагентів, у тому числі наданих ними документів на предмет відповідності кваліфікаційним вимогам ;

вибіркова перевірка об'єктивності проведення конкурсних процедур на предмет фальсифікації або умисної змови; об'єктивності прийняття рішень про закупівлю, вибору контрагента, вартості й умов оплати ;

вибіркова перевірка обґрунтованості закупівлі (за наявності інформації про ознаки фіктивності);

контроль виконання правил приймання, розвантаження й обліку ТМЦ через систему інформування за допомогою охорони (КПП/склади).

У здійсненні закупівель, пов'язаних з будівництвом, монтажем, ремонтом, або наданні інших послуг підрозділ ФЕБ має проводити заходи, спрямовані на попередження та виявлення:

здійснення фіктивних закупівель;

замовлення необґрунтованих проектних (будівельних, монтажних) робіт;

завищення розцінок під час оцінювання вартості проведення робіт;

навмисної підміни в ході будівництва раніше заявлених будівельних матеріалів;

недотримання процедури приймання виконаних робіт.

Вхідний контроль здійснюється шляхом проведення комплексу заходів у ході приймання та відвантаження продукції, контролю над якістю поставленого матеріалу та виконанням договірних зобов'язань постачальниками.

2. *Внутрішній контроль* – це система заходів, спрямованих на забезпечення достовірної інформації про використання фінансових ресурсів, оцінку ефективності господарської діяльності, виявлення та запобігання відхиленням, що перешкоджають законному й ефективному використанню коштів і майна організації. До компетенції внутрішнього контролю відносять виявлення та запобігання:

необґрунтованого списання матеріальних ресурсів;

надмірного та необґрунтованого нарахування заробітної плати;

недотримання штатної дисципліни;

формальне проведення інвентаризацій;

недотримання в процесі фінансово-господарської діяльності вимог чинного законодавства України та стандартів організації;

невиконання керівниками та працівниками структурних підрозділів своїх посадових обов'язків належним чином і в повному обсязі.

3. *Забезпечення фізичного захисту (безпеки) матеріальних об'єктів і цінностей, контролю та регулювання доступу*. Основними завданнями забезпечення безпеки в плані збереження матеріальних цінностей, фізичного захисту об'єктів і персоналу є:

установлення режиму охорони виробничих об'єктів та об'єктів життєдіяльності;

здійснення пропускного та внутрішньооб'єктного режиму;

забезпечення фізичної безпеки персоналу організації;

забезпечення захищеного зберігання цінностей та документів (носіїв інформації), оснащення сучасними інженерно-технічними засобами охорони;

організація фізичного захисту цінностей у процесі їх внутрішньооб'єктного транспортування;

забезпечення взаємодії всіх структур, що беруть участь у забезпеченні фізичного захисту.

Крім того, на службу безпеки та підрозділ охорони покладається: виявлення факту незаконного вилучення ТМЦ з обігу або зберігання, можливість установлення суб'єкта та часу незаконного вилучення ТМЦ, проведення пошуку можливого місця зберігання втрачених ТМЦ на території організації, оперативне інформування керівництва організації про події та критичні ситуації.

4. *Система взаємодії з правоохоронними органами* передбачає:

інформування правоохоронних органів про факти вчинення на території організації дій, які містять ознаки кримінального правопорушення або адміністративно-караного діяння;

надання необхідної допомоги та сприяння правоохоронним органам у виконанні покладених на них завдань;

проведення, з дозволу керівництва організації, спільних перевірок або інших заходів, спрямованих на недопущення фактів розкрадання товарно-матеріальних цінностей, ушкодження майна організації, інших криміногенних проявів на території заводу;

підготовку та подання у правоохоронні та контролюючі органи інформації, необхідної для з'ясування питань, що належать до їх компетенції;

виявлення причин і умов, що сприяють вчиненню правопорушень на території організації, та прийняття, у межах компетенції, необхідних заходів, спрямованих на їх усунення;

забезпечення охорони громадського порядку під час проведення масових заходів з організованою участю співробітників організації (проведення спортивних заходів, святкових концертів тощо).

Усі заходи, що проводяться в рамках взаємодії з правоохоронними органами, виконуються з суворим дотриманням вимог чинного законодавства за умови недопущення фактів порушення прав і свобод громадян, економічних, майнових та іміджевих інтересів організації.

5. *Забезпечення інформаційної безпеки.* Інформаційний захист передбачає створення системи захисту відомостей, які є комерційною таємницею організації, та забезпечення її функціонування, в тому числі через роботу з персоналом, дотримання режиму роботи з даною категорією інформації.

Система захисту інформації, яка є комерційною таємницею організації, передбачає:

порядок віднесення інформації до комерційної таємниці організації та термінів її дії;

систему допуску працівників організації й інших осіб до відомостей, що є комерційною таємницею;

порядок роботи з документами, які мають гриф "комерційна таємниця" та забезпечення їх збереження;

забезпечення захисту інформації, що міститься у електронному вигляді;

обов'язки осіб, допущених до роботи з документами, які є комерційною таємницею;

відповідальність за розголошення комерційної таємниці та втрати документів, що містять відомості, які є комерційною таємницею;

організація контролю за дотриманням режиму безпеки під час роботи, зберігання та передання всіх видів документів, які містять відомості, що є комерційною таємницею.

Усі завдання, розподіл повноважень і відповідальність за їх виконання мають бути розписані у організаційно-розпорядчій та робочій документації підрозділу ФЕБ.

Рекомендована література: [7; 9; 13; 18; 20; 21; 27; 28; 44; 48].

Практична частина

Контрольні запитання

1. Опишіть можливі варіанти організації управління ФЕБ. Охарактеризуйте підрозділ ФЕБ, розкрийте його функції та доцільність організації.
2. Розкрийте послідовність організації й управління ФЕБ, надайте характеристику етапів.
3. Наведіть принципи управління ФЕБ організації, визначте їх сутність.
4. Які чинники обумовлюють вибір організаційної моделі УФЕБ? Розкрийте їх.
5. Наведіть типові види підрозділів, рекомендовані для організації підрозділів ФЕБ.
6. Визначте місце підрозділу ФЕБ у лінійній структурі організації, розкрийте переваги та недоліки такої організації УФЕБ.
7. Проілюструйте місце підрозділу ФЕБ у лінійно-штабній структурі організації, розкрийте переваги та недоліки такої організації УФЕБ.
8. Розкрийте повноваження та функції в управлінні ФЕБ Ради директорів (наглядової ради), Комітету з безпеки ради директорів (наглядової ради), генерального директора, фінансового директора, керівників підрозділів і персоналу компанії.
9. Визначте та прокоментуйте повноваження та функції підрозділу ФЕБ компанії.
10. Проілюструйте й охарактеризуйте можливі організаційні моделі підпорядкованості підрозділів з безпеки.
11. Визначте, в чому має полягати незалежність підрозділу ФЕБ. Розкрийте об'єктивність роботи підрозділу ФЕБ.
12. Наведіть приклади функціональної підзвітності підрозділу ФЕБ. Які функції генерального директора компанії в організації роботи підрозділу ФЕБ?
13. Розкрийте правове та нормативно-методичне забезпечення УФЕБ. Які документи воно включає й якою є послідовність їх формування?

14. Які обов'язки та відповідальність можуть бути покладені на підрозділ з ФЕБ? Які завдання підрозділу ФЕБ?

15. Розкрийте зміст Положення про підрозділ з безпеки організації. Які елементи воно має включати? Наведіть приклади організаційно-розпорядчих документів, що регламентують порядок і правила роботи підрозділу ФЕБ.

Тестові завдання

1. Принцип законності в управлінні ФЕБ – це:

а) розроблення профілактичних заходів проти виникнення реальних загроз;

б) розроблення та запровадження стандартів забезпечення фінансово-економічної безпеки організації, які відповідають нормативно-правовим вимогам;

в) використання всіх наявних у розпорядженні підприємства ресурсів для протидії загрозам;

г) урахування всіх факторів впливу на безпеку підприємства, включення в діяльність з його забезпечення всіх співробітників підрозділів, використання в цій діяльності всіх сил і засобів.

2. Сукупність методів роботи, що застосовуються підрозділом ФЕБ з метою зберегти в таємниці свою діяльність, – це:

а) гласність;

б) законність;

в) конспірація;

г) координація.

3. Максимальна відкритість методів роботи, протилежна конспірації, – це:

а) гласність;

б) законність;

в) конфіденційність;

г) координація.

4. Принцип економічної доцільності в управлінні ФЕБ:

а) вартість фінансових витрат на забезпечення безпеки не повинна перевищувати той оптимальний рівень, за якого втрачається економічний сенс їх застосування;

б) вартість фінансових витрат на забезпечення безпеки виправдовується професіоналізмом кадрів підрозділу ФЕБ, рівнем їх кваліфікації та досвідом роботи;

в) вартість фінансових витрат на забезпечення безпеки становить 15 % витрат компанії;

г) вартість фінансових витрат на забезпечення безпеки становить 15 % чистого прибутку компанії.

5. З якою чисельністю працівників у штаті може створюватися департамент ФЕБ:

а) не менше трьох осіб (включаючи посаду керівника);

б) не менше чотирьох осіб (включаючи посаду керівника);

в) не менше семи осіб (включаючи посаду керівника);

г) не менше п'ятнадцяти осіб (включаючи посаду керівника)?

6. З якою чисельністю працівників у штаті може створюватися служба ФЕБ:

а) не менше трьох осіб (включаючи посаду керівника);

б) не менше чотирьох осіб (включаючи посаду керівника);

в) не менше семи осіб (включаючи посаду керівника);

г) не менше п'ятнадцяти осіб (включаючи посаду керівника)?

7. З якою чисельністю працівників у штаті може створюватися відділ ФЕБ:

а) не менше трьох осіб (включаючи посаду керівника);

б) не менше чотирьох осіб (включаючи посаду керівника);

в) не менше семи осіб (включаючи посаду керівника);

г) не менше п'ятнадцяти осіб (включаючи посаду керівника)?

8. Перевагою якої організаційної структури є чітка підпорядкованість, чіткий розподіл і контроль витрат між підрозділами:

а) лінійної;

б) лінійно-штабної;

в) дивізіональної;

г) матричної?

9. Свобода від умов, які створюють загрозу здатності підрозділу неупереджено виконувати свої обов'язки, – це:

а) об'єктивність;

б) конспірація;

в) гласність;

г) незалежність.

10. Наявність умов неупередженого виконання підрозділом ФЕБ своїх обов'язків – це:

а) об'єктивність;

б) конспірація;

в) гласність;

г) незалежність.

11. До компетенції якого органу входить призначення та зняття з посади керівника ФЕБ:

а) Ради директорів;

б) директора підприємства;

в) корпоративного секретаря;

г) трудового колективу?

12. До компетенції якого органу входить ухвалення концепції, бюджету та ресурсного плану ФЕБ:

а) Ради директорів;

б) директора підприємства;

в) корпоративного секретаря;

г) трудового колективу?

13. До компетенції якого органу входить адміністративне управління системою ФЕБ (ухвалення необхідних організаційно-розпорядчих документів):

а) Ради директорів;

б) директора підприємства;

в) корпоративного секретаря;

г) трудового колективу?

14. До компетенції якого органу входить створення режиму збереження комерційної таємниці:

а) Ради директорів;

б) директора підприємства;

в) корпоративного секретаря;

г) трудового колективу?

15. До організаційних документів, які складаються у підрозділі ФЕБ і прийняті вищими державними органами управління, належать:

а) закони, підзаконні акти, статут, положення, накази, інструкції, методичні рекомендації;

б) статут, положення, посадові інструкції, штатний розклад, правила внутрішнього трудового розпорядку;

в) протоколи, акти, довідки, статут, положення, листи, доповідні та пояснювальні записки, телефонограми, телеграми, досьє;

г) закони, підзаконні акти, статут, положення, накази, інструкції.

Генерали-переможці зазвичай будують військові плани, які будуть працювати незалежно від того, що робить ворог.
Це сутність хорошої стратегії.
Джек Траут

Розділ 4. Планування та координація в системі фінансово-економічної безпеки організації

Після вивчення матеріалів теми ви повинні:

знати:

функції УФЕБ у циклі управління організацією;

змістовність стратегічного та тактичного планування в УФЕБ, структуру бізнес-планів організації;

компоненти та послідовність формування програми та бюджету заходів щодо забезпечення ФЕБ організації;

елементи внутрішніх підрозділів організації з вирішення завдань забезпечення ФЕБ;

напрями зовнішньої взаємодії щодо запобігання злочинних посягань і проведення спільних заходів з безпеки діяльності організацій;

уміти:

описувати механізм управління ФЕБ;

упорядковувати й описувати стратегічні, тактичні та річні плани УФЕБ;

формувати програму заходів із забезпечення ФЕБ, визначати її елементи;

визначати елементи та формувати програму та бюджет заходів ФЕБ організації;

здійснювати взаємодію з внутрішніми та зовнішніми суб'єктами щодо ФЕБ організації.

План теми

4.1. Механізм управління фінансово-економічною безпекою.

4.2. Стратегічне та тактичне планування в управлінні фінансово-економічною безпекою.

4.3. Програма забезпечення фінансово-економічної безпеки організації.

4.4. Взаємодія підрозділу фінансово-економічної безпеки з іншими підрозділами організації та зовнішніми структурами щодо протидії загрозам.

Ключові поняття та терміни: організація, механізм управління, стратегічне планування, тактичне планування, програма, взаємодія, повноваження.

4.1. Механізм управління фінансово-економічною безпекою

Організаційний механізм УФЕБ – це СФЕБ організації в дії.

Управління безпекою знаходить своє відображення в циклі управління організацією (рис. 4.1): планування, організація, мотивація, облік і контроль, регулювання [26].

Плануванню належить вирішальне значення, оскільки розроблення плану передбачає вибір напряму розвитку організації, визначення складу та послідовності робіт, обґрунтований відбір коштів для реалізації політики безпеки. За результатом аналізу стану системи та побудови дерева цілей здійснюється вибір альтернатив, визначається певний варіант розвитку та забезпечення безпеки.

Для управління в перспективі використовується інформація, сформована на підставі даних прогнозних оцінок, кількісних і якісних характеристик бажаного стану суб'єкта господарювання. У такому циклі управління особливу роль виконує моніторинг. Тут інформація піддається оцінюванню щодо актуальності, достовірності та цінності. Отримувати інформацію про стан суб'єкта господарювання та конкурентного середовища, виявляти й оцінювати фактори загроз внутрішнього та зовнішнього впливу можна тільки в системі стратегічного моніторингу.

Організація передусім забезпечує ефективне функціонування організації, розроблення та реалізацію стратегії розвитку, формування структури системи безпеки суб'єкта господарювання й умов її забезпечення. Організаційно-функціональне забезпечення відповідає за чітку підготовку й організацію розподілу праці за функціональними підсистемами, підрозділами, виконавцями та рівнями управління та створення умов для ефективного виконання робіт, передбачаючи відповідне інформаційне, методичне, технічне та кадрове забезпечення.

Регулювання передбачає уточнення планів і заходів із забезпечення безпеки в рамках функціонування та розвитку організації та коригування процесів управління на підставі аналізу змін організації.

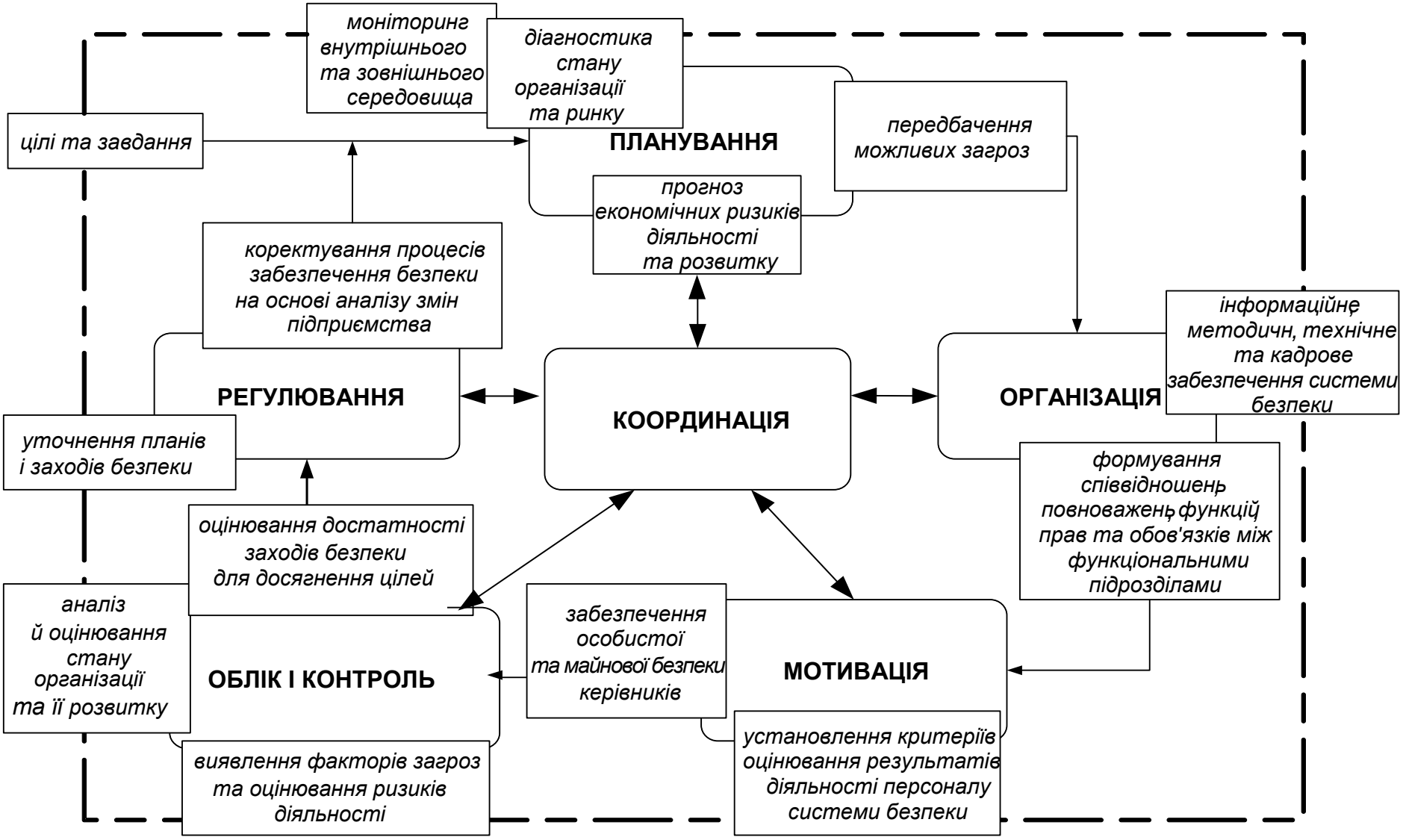

Рис. 4.1. **Організаційний механізм управління фінансово-економічною безпекою організації**

Ця функція, враховуючи впливи зовнішнього середовища, дозволяє досягати запланованого стану організації. Функція мотивації сприяє активізації процесів саморозвитку працівників організації, підвищення їх компетентності та максимальній віддачі творчого й інноваційного потенціалу персоналу управління та керівної ланки, стимулювання зацікавленості у вирішенні поставлених перед ними завдань.

Механізм мотивації реалізується таким чином: на перших кроках становлення та розвитку свідомості індивідууму, під впливом безпосереднього оточення (людського фактора) та суспільства в цілому; в результаті поетапного усвідомлення інстинктів, осмислення сукупності потреб і оцінювання власних можливостей формується система інтересів особистості, яка обумовлює більшість її подальших дій.

Механізм організації, дія важелів мотивації поведінки особистості ґрунтуються не тільки на її безпосередніх потребах, що реалізуються у вигляді системи усвідомлення та задоволення власних потреб. Громадський вплив цілеспрямовано формує інтереси, які виходять за межі безпосередніх потреб особистості та певним чином мотивують відповідну активність. Їх дія обумовлена інтеграцією особистості в соціум, відображає соціальний характер безпосередньої взаємодії індивідуума з оточуючими, особливості побудови його взаємин із суспільством у цілому.

Ряд дій індивідуума, форми прояву та змістовність яких залежать від рівня розвитку його інтелектуальної організації та сукупності особистих якостей, продовжують визначатися безпосередньо неосмисленими потребами та навіть неусвідомленими інстинктами. Вони також обумовлюють і формують певні мотиви поведінки індивідуума, які у вигляді прихованих важелів нерідко спонукають його до частково або повністю неусвідомлених вчинків.

Природно, що подібні дії можуть порушувати інтереси інших. Це, відповідно, спонукає оточуючих до протидії та, нарешті, до відкритого зіткнення. Такий розвиток ситуації руйнує соціальну організацію та змушує суспільство вживати відповідні заходи безпеки. Механізм соціальної організації стабілізує розвиток подібних тенденцій, забезпечуючи своєчасне застосування ефективних заходів впливу. Теоретично подібні заходи можуть включати найрізноманітніший спектр як превентивних, так і оперативних реакцій соціуму. Проте на практиці вони здійснюються у вигляді формування та застосування певної жорсткої системи примусу індивідуума до дотримання певних норм поведінки в суспільстві.

З метою забезпечення ефективної координації та гармонійної взаємодії індивідуумів організація або суспільство в цілому формують систему зовнішніх інструментів впливу на особистість. Така система є універсальною палітрою різноманітних стимулів, що примушують індивідуума або цілу групу до певної активності, цілеспрямованої діяльності, дотримання сформованих норм поведінки.

Таким чином, управління безпекою організації означає управління поведінкою та мотивацією персоналу. Ця функція безпекової політики формує мотиви та стимули забезпечення особистої та майнової безпеки керівників управлінської ланки як гарантів надійності та сталості функціонування та розвитку організації.

Координація дії забезпечує узгодження й ув'язку між цілями та завданнями поточного та стратегічного управління. Хоча вибір і пріоритети організацій природним чином розрізняються, економічні цілі мають найбільший вплив на їх поведінку, формуючи основу ієрархії в структурі цілей. Це пояснюється тим, що тільки ефективне функціонування організації може знайти внутрішні засоби для постановки та реалізації довгострокових цілей розвитку. Економічні цілі спрямовані на оптимізацію процесів використання ресурсів організації та забезпечення достатнього рівня повернення інвестицій у довгостроковому періоді.

Соціальні або позаекономічні цілі, що відповідають потребам і особистим прагненням працівників організації, очікуванням впливових зовнішніх представників (зовнішні акціонери, кредитори, органи влади, громадські організації), надають вторинний вплив на поведінку системи управління. На додаток до цих цілей можна виділити ще два фактори, що впливають на поведінку керівництва організації: обов'язки й обмеження. Тому одним із завдань функції координування є досягнення балансу суспільних, групових і приватних інтересів між працівниками, персоналом управління та керівною ланкою організації як основа гарантування їх спільної безпеки.

Функції обліку та контролю на підставі зіставлення планових і фактичних параметрів станів системи дозволяють проаналізувати й оцінити достатність заходів з безпеки. Управлінська діяльність спрямована на керовані об'єкти. Її можна аналізувати й оцінювати за рівнем стану та безпеки організації, сталості її функціонування та розвитку. Результатом управління є відображення взаємодії суб'єктів і об'єктів управління, його визначення має комплексний характер і позначається на стані організації та її складових.

Дане положення обумовлює формування нових підходів до оцінювання системи безпеки організації з метою визначення оцінки процесів змін стану організації й економічної ефективності системи безпеки. Така оцінка повинна бути доповнена оцінкою рівня особистісних якостей персоналу системи безпеки організації. Шкала координатних вимог такої оцінки повинна включати рівень професійної підготовки, загальнокультурного та морального розвитку, фізичних, психологічних та інших особистісних якостей керівників.

Ці основні управлінські функції зв'язуються в єдиний процес управління такими діями, як комунікація та прийняття рішень. Крім зазначених, важливою функцією механізму управління організацією є функція, яка об'єднує ланки між зовнішнім і внутрішнім середовищами організації. У даному аспекті функція механізму управління безпекою здійснюється на базі комплексного дослідження впливу факторів загроз зовнішнього середовища на стан і передумови розвитку організації.

4.2. Стратегічне та тактичне планування в управлінні фінансово-економічною безпекою

В основному місія ФЕБ полягає в тому, щоб убезпечити організацію від злочинного посягання співробітників організації, клієнтів і контрагентів, а також наданні гарантій у тому, що власність організації буде захищена від шахрайства й інших посягань. За допомогою спеціальних методів і засобів ФЕБ сприяє скороченню зайвих грошових втрат для організації, одночасно захищаючи її імідж. За відсутності плану забезпечення ФЕБ не може гарантувати виконання заходів у повному обсязі. Відповідно, власники, акціонери та керівники не будуть впевнені в тому, що їх активи будуть належним чином захищені та збережені. Отже, це впливає на продуктивність роботи співробітників організації, а також на їх ставлення до активів організації. Таким чином, підвищується ймовірність різного роду розкрадань, викривлень результатів роботи, саботажу. Така ситуація позначається і на людському факторі, зменшуючи бойовий дух персоналу, його готовність добре виконувати свою роботу та захищати активи організації за власною ініціативою. Іншим наслідком може бути і те, що відвідувачі (особливо постачальники та клієнти), які сумніваються в достатності безпеки організації, не будуть впевнені, що їх продукція й інтелектуальна

власність захищається належним чином. Отже, клієнти організації не повинні відчувати вразливість з боку персоналу, будучи змушені вимагати підвищення безпеки.

Усе це підкреслює важливість розроблення лаконічного, функціонального та прозорого плану ФЕБ організації. Керівники всіх рівнів повинні зрозуміти та прийняти план забезпечення безпеки у своїх підрозділах і бізнес-одиницях. Крім того, менеджери повинні усвідомлювати, що такий план є обов'язковим не тільки для керівника служби безпеки організації, це відповідальність кожного окремого керівника. Для цього керівникам усіх бізнес-одиниць необхідно узгоджено діяти з керівником підрозділу ФЕБ, щоб гарантувати виконання політики та процедур у сфері забезпечення плану безпеки організації. Керівники підлеглих підрозділів і бізнес-одиниць організації мають довести план до кожного співробітника та пересвідчитися в тому, що він ними засвоєний.

Керівник безпеки повинен розуміти особливості бізнесу та конкуренції як на рівні ділового середовища, так і в світовому масштабі. Це означає, що він повинен ознайомитися з планами розвитку організації. Такі плани включають стратегічний, тактичний та річний бізнес-плани. Їх складають на рівні виконавчого керівництва та передають усім підрозділам і бізнес-одиницям організації. Керівники підрозділів доповнюють цю інформацію, докладаючи внеску в загальну концепцію безпеки. Надалі така інформація розглядається й ухвалюється на рівні виконавчого керівництва. Затверджені плани передаються в підрозділи та бізнес-одиниці організації, які розробляють свої функціональні плани з підтримки загального плану розвитку організації (рис. 4.2).

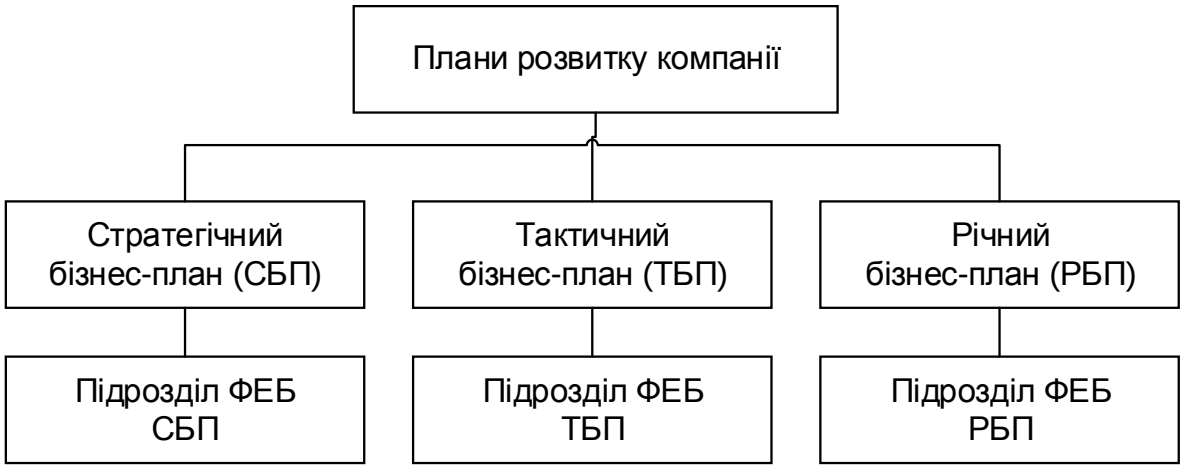

Рис. 4.2. **Структура бізнес-планів компанії**

Стратегічний бізнес-план (СБП) описує стратегію організації для підтримки конкурентоспроможності в області проектування, виробництва та продажу товарів і послуг. Цей план установлює базові напрями, яких організація буде дотримуватися протягом наступних п'яти-семи років. Він є довгостроковим планом організації. СБП складається на термін, який не перевищує семи років, оскільки мінливі умови, викликані розвитком технологій і можливою зміною конкурентоспроможності та бізнес-середовища організації, не дозволяють розробляти його на більший період. Стратегічний бізнес-план встановлює:

очікуваний річний прибуток протягом наступних семи років;

щорічні показники ринкової частки;

майбутні проекти модернізації, засновані на очікуваних змінах у технології, більш швидких, дешевих і більш потужних інформаційних і програмних продуктів;

цілі розширення бізнесу;

придбання субпідрядників та інших конкурентоспроможних організацій, злиття бізнесу.

Стратегічний і *тактичний бізнес-плани* (СБП, ТБП) підрозділу ФЕБ є програмою із забезпечення ФЕБ організації. ТБП призначений захистити цінні активи організації, особливо її конфіденційну інформацію та бізнес-процеси, одночасно забезпечуючи доступ до цих активів з боку міжнародних і національних клієнтів і контрагентів. Такий план:

здатний підтримувати безпечну інтеграцію процесів організації та систем з іншими суб'єктами ринку;

передбачає стратегії, необхідні для підтримки СБП організації.

В. П. Мак-Мак стратегію безпеки суб'єкта господарювання визначає як сукупність найбільш значущих рішень, спрямованих на забезпечення прийнятного рівня безпеки функціонування організації. Він виділяє такі типи стратегій безпеки [17]:

1) орієнтовані на усунення існуючих або запобігання виникнення можливих загроз;

2) націлені на запобігання впливу існуючих або можливих загроз на предмет безпеки;

3) спрямовані на відновлення або компенсацію збитку.

Перші два типи стратегій передбачають таку діяльність із забезпечення безпеки, в результаті якої не відбувається загрози або створюється

перепона її впливу. У третьому випадку збиток допускається (виникає), однак він компенсується діями, які передбачає відповідна стратегія. Цілком очевидно, що стратегії третього типу можуть розроблятися та реалізовуватися стосовно до ситуацій, де збитки можна нівелювати або коли немає можливості здійснити яку-небудь програму реалізації стратегій першого або другого типу.

Власний ТБП підрозділу ФЕБ – це, як правило, трирічний план, який встановлює більш чіткі цілі, наміри та завдання. ТБП є короткодіючим планом, який використовується на підтримку СБП.

ТБП спрямований також на захист активів і конфіденційної інформації організації і його бізнес-процесів, водночас надаючи доступ до них у міру необхідності в межах контрактних угод з національними та міжнародними клієнтами та контрагентами. ТБП включає опис необхідних спеціальних методів і засобів, процесів гарантування безпеки з описом необхідного мінімального часу та витрат ресурсів.

Керівник підрозділу ФЕБ має завжди пам'ятати, що інформація є конфіденційною та чутливою до змін зовнішнього середовища, її вартість залежить від часу та змінюється зі зміною кон'юнктури ринка. Тому і інформація, що міститься в планах, має бути захищена з використанням тих методів, які необхідні тільки на визначений період, виходячи зі зміни її вартості з часом. СБП і ТБП мають бути взаємоузгодженими.

Річний бізнес-план (РБП) установлює свої цілі та завдання на рік. РБП організації визначає конкретні проекти, які будуть реалізовані та завершені до кінця року. Успішне завершення цих проектів буде сприяти успіху тактичного та стратегічного бізнес-планування організації.

Таким чином, усі три типи планів організації (СБП, ТБП і РБП) мають бути підтримані з боку УФЕБ. Керівник підрозділу ФЕБ має ознайомитися з ними та розкласти на різні елементи. Цими елементами є окремі напрями та цілі організації, які дозволяють успішно конкурувати на ринку (національному або світовому). СФЕБ має гарантувати заявлене в планах і надавати їх більшу деталізацію.

Важливо, щоб інтерпретація різних планів керівником ФЕБ була правильною, тому що програма забезпечення безпеки не може ґрунтуватися на помилкових припущеннях. Саме тому керівник підрозділу ФЕБ має входити до складу робочих груп із вироблення стратегічних і тактичних

планів, зустрічатися з ключовими співробітниками організації, ставити запитання в разі потреби. Нерозуміння або неправильне тлумачення планів керівником ФЕБ буде вважатися непрофесійним.

4.3. Програма забезпечення фінансово-економічної безпеки організації

Підрозділи корпоративної безпеки мають підтримувати розвиток організації через втілення бізнес-планів (стратегічних, тактичних, річних). Це потребує наявності програми захисту, яка:

мінімізує вірогідність успішної атаки з боку джерел загрози функціонуванню та розвитку організації;

мінімізує втрати, якщо атака загрози відбувається;

проводить заходи швидкого реагування та відновлення у разі успішної атаки.

Уся діяльність із забезпечення ФЕБ організації повинна будуватися на основі комплексної програми забезпечення економічної безпеки організації, підпрограм забезпечення безпеки за основними його видами (фінансової, екологічної, інформаційної тощо) та розроблюваних для їх виконання планів роботи підрозділів організації й окремих працівників.

Орієнтовна програма економічної безпеки суб'єкта господарювання (табл. 4.1) включає конкретні заходи, згруповані за розділами, які підкріплюються необхідними розрахунками ресурсного забезпечення та системою персоніфікованої відповідальності за виконання заходів.

Таблиця 4.1

Структура та склад комплексної програми економічної безпеки суб'єкта господарювання

Розділи програми	Підрозділи програми	Змістовність підрозділів
1	2	3
Захист бізнес-середовища	Діловий моніторинг	Збирання відомостей про контрагентів і конкурентів

Закінчення табл. 4.1

1	2	3
	Моніторинг внутрішнього середовища	Контроль лояльності персоналу, соціально-психологічного клімату в колективі
	Формування іміджу	Створення та підтримка іміджу юридично та соціально відповідального організації
Захист інформаційних ресурсів і нематеріальних активів	Захист інформаційних ресурсів	Забезпечення збереженості інформаційних систем, програмного забезпечення й інформації; захист від витоку інформації
	Захист нематеріальних активів	Захист інтелектуальної власності, майнових прав, гудвіл
Захист матеріально-технічних ресурсів	Пропускний режим	Фізичний захист ресурсів організації від розкрадань, псування
	Пожежна охорона	Забезпечення протипожежної безпеки
	Техніка безпеки	Захист ресурсів організації від технічних ризиків
Захист фінансових ресурсів	Фінансовий моніторинг	Контроль платоспроможності та фінансової стійкості організації
	Страхування	Захист ресурсів шляхом передання відповідальності страховим компаніям
	Правовий захист	Оформлення й юридичне супроводження документації організації
Захист трудових ресурсів	Кадровий менеджмент	Захист від кадрових ризиків, робота з персоналом, який приймається на роботу та звільнюється
	Соціальний захист	Соціальне та пенсійне страхування, реалізація соціальних програм

Комплексна програма безпеки організації має передбачити форми та методи роботи підрозділів, які її забезпечують. Серед існуючих засобів забезпечення безпеки можна виділити:

технічні засоби. До них відносять охоронно-протипожежні системи, відео-радіоапаратуру, засоби виявлення вибухових пристроїв, бронежилети, загородження та ін.;

організаційні засоби. Створення спеціалізованих організаційних формувань, що забезпечують безпеку організації;

інформаційні засоби. Насамперед це друкована та відеопродукція з питань збереження конфіденційної інформації. Важлива інформація для прийняття рішень з питань безпеки зберігається в комп'ютерах;

фінансові засоби. Цілком очевидно, що без достатніх фінансових засобів неможливе функціонування системи безпеки, питання лише в тому, щоб використовувати їх цілеспрямовано та з високою віддачею;

правові засоби. Тут мається на увазі використання не тільки виданих вищими органами влади законів і підзаконних актів, а також розроблення власних, так званих локальних правових актів з питань забезпечення безпеки;

кадрові ресурси. Це насамперед достатність кадрів з питань забезпечення безпеки. Одночасно з виконанням прямих обов'язків вони мають постійно підвищувати свою професійну майстерність у цій сфері діяльності;

інтелектуальні засоби. Залучення до роботи висококласних фахівців, наукових працівників (іноді доцільно залучати їх ззовні) дозволяє впроваджувати нові системи безпеки.

Слід зауважити, що окреме застосування кожного зі вказаних засобів не дає необхідного ефекту, він можливий тільки на комплексній основі. Проте необхідно зазначити, що одночасне запровадження всіх ресурсів у принципі неможливе. Воно проходить через низку етапів:

I етап – виділення фінансових коштів;

II етап – формування кадрових і організаційних засобів;

III етап – розроблення системи правових засобів;

IV етап – залучення технічних, інформаційних та інтелектуальних засобів.

Переведені зі статичного в динамічний стан, такі засоби стають методами, тобто прийомами, способами дії. Відповідно, можна говорити про технічні, організаційні, інформаційні, фінансові, правові, кадрові й інтелектуальні методи. Наприклад:

технічні – спостереження, контроль, ідентифікація;

організаційні – створення зон безпеки, режим, розслідування, пости, патрулі;

інформаційні – складання детективами характеристик на працівників, аналітичні матеріали й обліки конфіденційного характеру;

фінансові – матеріальне стимулювання співробітників, які мають досягнення у забезпеченні безпеки, грошове заохочення інформаторів;

правові – дозволи, судовий захист законних прав та інтересів, сприяння правоохоронним органам;

кадрові – підбір, розстановка та навчання кадрів, які забезпечують безпеку організації, їх виховання;

інтелектуальні – патентування, ноу-хау.

Механізм реалізації програми економічної безпеки передбачає:

створення координаційного центру (комітету з безпеки) на чолі з керівником організації, оперативним органом якого є підрозділ ФЕБ;

розроблення та затвердження наказом по організації нормативно-методичного забезпечення програми;

визначення ресурсного забезпечення та цільового використання ресурсів.

Останнє передбачає складання бюджету заходів щодо забезпечення ФЕБ організації.

4.4. Взаємодія фінансово-економічної безпеки з іншими підрозділами організації та зовнішніми структурами щодо протидії загрозам

Організаційно в управлінні фінансово-економічною безпекою (зокрема його основного підрозділу) приймають участь такі функціональні служби, як: фінансово-економічна, бухгалтерія, юридична, управління персоналом, кадровий відділ, матеріально-технічного постачання, внутрішнього аудиту та ревізії, матеріально-технічного забезпечення.

У процесі організації СФЕБ важливо правильно вибудувати взаємодію служби фінансово-економічної безпеки й інших функціональних підрозділів (рис. 4.3). Помилковий розподіл функцій між ними або неправильна побудова регламентів взаємодії може призвести до хибних дій або до конфлікту в організаційній структурі суб'єкта господарювання.

Бухгалтерія здійснює контроль за збереженням власності організації, цільовим витрачанням грошових коштів і матеріальних цінностей, своєчасним проведенням інвентаризації, правильним веденням розрахунків із заробітної плати, податковим обліком. Бухгалтерський облік відображає факти вже виконаних операцій, формуючи первинний документальний контроль усієї фінансово-господарської діяльності організації.

Юридичний відділ несе відповідальність за правовстановлювальні документи, розробляє Положення про порядок укладання договорів і, якщо суб'єкт господарювання є акціонерним товариством, може відповідати за ведення реєстру акціонерів або взаємодію з реєстратором.

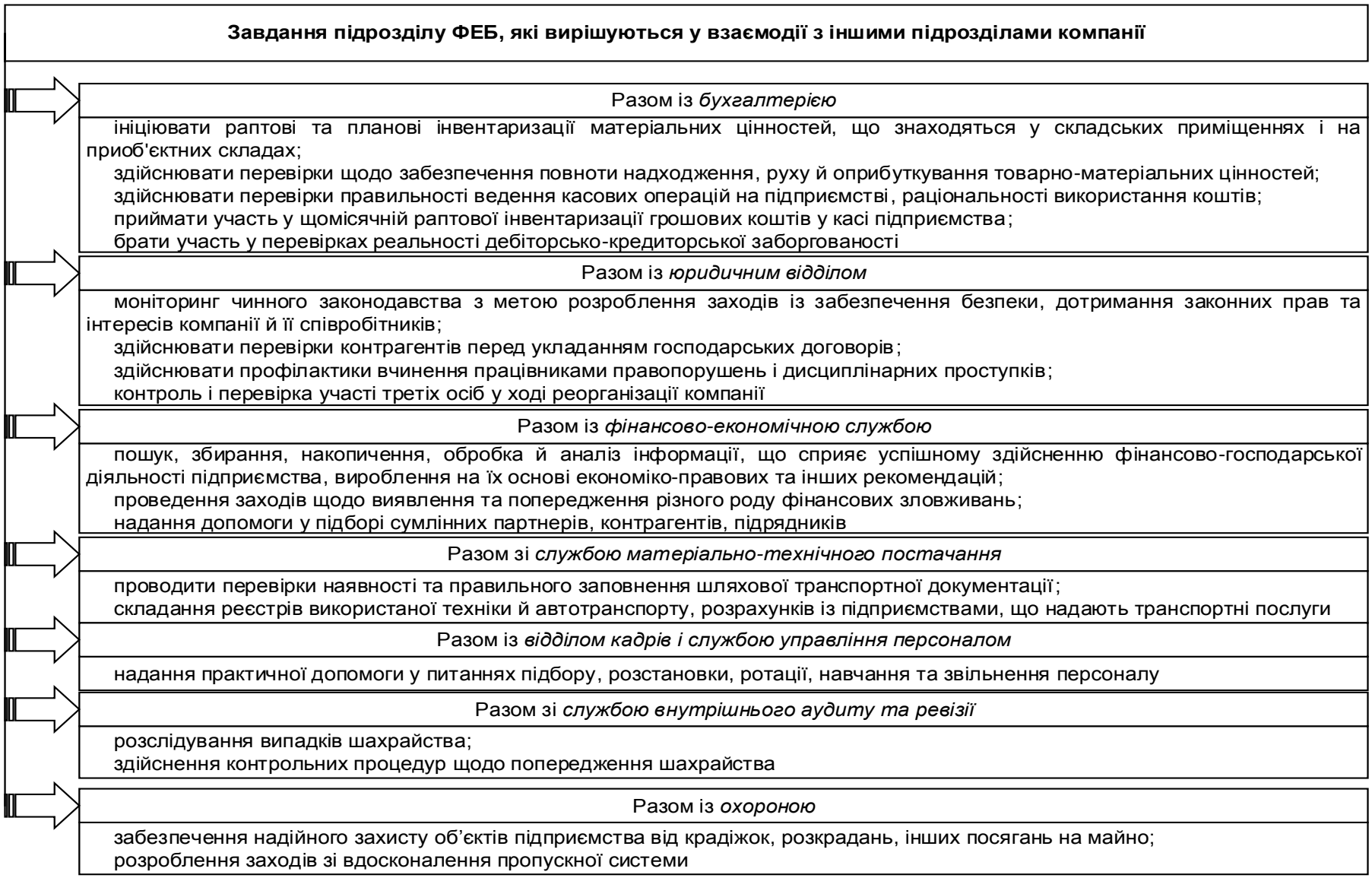

Рис. 4.3. **Структура взаємодії підрозділу ФЕБ з іншими підрозділами організації**

Юридичний відділ відповідає за виконання всіх стандартних обов'язків, пов'язаних з юридичним супроводженням діяльності організації, у тому числі надання консультацій та допомоги керівникові та співробітникам ФЕБ на вимогу або за необхідності.

Фінансово-економічна служба – головний інструмент регулювання та контролю фінансового результату бізнесу. Її правильна організація дозволяє досягти істотного зростання прибутку без серйозних додаткових вкладень і технологічних інновацій. Вона формує систему планування та збирання звітної інформації, визначає методологію, аналітику та склад форм планування та звітності. Фінансово-економічна служба відповідає за планування та збирання фактичної інформації, необхідної для ефективного управління, з періодичністю та в аналітиці. Безумовно, в її роботі повинні враховуватися потреби служби ФЕБ.

Відділ кадрів і служба управління персоналом, як випливає з назви, організовують кадрову роботу та займаються питаннями співробітників, (такими, як перевірка достовірності анкетних і професійних даних претендентів на окремі кадрові позиції, скарги співробітників) і сповіщає керівників про дисципліну працівника. Ці служби встановлюють правила перевірки нових співробітників, а часто і перелік відомостей та складових комерційної таємниці та правила роботи з ними.

Відділ матеріально-технічного постачання здійснює забезпечення виробничих підрозділів організації матеріально-технічними ресурсами, проводить підготовку й укладання договорів на поставку матеріально-технічних ресурсів, організацію раціонального використання матеріально-технічних ресурсів.

Внутрішній аудит і ревізія мають гарантувати, що суб'єкт господарювання працює, а його працівники виконують свої обов'язки відповідно до чинного законодавства, корпоративної політики та процедур. Внутрішній аудит і ревізія проводять періодичні перевірки фінансово-господарської діяльності підрозділів і, що дуже важливо, контролюють дотримання регламентів управління. Керівники внутрішнього аудиту та ФЕБ обмінюються інформацією, що представляє взаємний інтерес.

Служба ФЕБ веде постійний моніторинг функціонування найважливіших підсистем управління організації, виявляє випадки суттєвих

відхилень від встановлених нормативів, аналізує їх причини, веде оперативну роботу з профілактики та запобігання порушенням.

Особливу увагу в процесі повсякденної діяльності УФЕБ слід приділяти постійній взаємодії з державними та правоохоронними органами, а саме: з органами державної влади, органами місцевого самоврядування, силовими структурами (СБУ, МВД, ДПАУ та іншими), державними та недержавними підприємствами, установами й організаціями, громадськими об'єднаннями та громадянами. Метою співпраці є запобігання злочинних посягань і проведення спільних заходів щодо забезпечення безпеки діяльності установ, організацій, підприємств.

Взаємодія підрозділу ФЕБ і правоохоронних структур може здійснюватися за такими напрямами:

кадри – перевірка правоохоронними органами кандидатів на роботу, спільне розроблення та запровадження правил щодо відповідальності персоналу за протиправне використання або розголошення комерційної таємниці, повідомлення керівників організації про порушення щодо конкретних осіб, підготовка працівників служб безпеки за допомогою правоохоронних органів. Робота з підбору, розстановки, професійної, спеціальної підготовки персоналу служби безпеки;

інформація – обмін взаємною інформацією про: способи вчинення протиправних дій, факти (способи) розкрадання грошових коштів з використанням підроблених банківських документів, кредитних карток та інших документів; потенційно небезпечних осіб, які працюють в організаціях, і підозрюваних у скоєнні злочинів або таких, які знаходяться в розшуку та ін.

організаційна взаємодія – створення системи спільної протидії незаконній діяльності з боку фізичних і юридичних осіб (організація охорони, встановлення сигналізації, системи швидкого оповіщення правоохоронних органів; участь у формуванні централізованого, регіонального банку даних про організації різних форм власності, недобросовісних учасників ділових операцій, кримінальних авторитетів).

Працівники служби безпеки повинні знати, що правопорушення, яке вони виявили з боку інших осіб, може спричинити настання відповідальності, яка має як цивільно-правовий, так і кримінальний характер. Ця тема достатньо розкрита авторами посібника з економічної безпеки [13].

Взаємодія служб безпеки організацій з державними правоохоронними органами є дуже серйозною, проте не вповні законодавчо вирішеною проблемою. Тому досі в діяльності цих органів та підприємницьких структур існує чимало проблем і навіть суперечностей. Це нерідко призводить до незахищеності підприємців перед неправомірними діями працівників поліції та контролюючих органів і навіть до порушення їх прав і свобод як громадян і власників.

Рекомендована література: [13; 18; 27].

Практична частина

Контрольні запитання

1. Надайте визначення механізму управління ФЕБ організації, визначте та розкрийте його основні функції.
2. Доведіть необхідність планування в управлінні ФЕБ організації.
3. Розкрийте структуру бізнес-планів організації, визначте стратегічний, тактичний та річний плани.
4. Розкрийте призначення та змістовність стратегічного бізнес-плану підрозділу ФЕБ.
2. Розкрийте призначення та змістовність тактичного та річного бізнес-планів підрозділу ФЕБ.
3. Доведіть необхідність розроблення програми ФЕБ організації.
4. Наведіть структуру та склад орієнтовної програми економічної безпеки організації.
5. Розкрийте методи та засоби, використовувані для забезпечення ФЕБ організації.
6. З якими підрозділами організації взаємодіє підрозділ ФЕБ для виконання своїх функцій? Визначте завдання, які вони вирішують сумісно.
7. З якими зовнішніми структурами взаємодіє підрозділ ФЕБ для протидії загрозам і з яких питань?

Тестові завдання

1. Який з видів планів установлює базові напрями, яких підприємство буде дотримуватися протягом наступних п'яти-семи років:

а) річний;

б) стратегічний;

в) тактичний;

г) фізичний?

2. Який з видів планів установлює очікуваний річний прибуток у довгостроковій перспективі, щорічні показники ринкової частки, організаційні та технологічні проекти, цілі розширення бізнесу:

а) річний;

б) стратегічний;

в) тактичний;

г) фізичний?

3. Сукупність найбільш значущих рішень, спрямованих на забезпечення прийнятного рівня безпеки функціонування підприємства визначається як:

а) стратегія;

б) тактика;

в) програма;

г) бюджет.

4. Який з видів планів, що включає опис необхідних спеціальних методів і засобів, процесів гарантування безпеки з описом необхідного мінімального часу та витрат ресурсів, приймається на період максимум до трьох років:

а) річний;

б) стратегічний;

в) тактичний;

г) фізичний?

5. Який документ описує комплекс дій підрозділів щодо забезпечення ФЕБ:

а) стратегія;

б) тактика;

в) програма;

г) бюджет?

6. Контроль платоспроможності та фінансової стійкості підприємства знаходиться в компетенції:

а) фінансового моніторингу;

б) страхування;

в) правового захисту;

г) кадрового менеджменту.

7. Фізичний захист ресурсів організації від розкрадань, псування знаходиться в компетенції:

а) захисту інформаційних ресурсів;

б) захисту нематеріальних активів;

в) пропускного режиму;

г) техніки безпеки.

8. Який з підрозділів підприємства здійснює контрольні процедури щодо попередження шахрайства з боку відповідальних осіб:

а) юридичний;

б) охорони;

в) внутрішнього аудиту;

г) фінансово-економічний?

9. Який з підрозділів підприємства формує систему планування та збирання звітної інформації, визначає методологію, аналітику та склад форм планування та звітності, відповідає за збирання фактичної, яка необхідна для ефективного управління ФЕБ, інформації з періодичністю та в аналітиці:

а) юридичний;

б) бухгалтерія;

в) фінансово-економічний;

г) відділ кадрів?

10. Який з підрозділів підприємства займається питаннями співробітників перевіркою достовірності анкетних даних претендентів на окремі вакантні позиції, скаргами співробітників і сповіщає керівників про дисципліну працівника:

а) юридичний;

б) бухгалтерія;

в) фінансово-економічний;

г) відділ кадрів?

Бізнес – дуже проста річ. Єдина складність у ньому – це люди.
Фахівці HR-департаментів.
Якби шахраї знали всі переваги чесності, то вони заради вигоди перестали б шахраювати.
Бенджамін Франклін

Розділ 5. Кадрова безпека в системі фінансово-економічної безпеки організації

Після вивчення матеріалів теми ви повинні:

знати:

зміст кадрової безпеки, внутрішні та зовнішні загрози організації з боку персоналу;

чинники, що призводять до шахрайства в організації;

методи попереджувально-профілактичного характеру забезпечення кадрової безпеки в організації;

техніки та прийоми роботи з персоналом у системі ФЕБ;

ключові вимоги до професіоналів підрозділу ФЕБ;

уміти:

виявляти загрози з боку персоналу організації;

ідентифікувати дії з боку персоналу, що призводять до шахрайства в організації;

демонструвати володіння профілактичними методами й агентурними техніками роботи в сфері УФЕБ;

уміти оцінювати стан управління персоналом підрозділу ФЕБ;

демонструвати етичну відповідальність у сфері УФЕБ.

План теми

5.1. Кадрова безпека організації, її сутність і чинники загроз.

5.2. Система мотивації та культура безпеки організації.

5.3. Профілактичні методи кадрової безпеки в системі фінансово-економічної безпеки.

5.4. Техніки агентурної роботи професіоналів з фінансово-економічної безпеки.

5.5. Управління персоналом та етична відповідальність підрозділу фінансово-економічної безпеки.

Ключові поняття та терміни: кадрова безпека, персонал, шахрайство, методи, техніки, культура, етика.

5.1. Кадрова безпека організації, її сутність і чинники загроз

Кадрова безпека – це процес запобігання негативним впливам на корпоративну (економічну) безпеку організації через ризики та загрози, пов'язані з персоналом, його інтелектуальним потенціалом і трудовими відносинами у цілому. Кадрова безпека відіграє домінантну роль у системі корпоративної безпеки, оскільки це робота з персоналом, кадрами, а вони в будь-якій організації первинні. Персонал – це не тільки інструмент для залучення прибутку в компанію, її розвитку, але і загрози, які можуть спричинити істотний негативний вплив на бізнес.

Людський фактор у питаннях забезпечення безпеки організації відіграє ключову роль, змушуючи керівництво серйозно замислитись над ретельністю підбору персоналу. Розподіл найбільш розповсюджених внутрішніх і зовнішніх загроз організації з боку схематично подані на рис. 5.1.

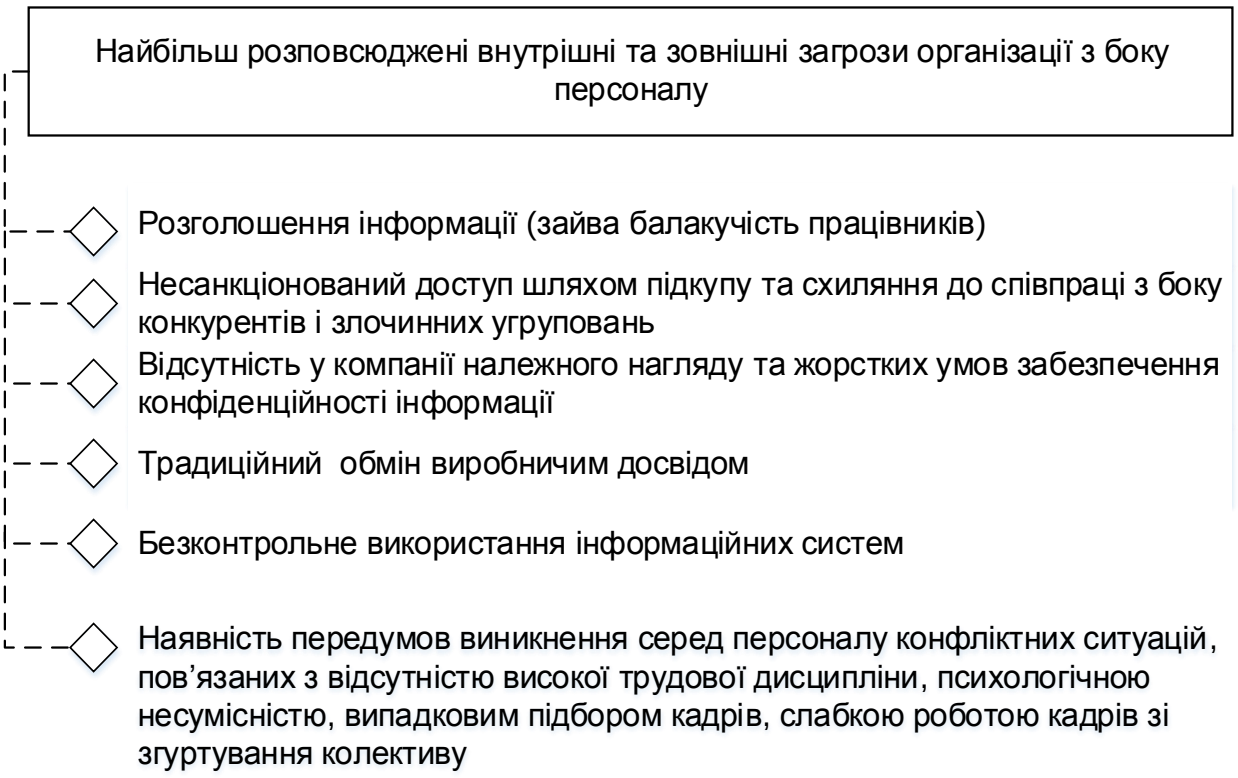

Рис. 5.1. **Найбільш розповсюджені внутрішні та зовнішні загрози організації з боку персоналу**

Завдання підрозділу з безпеки полягає не тільки в запобіганні нанесенню фінансово-економічної або моральної шкоди ззовні, але і в забезпеченні гарантій внутрішньої безпеки – запобігання нанесення збитку компанії її співробітниками.

Ймовірні фактори виникнення загроз кадровій безпеці організації можна розподілити на внутрішні та зовнішні.

Внутрішні загрози:

неякісний вхідний контроль під час наймання нових співробітників;

відсутність системи внутрішнього контролю або слабкість її організації, дублювання функцій контролю (відсутні служба безпеки, служба внутрішнього аудиту та система нетерпимості до різного роду недобросовісних дій);

відсутність чіткої, прозорої організаційної структури й адекватного розподілу повноважень;

недосконалість правил роботи з секретною інформацією та документами, відсутність юридичних зобов'язань щодо нерозголошення інформації під час роботи та після звільнення;

незадоволеність умовами праці, рівнем її оплати, методами мотивації, стилем управління персоналом, відсутністю стабільності колективу, невмотивованість у досягненні цілей, відсутність можливостей особистісного зростання;

плинність управлінського персоналу, скорочення/реорганізація;

невідповідність займаній посаді – можливість допущення помилок через некомпетентність;

відсутність кодексу корпоративної етики та чітких правил "що добре, а що погано" всередині компанії, зневажливе ставлення з боку керівництва та персоналу до етичних цінностей організації;

відсутність чіткої, документально завіреної відповідальності, підзвітності кожного працівника й її усвідомлення;

неможливість/небажання публічного покарання (наприклад, відкриття кримінальної справи) виявлених корпоративних шахраїв.

Зовнішні загрози:

залякування працівника ззовні (шантаж, тиск, погрози) з метою отримання інформації;

отримання пропозиції співробітником щодо продажу важливої інформації організації;

несанкціоноване передання стороннім особам (продаж) конфіденційної або іншої службової інформації, яка є значущою для діяльності організації;

переманювання та вербування працівників організації конкурентами;

викрадення провідних працівників організації або їх ліквідація;

робота співробітника організації на конкурента, використання співробітника "втемну";

заподіяння організації шкоди внаслідок диверсійних актів – застосування вибухових пристроїв, виведення з ладу комп'ютерної техніки, зміна програмного забезпечення та ін.

За результатами дослідження *PWC*, найтиповіший шахрай у світі – це так званий "білий комірець". Типовий суб'єкт посадових злочинів – це чоловік старше тридцяти років з вищою освітою, стійкою психікою та стабільною родиною, який працює в організації від трьох до десяти років. Більшість посадових злочинців в Україні – представники вищої та середньої керівної ланки (по 40 %). Для порівняння, у світі 60 % внутрішніх злочинів здійснює керівництво середньої ланки та рядові співробітники. Фахівці з безпеки та боротьби з шахрайством вважають, що кожен з персоналу здатен скоїти злочин.

Сучасні дослідження причин і чинників шахрайських дій та злочинів з боку персоналу ґрунтуються переважно на роботі Е. Х.Сазерленда, який в 1939 р. ввів поняття "злочини білих комірців" – "незаконні дії корпорацій та їх вищих посадових осіб з використанням службового становища" [58].

З тих пір поняття розширилося, включаючи майже всі економічні (у тому числі й фінансові) злочини, що вчиняються на всіх рівнях. Попадаючи в корпоративну середу та просуваючись кар'єрними сходами, керівники та менеджери отримують більше пільг. Проте спостерігається, що більшою мірою вони зацікавлені у власній кар'єрі, їх власні інтереси превалюють над інтересам організації (наприклад, швидкі гроші, привласнення акцій компанії, можливість перейти до іншої компанії). Таким чином, вони приймають рішення, керуючись позицією "що мені за це буде".

Коли співробітник не отримує заслуженого збільшення винагороди або підвищення (на думку самого працівника) або отримує звістку про скорочення або звільнення, то відчуває початковий шок. Після цього шоку, може виникнути бажання "поквитатися" та "взяти те, що належить мені", "покарати винного". Подібні явища, які призводять до вчинення злочинів, часто відбуваються в сучасних суспільствах: на рівні можновладців і урядовців, у корпораціях, соціальних угрупуваннях або з боку дітей та підлітків,

які демонструють неповагу до батьків або офіційних органів і структур. У подальшому діти переносять таку модель поведінки на доросле оточення, керуючись таким же ставленням до влади або суспільних правил, закону, оскільки в компаніях і на підприємствах професіонал з безпеки та персонал уособлюють для них одну із форм влади.

Дослідження Е. Х. Сазерленда продовжив Д. Р. Кресі, який займався вивченням поведінки розтратників. У 1953 р. він висунув гіпотезу, згодом названу "трикутником шахрайства" (рис. 5.2). Науковець стверджує, що "довірені особи стають злочинцями на довірі в тому випадку, якщо починають відчувати фінансові труднощі, про які не можуть говорити публічно, можливим виходом вважаючи вчинення таємних фінансових махінацій. Вони здатні застосовувати до своєї поведінки в даній ситуації пояснення, що дозволяють узгодити уявлення про себе як про наділених довірою осіб і як про користувачів ввірених коштів або майна" [58].

Мотивація, тиск – це обставини, що змушують людину зчинити шахрайську дію. Ці обставини можуть бути як особистого плану (несподівано знадобилася велика сума грошей для лікування близької людини), так і корпоративного (вкрай необхідно показати виконання плану). Проте якщо людина не мотивована до скоєння порушення правил, положення або закону відносно до корпоративної власності, вона не заподіє правозлочину, навіть якщо є можливість і розуміння, як його скоїти.

Рис. 5.2. **"Трикутник шахрайства" за Д. Р. Кресі** [58]

Найбільш поширені види тиску, здатні змусити людину піти на вчинення злочину – це:

фінансовий тиск (нестача коштів, інфляція, особистий борговий тягар з причини зниження особистих фінансових доходів, екстравагантний спосіб життя, витрати на охорону здоров'я, потреби сім'ї або соціальний тиск);

непереборне прагнення до особистої вигоди;

тиск вад і згубних пристрастей (азартні ігри, алкоголь, наркотики);

тиск, пов'язаний з роботою (наприклад, щоб помститися комусь);

тісний зв'язок з клієнтами;

тиск з боку керівництва;

думка, що зарплата є непорівнянною з обов'язками;

бажання суспільного визнання;

почуття виклику з бажанням зруйнувати систему;

тиск з боку сім'ї або однолітків.

Можливість вчинити шахрайство, приховати його й уникнути покарання – другий елемент трикутника шахрайства, який поділяють на чинники, пов'язані та не пов'язані з контролем. Якщо немає можливості, навіть вмотивована людина, яка знає, як здійснити крадіжку цінностей організації, не зможе успішно вчинити злочин.

До головних чинників, пов'язаних з контролем, відносять:

відсутність або недостатність заходів з контролю, що дозволяють попередити/виявити шахрайство;

неможливість або нездатність оцінити якість виконаної роботи;

відсутність виробничої дисципліни;

надання спотвореної або недостатньої інформації;

байдужість до подій з боку начальства і/або колег;

відсутність ревізій, попередження, розслідувань і доведення злочину.

Чинники, не пов'язані з контролем, включають:

неможливість або нездатність оцінити якість роботи;

порушення принципу невідворотності покарання;

відсутність доступу до необхідної інформації;

некомпетентність, байдужість або особлива вразливість;

відсутність ревізій та попередження порушень.

Якщо є тільки мотив (бути звільненим) і можливість (комп'ютер або ноутбук просто лежав і не було поруч нікого), цього замало для скоєння протиправної дії. Знання способів і засобів здійснення злочину перетворюють мотиви та наміри на здійснення вчинку. Майже кожен випадок шахрайства містить елемент *самовиправдання, доведення раціональності дій*.

Фактори третьої вершини "Трикутника шахрайства" важко піддаються типізації, оскільки цілковито та повністю залежать від внутрішнього психологічного ставлення суб'єкта шахрайства до вчинюваного злочину. На самовиправдання часто висловлюються такі причини:

"я лише беру в борг у компанії та все поверну";

"я не краду у компанії, а забираю тільки те, що мені недодають";

"якщо всі крадуть, то чому мені не можна";

"ніхто не постраждає";

"це заради благих цілей" та ін.

Трикутник шахрайства є ефективною концептуальною моделлю, яка допомагає в питаннях кадрової безпеки: боротьбі з шахрайством з боку посадових осіб, розумінні передумов шахрайства, організації системи контролю та попередження:

мотивація стосується до потреби, яка веде до шахрайства;

можливість – до ситуації, яка сприяє виникненню шахрайства;

раціональність пояснює причини скоєння нечесного вчинку.

За загальними оцінками професіоналів служб безпеки, сімдесят сім відсотків усіх шахрайств відбуваються в одному з таких відділів: бухгалтерського обліку, операцій, продажу, топ-менеджмент/вищий менеджмент, обслуговування клієнтів, закупівель і фінансів. Банківські та фінансові послуги, уряд і державна адміністрація, обробна промисловість – зазвичай це ті галузі, які потерпають від самого високого ризику випадків шахрайства.

5.2. Система мотивації та культура безпеки організації

Як стверджують іноземні фахівці [56, с. 145], типовий шахрай – це представник "білих комірців", зазвичай особа, яка вчинила злочин вперше, середнього віку, добре освічена та розумна, в основному довірений співробітник, який займає відповідальну посаду та вважається хорошим громадянином, добропорядним сім'янином, має добру репутацію за весь час роботи. Згідно з "трикутником шахрайства" для такого злочинця основним мотивом буде тиск фінансової проблеми. І за умови, якщо можливість скоєння злочину та раціональність співпадають, ця людина з високою ймовірністю здійснить акт шахрайства. Таку людину розглядають як "випадкового шахрая".

Такий тип шахрая буде мати внутрішній етичний конфлікт, але це буде тимчасова дилема. Психологія злочинця буде такою, що навіть розуміючи, що після вчинення діяння (і особливо якщо це відбувається протягом тривалого періоду часу) його можуть звільнити, він все одно йде на злочин. Злочинців, які після вдалого першого шахрайського акту мають наміри його повторити та здійснюють їх, називають "хижаками".

Ключовим у цьому ланцюжку є мотив, оскільки саме він спонукає людину діяти або є приводом до якої-небудь дії. Це пов'язано із самою природою економічних злочинів: усі злочини та шахрайства здійснюються людьми та пояснюються їхніми цінностями, інтересами та мотивами. Автори книги з корпоративної безпеки [40] зазначають, що, будучи не мотивованою до вчинення порушення правил або закону щодо корпоративних активів, людина не зробить цього, навіть якщо будуть всі можливості й умови.

Мотиви злочинів або обставини, що спонукають людей до протиправних дій, постійно знаходяться в центрі досліджень психіатрів, кримінологів, соціологів і психологів. Вчені пояснюють "людські слабкості", керуючись різними чинниками (раса, вік, стать, навколишнє середовище тощо) та розробляють теорії. Для повного уявлення розкриття проблеми слід зупинитися на їх розгляді.

1. *Теорія аномії*, яку пов'язують з ім'ям Е. Дюркгейма (1893 р.). Згідно з його концепцією, аномія як протилежність стабільного соціального порядку виникає тоді, коли держава та суспільство послаблюють свій контроль за велінням індивідів. Це відбувається в епохи промислових, економічних і соціально-політичних криз. Зайнята собою та власними проблемами, державна машина на деякий час самоусувається від вирішення нагальних соціокультурних, духовно-моральних завдань. У результаті в індивідів зникає почуття спільності, а з ним – і дух солідарності. В умовах аномії відбувається руйнування норм, які регулюють поведінку індивідів, істотно розширюються можливості для вільних волевиявлень, у тому числі для тих з них, що виходять за межі цивілізованої норми. Поширюються егоїстичні настрої, зникає належна повага до моральних і правових норм, погіршується стан моралі, зростає кількість самогубств і злочинів.

2. *Теорія диференційної асоціації* базується на положенні про те, що девіація – не що інше, як продукт особливих девіантних норм і цінностей. Цю теорію у 1937 р. висунув Е. Х. Сазерленд – один з видатних кримінологів XX ст. Він вважав, що девіантна (злочинна) поведінка – це результат

соціалізації особистості. Теорія диференційної асоціації акцентує увагу на тому, які індивіди можуть бути соціалізовані групою людей, які застосовують девіантну поведінку, та визначаючи її як абсолютно адекватну та нормальну. Назва теорії відображає ідею про те, що люди ведуть себе певним чином під впливом свого оточення. Цей аргумент продовжує народну приказку про те, що "з ким поведешся – від того й наберешся". Згідно з теорією диференційної асоціації люди, які мають інтенсивні емоційні відносини в ранньому віці з особами, які є прихильниками порушення закону, швидше за все самі порушуватимуть закон.

3. *Теорія маркування*, яка набула поширення у 1960 – 1970-х рр., указує на "здатність деяких груп нав'язувати марку "девіант" на деяких членів суспільства" (наприклад, група "борців за свободу" або "терористи" – в іншому випадку). Ця теорія фокусується на так званих лейблах меншин та інших верств суспільства, заснованих на їх відхиленні від передбачуваних суспільних норм.

Професіонал з ФЕБ має розуміти безліч теорій щодо злочинної поведінки. Це допоможе йому накопичувати інформацію та використовувати її для розроблення корпоративної програми безпеки. Знання мотивації агентів загроз є не менш важливим, ніж розуміння того, кого слід захищати та чиї інтереси.

Таким чином, система мотивації організації має бути в центрі уваги та сфери впливу професіоналів з ФЕБ. Автори роботи [7] зазначають ряд заходів, які має проводити служба безпеки для зменшення ймовірності появи мотивів щодо отримання неправомірної особистої вигоди за рахунок організації. Тому прийнята в організації система мотивації повинна :

ефективно налаштовувати співробітників на сумлінну роботу;

бути стійкою до небажаних змін у фінансово-господарській діяльності. Вона має бути такою, щоб працівники отримували додаткову вигоду. Наприклад, відділ збуту за можливості визначення відпускних цін отримує премію як відсоток від обсягу продажів. Можна бути впевненим, що з високою часткою ймовірності рентабельність продажів впаде до мінімуму, а обсяг їх зросте та буде визначатися можливостями суб'єкта господарювання та ринком. У випадку, якщо співробітники мотивовані залежно від маржинального прибутку, ймовірність такого явища знижується;

чітко визначатися і не дозволяти окремим співробітникам вирішувати свої проблеми та задовольняти потреби за рахунок організації. Наприклад, надмірно строгий начальник підрозділу шляхом введення зайвого

контролю та покарань ускладнює трудову діяльність підлеглих, задовольняючи тим самим свої власні потреби. Також сюди можна віднести кар'єрні прагнення та владні амбіції керівників підрозділів, які вирішуються постійним і посиленим проштовхуванням непотрібних і шкідливих для організації структурних перетворень, рішень, імітацією бурхливої діяльності. Таким же чином найменш корисні співробітники зазвичай намагаються підвищити свою роль і значущість в організації;

зводити до мінімуму бажання працівників поліпшити своє становище за рахунок організації незаконним шляхом.

Система мотивації тісно пов'язана із культурою безпеки в організації. *Культура безпеки* спрямована на підвищення мотиваційної надійності персоналу, створення та розвиток базових для персоналу цілей і цінностей щодо безпеки організації [26, с. 101]. Культура безпеки є складовою частиною загальної корпоративної культури. Вона поєднує діяльність адміністрації та поведінку персоналу, спрямовані на забезпечення сталої та конструктивної взаємодії людей щодо захищеності їх від неприйнятних ризиків, загроз і викликів. Культура безпеки також неоднорідна та містить такі елементи, як: культура фінансово-економічної безпеки, культура взаємодії з клієнтами, культура безпеки на виробництві й інші елементи, перелік яких може бути довгим. Організації мають проводити політику, яка показує, що забезпечення безпеки є вищим пріоритетом у всіх видах їх діяльності.

Культура безпеки має ґрунтуватися на принципах:

усвідомлення важливості та значення забезпечення безпеки кожним працівником;

відповідальність кожного працівника, яка реалізується через розуміння та неухильне виконання посадових інструкцій;

високий рівень знань і компетентності керівників, які забезпечують підготовку персоналу та реалізацію заходів щодо забезпечення безпеки;

регулярне здійснення нагляду та контролю за станом відповідальних за безпеку організації систем і за підготовкою персоналу.

5.3. Профілактичні методи кадрової безпеки в системі фінансово-економічної безпеки

Для того щоб запобігти протиправним діянням і злочинам з боку персоналу організації, має бути створена система попередження та контролю,

яка ґрунтується на узгодженій роботі підрозділів безпеки, внутрішнього аудиту, управління персоналом, комплаєнсу. Будь-які кошти, витрачені на профілактику й попередження ризиків злочину будуть виправданими й економічно доцільними порівняно зі шкодою, яку може понести організація внаслідок дій шахраїв.

За умови розуміння чинників шахрайства, виявлення агентів загроз і керуючись "трикутником шахрайства" як інструментом кадрової безпеки, кожен з трьох кутів може бути контрольований і покладений в основу внутрішніх заходів управління, спрямованих на мінімізацію ризиків шахрайства.

Підрозділ з безпеки визначає напрями своєї роботи з урахуванням організаційної структури організації, територіального розташування її підрозділів і особливостей їх роботи. Співробітники з безпеки приділяють особливу увагу персоналу тих підрозділів, де зосереджені або знаходяться на зберіганні матеріальні цінності, а також документи, що містять конфіденційні відомості, з метою запобігання розкрадань і витоку інформації, складової комерційної таємниці. Крім того, співробітники ФЕБ відповідальні за роботу з тими категоріями працівників, які можуть вчинити неправомірні дії, нанести збиток фінансово-економічній безпеці організації. Насамперед мова йде про: співробітників, які працюють з договорами; персонал бухгалтерії; осіб, які мають право розпоряджатися печатками та бланками; співробітників інформаційно-технічних відділів; персонал, який має доступ до комерційної таємниці.

Співробітники з безпеки у своїй роботі з персоналом використовують різні методи профілактичного характеру – такі, як: перевірка, оцінювання, навчання, інструктажі, санкції. Підрозділ з безпеки тісно співпрацює зі службою управління персоналом (відділом кадрів) і керівниками структурних підрозділів. Функції управління персоналом і корпоративної безпеки тісно перетинаються, але завдання у них різні. У табл. 5.1 наведений перелік основних функцій цих підрозділів.

Таблиця 5.1

Функції, виконувані спільно підрозділами ФЕБ та управління персоналом

Функції відділу управління персоналом	Функції підрозділу ФЕБ
1	2
Підбір персоналу	Перевірка кандидатів під час наймання на роботу

Закінчення табл. 5.1

1	2
Оформлення на роботу	Забезпечення рівня допуску працівників до інформації
Адаптація працівників	Інструктаж з правил безпеки та внутрішнього розпорядку
Соціальна підтримка працівників	Консультативна допомога працівникам
Управління трудовою дисципліною	Пропускний та внутрішньооб'єктовий режим
Управління конфліктами	Розслідування конфліктів

Взаємодія зі структурними підрозділами регламентується у відповідному розділі Положення про підрозділ з безпеки, де визначаються функції, зони відповідальності та права підрозділу з безпеки. Але, як видно з табл. 5.1, між функціями відділів управління персоналом та корпоративної безпеки є розбіжності.

Робота з персоналом проводиться за такими напрямами:

перевірка кандидатів у ході приймання на роботу, виявлення можливих ризиків і загроз для організації;

забезпечення безпеки в процесі виконання персоналом службових обов'язків;

запобігання нанесенню економічного збитку та витоку інформації, складової комерційної таємниці у випадку звільнення співробітника.

Підбір кандидатів на роботу здійснюється згідно з вимогами, що пред'являються до фахівця на даному робочому місці з урахуванням його професійних умінь, навичок і особистісних якостей. У відборі кандидатів на вакантні посади необхідно керуватися тим, що потенційний працівник повинен:

мати належну кваліфікацію або можливість швидко її придбати;

бути лояльним до організації;

володіти високими моральними якостями.

Підрозділ з безпеки підключається до роботи з кадрами вже на етапі підготовки оголошень про вакантні робочі місця. Під час підбору кандидатів використовуються різні способи пошуку потенційних співробітників:

вивчаються пропозиції служби зайнятості, рекрутингових агентств;

розміщуються оголошення про вакансії в періодичних виданнях, на спеціалізованих інформаційних порталах з пошуку роботи;

розглядаються рекомендації лояльних співробітників, які вже працюють в організації;

проглядаються бази анкет і резюме, зібрані раніше тощо.

Іноді на початковому етапі пошуку кандидатів пропозицій виявляється занадто багато, що вимагає додаткової роботи відділу кадрів і підрозділу з безпеки. Кількість кандидатів можна скоротити, якщо грамотно скласти оголошення про найм, указавши в ньому обмежувальні вимоги: рівень освіти та професіоналізму, вікові рамки, необхідність проходження медичного обстеження, рівень передбачуваної оплати праці, графік роботи, за необхідності – обов'язкове проходження військової служби, знання іноземних мов, наявність водійських прав та ін.

Сьогодні у процесі підбору фахівців стає нормою звернення в спеціалізовані організації на ринку праці (служби зайнятості, рекрутингові агентства). Під час реструктуризації, ліквідації або скорочення робочих місць в організаціях інформація про співробітників передається в службу зайнятості. Але саме серед цих працівників можуть виявитися саме ті висококваліфіковані фахівці, які потрібні організації. Інформація, що знаходиться в розпорядженні організацій, що займаються підбором персоналу й працевлаштуванням, може бути дуже корисна на етапі попереднього вивчення кандидатів. Практика показує, що встановлення довірчих відносин з працівниками служби зайнятості й агентств дозволяє полегшити первинний пошук і вивчення даних про кандидатів на вакансію.

Підрозділ з безпеки бере участь у підготовці психологічних тестів, а також у підготовці професійних питань (разом з фахівцями тих підрозділів, де відкриті вакансії). Зміст усіх наданих кандидатами документів аналізується спільно співробітниками відділу кадрів і підрозділу з безпеки. Ними оцінюється рівень освіти кандидата, досвід роботи, вміння грамотно оформляти документи тощо.

Мета співробітника підрозділу з безпеки – зібрати максимум додаткової інформації про кандидата. Це дуже важливо для запобігання потенційної загрози безпеки організації і в сьогоденні, і в майбутньому. Необхідно з'ясувати, чи:

не притягувався кандидат до кримінальної відповідальності за правопорушення, пов'язані з фінансовою або іншою діяльністю на попередніх місцях роботи;

не був кандидат звільнений з колишніх місць роботи з причин, пов'язаних з фінансовими й іншими порушеннями, які офіційно не отримали розголосу;

не було в числі місць попередньої роботи організацій, які практикують "тіньові" схеми бізнесу.

Перевірка кандидата на роботу за рекомендацією працівників повинна проходити за комплексною схемою та в повному обсязі. Важливо враховувати репутацію людини, яка радить запросити на роботу в організацію свого знайомого, а також мотиви запрошення та ступінь родинних зв'язків, наявність у них спільних бізнес-інтересів.

Проведення співбесіди. Під час першого особистого контакту з кандидатом необхідно оцінити його зовнішній вигляд і манеру поведінки. Необхідно зазначати негативні ознаки: розв'язність, недбалість в одязі, помітний макіяж, татуювання з кримінальною символікою та ін. Стиль поведінки й одягу людини повинен відповідати вимогам посади, на яку він претендує.

Співбесіда кандидата з співробітниками підрозділу безпеки – обов'язковий етап приймання на роботу. Співбесіда повинна бути побудована таким чином, щоб сприяти вільному спілкуванню, та з певним рівнем довіри. Мета співробітника підрозділу безпеки під час проведення співбесіди – отримати максимум відомостей біографічного характеру від самого кандидата, а також перевірити достовірність поданої в документах інформації (рівень освіти, досвід роботи тощо). Якщо на вимогу надати якісь додаткові документи кандидат відповідає відмовою, важливо проаналізувати причини такої поведінки.

Під час бесіди з кандидатом потрібно з'ясувати:

основні спонукальні мотиви працевлаштування в дану організацію;

наявність необхідного досвіду роботи;

плани кандидата в перспективі (підвищення кваліфікації, кар'єрне зростання, очікування щодо заробітної плати тощо);

причини звільнення з попереднього (попередніх) місця роботи (незадоволеність рівнем заробітної плати; конфлікти з колегами, керівництвом);

наявність корисних (або підозрілих) особистих і ділових зв'язків;

характер відносин з керівниками та співробітниками на попередньому місці роботи;

готовність кандидата (за необхідності) допомагати колегам, працювати понаднормово й у святкові та вихідні дні;

найбільш прийнятний для кандидата режим роботи (рутинний, активний, з частими відрядженнями тощо).

У ході спілкування з потенційним співробітником необхідно звертати увагу на аргументацію відповідей, інтонацію, міміку, жестикуляцію,

стилістику мови. Якщо людина не здатна послідовно та логічно розповісти про свій досвід, то варто додатково перевірити її інтелектуальний рівень за допомогою тестів.

Аналіз відповідей кандидата дозволяє виявити такі моменти, як:

відсутність системності мислення;

невміння стисло та чітко викладати свої думки, відповідати на конкретні питання;

невміння слухати співрозмовника;

надмірна конфліктність, образливість;

надмірна амбітність, упертість у відстоюванні власних поглядів і переконань.

Рекомендується в загальних рисах інформувати кандидата про основні завдання та характер діяльності організації. Проте важливо не розголошувати конфіденційну інформацію, яка може бути використана конкурентами. Під час проведення співбесіди слід звернути увагу на такі негативні моменти:

схильність кандидата до алкоголізму, наркоманії;

наявність психічних розладів;

явно виражені прояви імпульсивності, недостатнього вольового контролю та інше.

Особи з подібними відхиленнями можуть становити потенційну загрозу безпеці організації.

Бажано організувати безпосереднє спілкування кандидата з працівниками, які виконують аналогічну роботу або задіяними в тому підрозділі, в якому планується робота новачка. Їхня думка дуже важлива. Зустріч з майбутніми колегами можна провести і поза офісом, на "нейтральній" території (у ресторані, барі, на пікніку) – залежно від передбачуваної посади кандидата в організації. У неформальній обстановці людина може повідомити важливу інформацію про себе, свої плани або обставини роботи на попередньому місці. Іноді навіть сам характер запитань, які кандидат задає своїм можливим колегам про умови роботи, оплату праці, про прийняті правила взаємин і дисциплінарні порядки в компанії (як і розповідь про те, що не подобалося на попередньому місці роботи), може багато розповісти про людину. Оскільки майбутніх колег не сприймають як перевірювачів, з ними кандидат може бути більш відвертим, ніж зі співробітниками підрозділу безпеки або відділу кадрів; таку інформацію потрібно уважно аналізувати.

Окремий напрям роботи підрозділу безпеки – безпосередня *перевірка відомостей про кандидата*. Після збирання необхідної інформації та документів, проведення попередньої співбесіди всі отримані дані вивчаються й аналізуються.

На практиці для отримання додаткової інформації про нового працівника професіонали з безпеки звертаються у приватні компанії, що спеціалізуються на наданні інформаційних послуг. Ці агенції працюють з різними масивами інформації, базами даних і можуть надати необхідні відомості щодо конкретної особи чи організації.

Звертаючись в інформаційні агентства, професіонал з безпеки може з'ясувати або уточнити:

перелік компаній, в яких перевірювана особа була (або є) засновником, керівником, головним бухгалтером, а також організаційно-фінансове становище цих компаній на даний момент;

наявність у кандидата судимостей, участь у діяльності злочинних угруповань;

наявність зв'язків (у тому числі родинних) з конкуруючими компаніями.

Виявити деякі негативні особливості кандидата можна, проаналізувавши надані ним документи, зокрема, вивчаючи причини стягнень і звільнення з попередніх місць роботи. За необхідності можна під слушним приводом (профогляд) рекомендувати кандидату пройти медичне обстеження.

У результаті аналізу документів біографія кандидата повинна бути подана як логічно несуперечливий ланцюг подій. Під час перевірки даних анкети та трудової книжки необхідно звертати увагу на безперервність стажу. Якщо на питання про причини перерв у роботі людина дає непереконливу відповідь, потрібно провести додаткову перевірку, в тому числі з використанням баз даних приватних інформаційних агентств. Наприклад, можна перевірити фінансовий стан компаній, в яких кандидат раніше працював і які, за його словами, ліквідовані або не проводять діяльності. Значна перерва в трудовому стажі може свідчити про самозайнятість, роботу або навчання за кордоном та інші обставини, які можуть впливати на роботу майбутнього співробітника.

Аналіз посад, займаних людиною в різних компаніях, дає уявлення про кар'єрне зростання фахівця. Професіонал з безпеки повинен уточнити причини підвищень (знижень) на посаді кандидата на колишніх місцях роботи. Пояснення не повинні містити суперечностей.

Одна з форм перевірки – *отримання відомостей про кандидата за попереднім місцем роботи та навчання*. Слід зауважити, що опитування контактних осіб найчастіше не дає об'єктивної інформації. Більш достовірні відомості про кандидата можна отримати, розмовляючи з колишніми товаришами по службі, працівниками відділу кадрів, керівниками структурних підрозділів, а за наявності служби безпеки на попередньому місці роботи кандидата – з її співробітниками. Такі бесіди можна проводити як в телефонному режимі, так і з виїздом в організації. Проводити їх можна, відкрито промовляючи мету візиту або використовуючи заготовлену "легенду". Другий варіант кращий, якщо кандидат ще працює в організації і тому небажано розголошувати інформацію про те, що він хоче перейти на інше місце роботи. "Легенди" можуть бути різними, вони розробляються залежно від ситуації (наприклад, доцільно звернутися в компанію під приводом проведення соціологічних або маркетингових досліджень). Виконує таку роботу підготовлений професіонал з безпеки, можливо, із залученням довірених осіб із внутрішніх рекрутерів служби зайнятості, рекрутингових агентств.

В окремих випадках використовується метод збирання інформації за місцем проживання кандидата. У ході опитувань і огляду важливо звернути увагу на умови його проживання, поведінку в побуті тощо. Збирання таких даних здійснюється професіоналом з безпеки, який має відповідну підготовку.

Ретельно проаналізувавши всю отриману інформацію, професіонал з безпеки проводить підсумкову співбесіду з кандидатом (як правило, спільно з працівником управління персоналом або керівником підрозділу).

Допуск працівника до роботи. Для забезпечення безпеки компанії не рекомендується приймати на роботу кандидата, якщо в результаті проведеної перевірки про нього виявлені такі негативні факти:

приховування важливої для роботодавця інформації, під час співбесід – нещирість у відповідях на запитання;

робота в конкуруючій компанії;

наявність ділових інтересів у сфері діяльності компанії (власний бізнес, родинні чи дружні зв'язки);

наявність значних або сумнівних боргових зобов'язань (як всередині країни, так і за кордоном);

надання недостовірної інформації;

звільнення з попереднього місця роботи з причини конфлікту.

У разі прийняття на роботу кандидата з виявленими негативними моментами всупереч рекомендаціям підрозділу безпеки діяльність його повинна бути під постійним контролем підрозділу безпеки.

У більшості випадків для нового працівника передбачається певний випробувальний термін, під час якого професіонали з безпеки повинні уточнити достовірність інформації, отриманої в результаті перевірки, і завершити вивчення особистості кандидата. Але говорити про "завершення" можна лише умовно, оскільки процес ознайомлення з особистістю працівника не повинен припинятися ніколи.

З ухваленням рішення про приймання кандидата на роботу співробітник СБ проводить з ним інструктаж з такого кола питань:

запобігання нанесення економічного збитку організації;

правила роботи з комерційною інформацією організації.

Потім новий працівник підписує "Зобов'язання у зв'язку з допуском до конфіденційної інформації, яка підлягає захисту", де вказані вимоги до виконання зобов'язань і відповідальність за їх порушення.

Створивши належні умови праці для найманих працівників, необхідно визначити основні принципи кадрової політики в організації, адже ризик прийняття на роботу працівника, потенційно здатного внаслідок дій або бездіяльності керівництва заподіяти шкоду, досить значний.

5.4. Техніки агентурної роботи професіоналів з фінансово-економічної безпеки

Робота професіоналів з ФЕБ у значній мірі пов'язана із пошуком та отриманням інформації, проведенням комунікацій зі співробітниками, розбудовою агентської мережі. Тому значну увагу в роботі професіонал з безпеки приділяє **виявленню перспективних для вербування осіб**.

Керівники організацій помиляються, вважаючи, що співробітнику, який працює на ключовий в інформаційному плані посаді, достатньо високої зарплати, щоб виключити небезпеку його переходу в конкуруючу організацію. Ще однією помилкою керівників є те, що вони поділяють людей на "своїх" і "чужих", тобто на тих, хто здатен, і тих, хто не здатний зрадити компанію. Насправді в певних умовах може зрадити будь-хто, а ціна зради може бути дуже високою. Тому необхідно своєчасно звертати увагу керівників і засновників на такі негативні фактори:

відсутність дієвої системи матеріальних стимулів, включаючи неучасть у розподілі прибутку;

відсутність гарантій довгострокової зайнятості;

відсутність можливостей перспективного кар'єрного зростання;

розстановка співробітників без урахування їх здібностей і бажань;

ставлення до співробітників як до простих виконавців волі керівництва;

відсутність перспективи бути почутим (а не просто вислуханим) керівником – як безпосереднім, так і вищої ланки управління;

психотравматична ситуація звільнень.

У роботі з кожним працівником організації необхідно враховувати поєднання трьох основних параметрів: ступеня обізнаності, особистісних особливостей, соціально-психологічного чинника.

Залежно від ступеня володіння конфіденційною інформацією всіх співробітників можна розподілити на *три основні групи*: слабо обізнані, досить добре обізнані, дуже добре обізнані.

Найбільше значення в методиці оцінювання мають такі *індивідуально-особистісні особливості співробітників*, як нещирість, а часом і брехливість, емоційна нестійкість, ступінь навіюваності та самоконтролю, душевна черствість, відсутність внутрішніх моральних норм. Вважається, що особи, у яких такі якості переважають, вразливі під час застосування до них вербувальних підходів.

Існує багато спеціальних тестів, за допомогою яких можна перевірити кожного члена колективу та попередньо оцінити його (наприклад, тест Кеттела). Вони досить ефективні, але перевагу слід віддавати індивідуально-психологічній роботі. Тому фахівці з безпеки рекомендують включати в трудовий контракт пункт про згоду працівника на проведення психологічного тестування.

Окрім індивідуальних особливостей співробітників, слід враховувати *соціально-психологічний клімат у колективі*: чи вільно та комфортно відчуває себе співробітник на роботі, чи задоволений він взаєминами з колегами. Потрібно звертати увагу на психологічну стабільність у сімейних відносинах співробітників.

У контррозвідувальній роботі професіонала з безпеки необхідно використовувати різні *джерела збирання інформації про кожного працівника*:

дані, отримані на етапі попереднього відбору персоналу (тестування, співбесіди та психодіагностика);

інформація з попередніх місць роботи;

дані, отримані зі звітів (довідок) безпосередніх керівників про роботу відділів (підрозділів) організації в цілому та кожного співробітника окремо. Ця інформація може бути отримана у вигляді карт атестації персоналу;

особиста думка кожного співробітника про своїх колег і відділ у цілому, отримана в неформальних бесідах;

інформація про життя, побут співробітника поза роботою, коло спілкування, зв'язки, способи проведення дозвілля, додаткові прибутки.

Інформація про кожного співробітника збирається в окремому досьє, яке постійно поповнюється, фіксуючи будь-які зміни, й аналізується. На основі результатів аналізу розробляються рекомендації, які коректують діяльність організації в цілому та його структурних підрозділів.

В основі інформаційно-аналітичної роботи підрозділу безпеки є **співпраця з агентурою**. Від того, наскільки якісно контррозвідка організує цю роботу, залежить швидкість та ефективність реагування керівників організації та підрозділу ФЕБ на будь-які зміни в загальному стані справ, твердість і впевненість в управлінні процесами, що відбуваються. Підрозділ з безпеки має тісно співпрацювати з керівництвом (правлінням), коригуючи ситуацію в інтересах організації.

Співробітників, які поставляють інформацію, умовно можна розподілити на три категорії:

прямі агенти, тобто джерела інформації, постійно надають пряме сприяння контррозвідці організації;

довірені особи, тобто джерела інформації, з якими контррозвідка підтримує систематичні відносини, гласні за формою, але суто конспіративні за змістом. Такі контакти вимагають підготовки легенди;

співробітники, які працюють "втемну" та не відчувають, що є джерелами інформації, не підозрюють про ступінь своєї участі в контррозвідувальних заходах.

У процесі підбору джерел інформації слід чітко визначити:

ступінь володіння інформацією;

готовність до прямої співпраці зі службою безпеки;

сприйнятливість до конспіративних контактів.

Помилка в оцінюванні кандидата може негативно позначитися на роботі корпоративної безпеки в цілому.

Вербувальний контакт здійснюється або на добровільній основі, або з примусу. Спонукальними мотивами до вербування на добровільній основі частіше всього бувають ідейні чи ідеологічні мотиви, особистісні відносини, схильності характеру (авантюризм, любов до інтриг і доносів; марнославство, що виражається в можливості надавати прихований вплив на події; прагнення отримати додаткові доходи та ін.).

Спонукальними мотивами до вербування з примусу найчастіше є матеріальна залежність або боязнь розголошення компрометуючої інформації. Для здійснення вербувальних підходів у цьому випадку часто використовують помилки та прорахунки співробітника, наприклад: порушення режимів конфіденційності, порушення (не дуже грубе, яке не призвело до серйозних наслідків) фінансової дисципліни, інші проступки, які можуть стати причиною звільнення, але які – на певних умовах – співробітник служби безпеки готовий "прикрити", перебравши відповідальність на себе.

Для будь-якого агента оператор, (співробітник служби безпеки, який розробляє агента) стає близьким, довіреною особою. Саме цю особливість відносин оператор враховує та використовує. Правило: "агента потрібно берегти" має стати не тільки формальним, але й особистісним способом його роботи з агентом.

В агентурній роботі обов'язковий принцип систематичних перевірок як інформації, що надходить, так і самих агентів. Способи перевірки можуть бути різними, наприклад:

дублювання, тобто зіставлення інформації, що надійшла від різних джерел;

"просвічування", тобто періодичне збирання інформації про агента з використанням його оточення. Для "просвічування" особливо важливих агентів часто використовують когось із дуже близьких людей, наприклад дружину або дітей;

провокація, тобто створення для агента умов, які змушують його проявити себе в тій або іншій якості (з його реакції судять про чесність, можливості подвійної гри тощо).

У процесі контррозвідувальної роботи іноді виникає необхідність оперативного проникнення – огляду робочого місця, транспортних засобів, а іноді й житла співробітника. Огляд службових приміщень проводять лише за згодою керівника організації, а житла – за сприяння кого-небудь з членів сім'ї.

У ході **аналітичної роботи** з персоналом можна виділити кілька основних помилок аналітиків ФЕБ:

невміння виявити розвідувальну чи диверсійну діяльність агента загроз;

помилка у визначенні осіб, причетних до роботи проти організації;

неправильно зроблені висновки.

У роботі з персоналом необхідно вести не тільки оперативну, контррозвідувальну роботу, але і профілактичну. Необхідно навчити співробітників

основам безпеки, а потім установити жорсткий контроль за виконанням усіх вимог, спрямованих на забезпечення корпоративної безпеки.

Застосування методів і технік роботи з персоналом – це превентивні заходи, спрямовані на мінімізацію можливостей для шахрайства.

5.5. Управління персоналом та етична відповідальність підрозділу фінансово-економічної безпеки

1. Наймання фахівців з безпеки. Перш ніж наймати професіоналів і фахівців з безпеки, необхідно: розробити й окреслити їх обов'язки та відповідальність; чітко визначити роботу, яку вони повинні виконувати, та необхідні навички, професійну підготовку й рівень освіти, якими кандидат повинен володіти. Довідковою літературою та рекомендаціями для підбору та формування штату підрозділу безпеки є Довідник кваліфікаційних характеристик професій працівників "Безпека господарської діяльності підприємства, установи, організації" [44]. Забезпечення професійності підрозділу безпеки – це в тому числі впевненість у тому, що існує взаємозв'язок між обов'язками за посадою та навичками, освітою та кваліфікацією кандидата, якому віддається перевага. Керівникові підрозділу безпеки потрібно оцінювати досвід, навички, розсудливість, надійність, сильні та слабкі сторони, лідерський потенціал кандидата. Освіта та досвід, дані, які надає кандидат, повинні перевірюватись незалежними засобами, для того щоб не допустити викривлення інформації та помилкових рішень щодо наймання персоналу.

2. Досвід і навички. Найпростішою та найбільш важливою характеристикою перспективних співробітників є рівень кваліфікації, компетентності та досвіду. Оцінювання кваліфікації, компетентності та досвіду найчастіше здійснюється під час співбесіди й інтерв'ю кандидата, або за допомогою рекомендацій.

Для того щоб бути готовим до проведення інтерв'ю із кандидатом, фахівець відділу безпеки має володіти рівнем необхідних знань. Формулювати та задавати кандидату конкретні запитання може бути відносно простим завданням, але за умови заздалегідь проведеної підготовки. Усі запитання завжди мають бути ретельно розроблені. Це дозволить сконцентрувати увагу та слухати відповіді, а не думати про наступні запитання. За рекомендаціями фахівців, щоб провести інтерв'ю з користю, оцінити

навички та досвід кандидата, зосередитися на наступних запитаннях, необхідно дотримуватись таких правил:

використовувати запитання, що вимагають від кандидатів підкреслити ті вміння, які відповідають кваліфікаційним вимогам на вакантну посаду;

давати можливість кандидату навести приклади ситуацій, в яких він успішно застосовував свої ключові навички у вирішенні актуальних для посади проблем;

дозволити кандидатам розповісти про їх сильні та слабкі сторони;

запитувати у кандидатів, як вони будуть реагувати в певних ситуаціях;

задавати кандидатам запитання, які потребують деталізованих відповідей, а не просто "так" або "ні".

Підтримку в проведенні співбесіди фахівцеві з безпеки має запропонувати відділ управління персоналом або кадрів – залежно від структури організації. Перевірка формальної освіти та професійної підготовки, а також фактичного досвіду роботи досить проста. Це може бути досягнуто за допомогою будь-якого стандартного процесу розслідування до початку роботи. Великі компанії регулярно здійснюють перевірку потенційних співробітників за допомогою підрозділів людських ресурсів або служб безпеки. Інші звертаються за цією послугою до компаній, які спеціалізуються на таких розслідуваннях.

3. Розсудливість і благонадійність. Благонадійність персоналу й її оцінювання посідають важливе місце у підборі персоналу для підрозділу безпеки. Це стосується перш за все етичної відповідальності, яку бере на себе компанія за наймання співробітника. В основу цих дефініцій закладене поняття надійності: наскільки та чи інша людина надійна та лояльна до організації. Так, більшість людей у звичайних, не екстремальний ситуаціях – хороші та порядні особи. Але коли зовнішнє оточення або внутрішній стан компанії змінюється певним чином, то люди здатні так чи інакше зрадити інтереси компанії. Немає жорсткої закономірності між змінами внутрішнього та зовнішнього світу та непорядними вчинками. Але існують певні тенденції. Якщо керівник організації або начальник підрозділу безпеки здатний визначати такі фактори, то, цілком можливо, він захистить компанію від фінансових і матеріальних втрат, а когось із працівників – і від кримінальної відповідальності.

Для оцінювання пошукувача мають бути задіяні складні характеристики, тому може знадобитися допомога професійних рекрутерів і кадрових організацій. Обрати кандидата, який найкращим чином впишеться

в штат організації, може бути складно, оскільки важко визначити, хто буде кращим працівником. Яким чином оцінити такі характеристики, як особистість, думки та розсудливість, амбіції та благонадійність?

Такі питання стосуються корпоративної етики, тому важливо знайти кандидата, який буде вписуватися в організацію з точки зору особистісних якостей, амбіцій, розсудливості та надійності. Для оцінювання розсудливості та надійності рекомендують враховувати такі настанови:

поставити потенційним кандидатам запитання щодо етичних ситуацій (наприклад: що вони будуть робити, якщо їх бос попросить сфальсифікувати звіт?);

задати кандидатам запитання щодо того, за якими критеріями, на їх думку, клієнти будуть оцінювати результати їх діяльності;

обговорити із кандидатом його слабкі сторони та що він вважає за потрібне зробити, щоб поліпшити їх.

Відповіді на запитання такого характеру повинні забезпечити розуміння того, як кандидат думає та реагує в різних ситуаціях. Це допоможе фахівцеві підрозділу безпеки більш об'єктивно оцінити потенційного кандидата.

Для повноти оцінювання кандидата важлива така характеристика, як лідерський потенціал. Керівники всіх ланок мають опікуватись пошуком і підготовкою потенційних наступників. Проте не кожен з управлінців переймається цією проблемою – з різних причин. Дехто не бажає допомагати корпорації після залишення посади через байдужість. Хтось не хоче плекати свого "могильника", який може зіштовхнути з посади – підсидіти. Деякі сповнені почуття помсти, оскільки вважають, що їх внесок у процвітання компанії недооцінюють, утискаючи в заслужених благах. Отже, це дуже суперечлива проблема, яка віддзеркалюється у відносинах "керівник – підлеглий". Але більшість корпорацій вимагає, щоб такий процес вівся постійно в кожному підрозділі, оскільки для того, щоб навчити потенційного наступника діяти професійно, потрібен час.

Безперервність діяльності організації покладена на відповідальність керівництва. Проводячи підготовку наступника, менеджер збільшує ймовірність збереження стабільного рівня продуктивності у разі зміни керівництва. Є ще одна важлива причина для оцінювання лідерського потенціалу кандидатів. Фахівці з безпеки, як правило, поміщають їх у середовище, де вони повинні приймати рішення, вирішувати проблеми, впливати на інших співробітників та їх поведінку, але можуть негативно

вплинути на ефективність. Тому важливо, щоб потенційний керівник був правильно зорієнтований та усвідомлював свою роль і завдання, пов'язані з виконанням обов'язків.

4. Звільнення або припинення роботи працівника. Припинення роботи працівника з певних причин – це стрес як для працівника, так і керівника. Причиною може стати не тільки вина працівника. Це можуть бути економічний спад або зміни у діловій активності, які негативно впливають на будь-яку галузь, що може призвести до скорочення робочої сили; працівник може припинити роботу в організації з поважної причини або через неуспішність чи недостойну поведінку.

Звільнення – це непростий процес, якого керівник може не допустити й упередити. З цією метою йому необхідно виконувати певні процедури.

По-перше, слід дотримуватися описаних принципів наймання працівників. Вони допоможуть в оцінюванні кандидата, визначенні й обранні найкращого фахівця.

По-друге, після наймання працівникові пропонують випробувальний термін (шістдесяти- або дев'яностоденний). Якщо фахівець не виправдовує очікувань, керівник може провести такі дії: надання рекомендацій, наставництво, забезпечення зворотного зв'язку в виконавцем. Одним з найбільш складних аспектів управління для більшості людей є забезпечення справедливої та чесної оцінки результатів роботи. Якщо співробітник не відповідає очікуванням, його треба сповістити про це. Усі співробітники повинні чітко розуміти, що від них очікують, і якщо вони не виконують ці очікування, вони мають усвідомити свої недоліки. Це посилює розуміння працівниками своїх обов'язків і необхідності удосконалення. Крім того, взаємно узгоджений план коригувальних дій між працівником і керівником повинен бути розроблений з метою допомогти співробітникові поліпшити продуктивність праці. Документування очікувань і встановлення параметрів результатів роботи та графіків створює рамки, в яких людина може працювати, щоб поліпшити свої показники. Ефективність працівника повинна оцінюватися на регулярній основі, поки він не досягне прийнятного рівня. Після досягнення цього рівня необхідно проводити періодичні огляди.

По-третє, за такі заходи та роботу з персоналом несуть відповідальність як керівник підрозділу з безпеки, так і менеджери. Деякі менеджери на місце працівника, який не відповідає стандартам, призначають іншу людину замість того, щоб консультувати його. Це негативно впливає

на моральний стан і результати праці, сумлінні працівники будуть перевантажені, виконуючи роботу за ледачих і некомпетентних. Від такого типу управління постраждає вся організація. Керівник підрозділу безпеки має боротися за штатний розклад і бюджет, а менеджери та професіонали з безпеки повинні опікуватися виконанням установлених стандартів. Керівник підрозділу та менеджери з безпеки повинні здійснювати керівництво й управління ефективно. І прийняття складних рішень – це частини їх роботи.

І, нарешті, якщо працівник не може або не бажає поліпшити результати своєї роботи, а виховні заходи не мали впливу на нього, слід поставити питання про доцільність перебування його на посаді.. Після того як визначено, що працівник не може працювати на рівні очікувань керівництва, необхідно понизити його на посаді або звільнити. Усі дії повинні бути виконані відповідно до корпоративних принципів, законно та професійно.

Важливим навиком управління є здатність розвиватися та працювати з людьми. Підрозділ ФЕБ та інші структури корпоративної безпеки, як і будь-яка управлінська команда, залежать від своїх співробітників, які мають виконувати свої обов'язки в міру здібностей та вимог до них як до професіоналів, тим самим забезпечуючи ефективність функціонування програми безпеки. Завдання керівника підрозділу – створити відповідну атмосферу, в якій співробітники можуть працювати та бути успішними. Для цього йому необхідно демонструвати лідерські якості, планувати розвиток поведінки співробітників підрозділу безпеки.

Уміння залучати людей і спрямувати їх роботу на продуктивний результат залежить від багатьох якостей керівника, як-то: лідерських, організаційних, психологічних і комунікативних. Управління персоналом підрозділу безпеки має ґрунтуватися на таких *компонентах*, як: співпраця, тимбілдинг, комунікація, мотивація, делегування, постановка цілей, оцінювання, управління конфліктами.

1. *Співпраця*. Ефективність організації безпеки повністю залежить від продуктивності співробітників, усі працівники повинні спрямовувати зусилля на процвітання організації. Найкращі результати досягаються, коли працівники підрозділу працюють спільно в рамках невеликих груп для вирішення поставлених завдань. Усвідомлення того, що колектив є частиною процесу прийняття рішень і кожен член має право голосу в ньому, створює середовище, в якому всі зацікавлені в результаті.

2. *Тимбілдинг* означає, що підрозділ як команда працює над досягненням спільних цілей, які зрозумілі та прийняті всіма членами команди.

Команда працює для досягнення довгострокових цілей і завдань. Її члени мають відкрито та чесно взаємодіяти для досягнення спільної мети, дослуховуватися до думки інших і пропонувати власні ідеї. Працюючи з членами команди, керівник і менеджери з безпеки спочатку мають визначити мету команди й її цілі. Сама команда повинна виявляти проблеми та співпрацювати, щоб розробити та реалізувати стратегію. Ефективні команди підвищують ефективність організації.

3. *Комунікація*. Зв'язок між співробітниками може здійснюватися різними способами: листи, записки, електронна та голосова пошта, повідомлення, телефонні дзвінки, живе звернення (обличчям до обличчя). Усі методи значущі, однак живе спілкування є найбільш ефективним. Воно дозволяє говорити, слухати, спостерігати, одразу відчуваючи реакцію співрозмовника. Це міжособистісний процес. Коли люди знаходяться у відкритому спілкуванні, важко щось приховати. Спілкування обличчям до обличчя дозволяє кожній людині реагувати на інформацію, що передається в даний момент й яку обговорюють. Крім того, очне спілкування надає таку перевагу, як читання мови тіла, що може бути дуже інформативним. Регулярна комунікація з працівниками є обов'язковою. Комунікація повинна бути обопільною: від вас до них і від них до вас. Кожен співробітник відділу безпеки повинен говорити відкрито та чесно. Відверта та чесна комунікація має сприяти довірі між людьми, дозволить уникнути непорозумінь. Чесне спілкування дає людині змогу сказати: "Я не знаю, про що ви думаєте." Це означає, що ви чесні та відкриті зі своїм співрозмовником.

Більше половини спілкування в системі безпеки передбачає прослуховування. Бути ефективним слухачем дозволяє краще зрозуміти зв'язки. Уважний слухач демонструє зацікавленість у тому, про що йому розповідають, мотивуючи співбесідника до відкритості та відвертості.

4. *Мотивація*. Існує багато теорій про те, як мотивувати співробітників. Оскільки всі люди різні, важко визначити, що найбільше мотивує кожну окрему особу. Мабуть, найкраще, що може зробити керівник підрозділу безпеки, щоб зосередитися на створенні середовища, в якому люди натхненні, це мотивувати себе. Мотивація дає людям опору в організації своїх дій. Коли люди включаються в процес цілепокладання, прийняття рішень і їх здійснення, вони створюють власну мотивацію. Зробити співробітників частиною процесу, закликаючи їх до участі в діяльності, та спонукати на виконання завищених очікувань – це вимагає від

керівника енергійних дій. Залучати людей до процесу – це не тільки дати їм відчути себе частиною процесу. Отже, участь, залученість і довіра можуть бути потужними засобами для мотивування працівників.

5. *Делегування*. Акт передання відповідальності іншим працівникам може бути складним і проблематичним для керівників. Він вимагає відмови від деякого контролю та повної довіри. Для керівників, які звикли виконувати роботу самі, важко покладатися на інших. Проте, маючи багато обов'язків і велике навантаження, вони не можуть контролювати все абсолютно. Щоб бути успішним, керівник повинен ефективно делегувати роботу. З цією метою йому необхідно правильно розподілити між підлеглими значущі завдання та надати чіткі настанови щодо їх виконання та відповідальності за їх успішне завершення. Співробітники, яким делегується робота, мають усвідомлювати, що від них очікується, а керівник має сприяти їм у роботі. Вони мають бути вмотивованими, щоб добре працювати практично без нагляду. Керівнику надаються функції консалтингу та коучингу, управління та підтримки. Отже, знання про можливості співробітників і демонстрація довіри від керівника є важливими компонентами успішного делегування.

Збої в роботі підрозділу з безпеки – це завжди відповідальність його керівника. Керівник може виступати в ролі адвоката для своїх співробітників, коли вони зазнають невдачі. Однак не можна виносити такі ситуації за межі департаменту безпеки, перебирати повну відповідальність за невдачі своїх співробітників на себе та перебільшувати успіхи своїх співробітників.

6. *Постановка цілей*. Керівник з безпеки несе відповідальність за створення відділу і його цілі та зобов'язаний узгодити їх з цілями компанії. Установлення індивідуальних цілей дозволяє визначити межі очікувань щодо конкретного співробітника. Доведення сутності очікувань до кожного члена колективу також є обов'язком керівника. Цілі повинні бути чітко та стисло викладені, бути конкретними, реалістичними, вимірюваними та зрозумілими. Усі задіяні співробітники повинні погодитися із цілями та розділяти їх. Якщо очікувані результати не адекватні, потрібно прийняти коригувальні заходи або застосувати альтернативні плани, щоб мати уявлення про хід виконання роботи. Щоб мати сенс, цілі повинні бути цінними для організації безпеки та компанії у цілому.

7. *Оцінювання*. Якщо все зроблено належним чином, оцінювання результатів роботи співробітників не буде складним завданням. Надання зворотного зв'язку співробітникам необхідне для їх розвитку. Процес оцінювання результатів і продуктивності є інструментом розвитку, який слугує

засобом для сприяння відкритому та чесному обговоренню проблем між керівником і менеджерами та працівниками. Оцінювання продуктивності не може проводитись наприкінці року. Це довготривалий та неперервний процес, підтримуваний щоденно. Періодичні та своєчасні збори з метою моніторингу, формальні та неформальні зустрічі мають відбуватися протягом усього року. Доцільно проводити незаплановані зустрічі для обговорення позитивних і негативних аспектів після завершення проекту або етапу програми та заплановані сесії для конкретного обговорення проблем з продуктивністю. Більшість компаній мають стандартний процес, що вимагає щорічного оцінювання ефективності поряд з рейтинговою системою порівняння, проте цього недостатньо. Цей процес не повинен відбуватися як щорічне змагання. Документація для оцінювання не повинна виглядати як щорічний контрольний опитувальний лист. Необхідно зазначати як позитивні, так і негативні аспекти результативності роботи працівника. Це може бути темою для конкретних обговорень проблем ефективності та забезпечить процес комунікації між працівниками та менеджерами. Процес оцінювання результатів і продуктивності має бути максимально об'єктивними. Надання працівникам вимірюваних цілей допоможе в цьому.

8. *Управління конфліктами*. На практиці керівники підрозділів з безпеки стикаються з такими важливими обов'язками, які також є частиною їх роботи, як управління конфліктами та робота з "важкими" особами. Нездатність справлятися з конфліктами та складними людьми може зруйнувати організацію. Коли керівник не в змозі контролювати та протистояти конфлікту або важким людям, то їх негативні прояви тільки посилюються. Самий ефективний шлях подолання подібних проблем – упереджувати конфлікти на ранніх стадіях. Перед зустріччю з працівниками керівник має визначити причину їх неправильної поведінки. З цією метою керівник має задатися такими питаннями:

що керівник або менеджер може зробити, щоб загасити конфлікт;

про які проблеми в організації керівник повинен знати;

які особисті проблеми працівників впливають на їх роботу;

які розбіжності виникають з у працівника зі співробітниками, продовжуючи загострення ситуації.

Для розуміння та вирішення конфліктних ситуацій може знадобитися консультація з іншими фахівцями (наприклад, зі сфери людських стосунків). Керівникові потрібно також замислитися про наслідки конфлікту та засоби уникнення рецидивів.

У фахівців є спеціальні техніки роботи в конфліктних ситуаціях. Такі техніки передбачають пряме спілкування з людьми та спільні обговорення. Певні поради дозволять керівникові управляти ситуацією, а саме:

роз'ясніть співбесіднику своє бачення;

говоріть стисло та по суті;

викладайте факти та свої спостереження, але не зупиняйтеся на них;

підходьте до ситуації з позитивно, але будьте твердими;

не сперечайтеся, якщо людина сердиться;

спробуйте встановити позитивний тон;

послухайте, що він або вона хоче сказати;

поділіться вашою точкою зору та занепокоєннями, не будучи поблажливим;

ніколи не ганьбіть і не принижуйте людей, які залучені до конфлікту й є учасниками дискусії, звертайтеся до них з гідністю та повагою;

допоможіть співбесіднику висловити свої сподівання та надії.

Підготовка, наймання та робота з персоналом підрозділу ФЕБ є не менш важливим питанням для забезпечення фінансово-економічної безпеки організації, ніж методи та техніки кадрової безпеки.

Організовуючи роботу ФЕБ, його керівник протягом першого ж тижня має ознайомитися з усіма процесами суб'єкта господарювання, безпосередньо спостерігаючи за процесом від початкової стадії до завершення. Дуже важливе для керівника з ФЕБ розуміння внутрішньої роботи, вивчення всієї можливої інформації про компанію та галузь, у якій вона працює. Це, в свою чергу, є одною з основних тем співбесіди під час наймання керівника з ФЕБ на роботу.

Обравши кабінетний стиль роботи, керівник підрозділу безпеки позбавляє себе можливості спостерігати за діяльністю компанії та процеси вироблення основного продукту. Вони рідко бачать або зустрічають працівників, які повинні відігравати певну роль у захисті життєво важливих активів та інтересів компанії: фахівців, які використовують автоматизовані системи на виробництві; співробітників відділів управління персоналом, контролю якості персоналу, аудиторів; персонал відділу закупівель, служби з роботи за контрактами; субпідрядників та інших зовнішніх співробітників. Як правило, вони пояснюють це браком часу та зайнятістю. Тому перед тим як приступати до виконання обов'язків, керівники мають не тільки проходити загальний інструктаж та отримувати відповідну до їх посади інформацію. Вони обов'язково мають пройти курс тайм-менеджменту, щоб навчитися розпоряджатися своїм часом. Недостатня компетентність

такого професіонала, як керівник з ФЕБ, загрожує успішній роботі всієї компанії, оскільки він не зможе надати послугу без вивчення оточення та культури компанії та розуміння процесу виготовлення продукції.

Керівник з ФЕБ повинен знати, як здійснюється виробничий процес, як виробництво підтримується іншою компанією, як співробітники використовують активи компанії та проблеми, з якими вони стикаються в процесі своєї роботи. Без цього неможливо дізнатися, наскільки прописані та встановлені політика та процедури щодо захисту активів розділяються співробітниками та як вони виконують свої функції. Керівник з ФЕБ може з'ясувати це тільки в ході прямого спостереження та спілкуючись з працівниками всіх рівнів – від корпоративного управління до охоронників. Проте це стосується не тільки керівника, професіонали та фахівці підрозділу ФЕБ також мають регулярно проводити такі огляди та співбесіди.

Рекомендована література: [7; 27; 40; 56; 58].

Практична частина

Контрольні запитання

1. Розкрийте змістовність поняття "кадрова безпека". Які завдання підрозділу з безпеки в сприянні та забезпеченні кадрової безпеки?
2. Наведіть найбільш розповсюджені загрози організації з боку персоналу, фактори виникнення цих загроз.
3. Надайте визначення шахрайству. Наведіть приклади шахрайських дій.
4. Розгляньте та прокоментуйте основні елементи поняття "злочин" за визначенням Д. Р. Кресі.
5. Наведіть мотиви злочинів на прикладі теорій: аномії, диференційної асоціації, маркування.
6. З'ясуйте та поясніть роль професіоналів з безпеки у становленні системи мотивації організації.
7. Перелічіть та надайте пояснення методам попереджувально-профілактичного характеру в роботі професіонала з безпеки з персоналом.
8. Які етапи та види робіт здійснює професіонал з безпеки на етапі підбору кандидата на вакантну посаду? Яку мету переслідує співробітник підрозділу з безпеки?
9. Опишіть техніки, застосовувані під час співбесіди з кандидатом на вакантну посаду. До яких висновків вони приводять?

10. Яка інформація про кандидата є предметом перевірки? Які джерела отримання цієї інформації?

11. Які вимоги щодо допуску працівника до роботи висуває підрозділ з безпеки?

12. Які особливості роботи з виявлення перспективних для вербування осіб? Перелічіть джерела збирання інформації про кожного працівника.

13. Опишіть, у чому полягає агентурна робота професіонала з безпеки? Назвіть способи перевірки отриманої через агентів інформації.

14. Назвіть та охарактеризуйте основні компоненти, на яких має будуватися керівництво персоналом підрозділу з безпеки.

15. Як професіоналу з безпеки діяти в конфліктних ситуаціях? Назвіть можливі техніки роботи в конфліктних ситуаціях.

Тестові завдання

1. Що означає поняття "кадрова безпека":

а) стан господарюючого суб'єкта, що характеризується наявністю стабільного доходу й інших ресурсів, які дозволяють підтримати рівень життя на поточний момент і в досяжному майбутньому;

б) фізична безпека співробітників підприємства, особливо представників керівництва підприємства;

в) запобігання негативних впливам на економічну безпеку підприємства від ризиків і загроз, пов'язаних з персоналом, його інтелектуальним потенціалом і трудовими відносинами в цілому;

г) стан правової захищеності важливих інтересів фізичної або юридичної особи, підприємця у зв'язку з функціонуванням цих суб'єктів у сфері господарських відносин, здатність юридичними засобами протистояти зовнішнім і внутрішнім загрозам?

2. Яка з категорій є дефініцією шахрайства:

а) шкода;

б) приховування;

в) корупція;

г) обман?

3. Викресліть елемент, якого немає в "трикутнику шахрайства":

а) тиск;

б) раціональність;

в) можливість;

г) довіра.

4. Який з елементів "трикутника шахрайства" належить до ситуації, яка сприяє виникненню шахрайства:

а) мотивація,

б) можливість;

в) раціональність;

г) ризик?

5. Який з елементів "трикутника шахрайства" акцентує на потребах і чинниках тиску, які призводять до злочину:

а) мотивація,

б) можливість;

в) раціональність;

г) ризик?

6. Обставини, що змушують людину зробити шахрайську дію, – це:

а) тиск;

б) можливість;

в) раціональність;

г) правильної відповіді немає.

7. Який з елементів "трикутника шахрайства" приводить мотиви та наміри до здійснення вчинку:

а) мотивація,

б) можливість;

в) раціональність;

г) ризик?

8. Створення та розвиток базових для розуміння персоналом цілей і цінностей щодо безпеки організації – це:

а) мотивація безпеки;

б) культура безпеки;

в) система безпеки;

г) оцінювання безпеки.

9. Яка з теорій акцентує увагу на руйнуванні норм, які регулюють поведінку індивідів, та істотно розширює можливості для волевиявлень, у тому числі для тих з них, що виходять за межі цивілізованої норми:

а) аномії;

б) стратифікації;

в) диференційної асоціації;

г) маркування?

10. Яка з теорій відображає ідею про те, що люди ведуть себе певним чином під впливом свого оточення:

а) аномії;

б) стратифікації;

в) диференційної асоціації;

г) маркування?

11. Яка з теорій фокусується на так званих лейблах меншин та інших верств суспільства, заснованих на їх відхиленні від передбачуваних суспільних норм:

а) аномії;

б) стратифікації;

в) диференційної асоціації;

г) маркування?

12. Виключіть з переліку наведених функцію, яка не належить до обов'язків професіоналів з ФЕБ організації:

а) виявлення можливих загроз для ФЕБ організації на етапі перевірки кандидатів під час приймання на роботу;

б) забезпечення безпеки в процесі виконання персоналом службових обов'язків;

в) запобігання витоку комерційної інформації у випадку звільнення співробітника;

г) усі відповіді правильні.

13. Усвідомлення того, що всі співробітники є частиною процесу прийняття рішень, кожен член має право голосу в цьому процесі, створює середовище, в якому всі зацікавлені в результаті, є наслідком:

а) співпраці;

б) тимбілдингу;

в) комунікацій;

г) делегування.

14. *Листи, записки, електронна та голосова пошта, повідомлення, телефонні дзвінки, живе звернення (обличчям до обличчя) – це* інструменти:

а) співпраці;

б) тимбілдингу;

в) комунікацій;

г) делегування.

15. Акт передання відповідальності іншим співробітникам, що вимагає відмовлення від деякого контролю та демонстрації повної віри в колег – це:

а) співпраця;

б) тимбілдинг;

в) комунікація;

г) делегування.

Кращий спосіб залишатися послідовним –
це змінюватися разом з обставинами.
Уїнстон Черчілль

Розділ 6. Моніторинг і контроль у системі фінансово-економічної безпеки організації

Після вивчення матеріалів теми Ви повинні:

знати:

роль і сутність моніторингу в СФЕБ;

контрольні процедури забезпечення ФЕБ;

методи, прийоми та способи аналізу та діагностики діяльності організації;

структуру та зміст фінансової звітності й управлінської документації організації;

ознаки зловживань з боку персоналу через фінансові показники, виконання функцій та реалізацію бізнес-процесів, поведінку й організаційні відносини;

уміти:

визначати послідовність моніторингу та контролю стану ФЕБ організації;

здійснювати збирання необхідної інформації й ефективно працювати з її джерелами;

формувати аналітичний інструментарій управління ФЕБ;

здійснювати аналіз і діагностику фінансово-економічних ризиків діяльності організації;

розпізнавати майнові, комерційні, інформаційні, кадрові, організаційні, комплаєнс-ризики діяльності організації;

попереджувати спотворення інформації в фінансовій звітності організації;

розробляти рекомендації щодо попередження ризиків ФЕБ організації та проводити ефективні контрольні процедури.

План теми

6.1. Організація моніторингу фінансово-економічної безпеки організації.

6.2. Основні компоненти внутрішнього контролю організації.

6.3. Аналіз стану фінансово-економічної безпеки організації.

6.4. Витрати та джерела фінансування управління фінансово-економічною безпекою.

Ключові поняття та терміни: внутрішній контроль, моніторинг, інформація, діагностика, аналіз, ризик.

6.1. Організація моніторингу фінансово-економічної безпеки організації

Моніторинг і контроль є предметом діяльності професіоналів з ФЕБ задля своєчасного виявлення та попередження можливих загроз і ризиків діяльності організації і її розвитку. У тій чи іншій формі моніторинг і контроль завжди присутні в управління організацією. Але найчастіше реакція на термін "контроль" негативна та сприймається як обмеження можливостей, примушення або позбавлення самостійності.

Моніторинг і контроль в управлінні ФЕБ є тісно пов'язаними функціями. **Моніторинг** – це перш за все спостереження за комплексом факторів фінансово-економічної безпеки, які створюють чи потенційно можуть створювати загрозу ФЕБ організації, з метою відстеження невідповідності стану початковим припущенням або бажаному результату. Сутність моніторингу розкривається через його інформаційну, діагностичну й аналітичну ролі.

Інформаційна роль моніторингу в СФЕБ полягає в отриманні даних щодо стану ключових фінансово-економічних показників організації. Передусім це показники фінансового стану, як то: ліквідності діяльності й оборотності ресурсів організації. Для таких показників є нормативні значення або допустимі межі їх зміни. Спостереження за цими індикаторами дозволяє робити висновки щодо тенденцій зміни фінансово-економічного стану організації, виявляти передумови розвитку та прогнозувати його наслідки з метою своєчасного попередження загроз.

У ході моніторингу здійснюється отримання інформації щодо факторів, які впливають або можуть здійснювати негативний вплив на ФЕБ організації. Усі сфери діяльності організації (виробництво, маркетинг, постачання, фінансова й інвестиційна діяльність) взаємозалежні та можуть комплексно впливати на стан захищеності організації. Будь-які події, як внутрішні так і зовнішні, можуть здійснювати вплив на ефективність і сталість функціонування та розвиток організації. Важливо своєчасно розпізнавати такі загрози, оцінювати їх та наслідки їх негативного впливу.

Отримання потрібної інформації є важливим елементом у роботі професіонала з ФЕБ. Канали отримання інформації умовно розподіляють на:

1) вільні – преса, телебачення, офіційні статистичні дані, які розміщені у відкритому доступі;

2) організовані – тобто ті, які формуються й обслуговуються фахівцями СФЕБ;

3) спеціалізовані – здійснюються фахівцями підрозділу конкурентної розвідки, іноді з використанням не завжди законних методів отримання інформації.

За рівнем доступності всі джерела інформації умовно також розділяють на три групи:

1) загальнодоступна інформація, отримання якої не вимагає додаткових витрат;

2) інформація з обмеженим доступом, яка вимагає проведення додаткових аналітичних розрахунків або оплати послуг сторонніх організацій;

3) закрита інформація, отримання якої передбачає не завжди законні дії та (або) вимагає значних витрат або залучення додаткових фахівців.

За ступенем достовірності можна розподілити таким чином:

1) достовірна інформація, яка в повній мірі відображає реальний стан певного явища чи динаміку процесу;

2) частково достовірна інформація, тобто така, яка поряд з достовірною інформацією містить і помилкову, дезінформацію або зайву, що не в повній мірі стосується об'єкта дослідження;

3) недостовірна інформація, яка не відповідає реальному стану справ та є продуктом контррозвідки конкурентів або отримана з ненадійних джерел інформації і т. п.

Інформацію з урахуванням витрат на її отримання також доцільно ранжувати за групами:

1) безкоштовна інформація, яка надходить через відкриті канали (телебачення, преса, Інтернет тощо);

2) інформація, отримання якої потребує організації інформаційного каналу, залучення фахівців (агентів), розроблення певного програмного забезпечення, визначених матеріальних, фінансових і трудових витрат;

3) інформація, яка є комерційною таємницею або має стратегічне значення для розвитку ринку, окремого його сегмента або виду діяльності, отримання якої є неможливим через відкриті канали інформації та вимагає істотних фінансових витрат.

Діагностична роль моніторингу полягає у тому, щоб усунути інформаційну недостатність у питаннях безпеки діяльності. Моніторинг має не тільки фіксувати загрози, які вже проявилися, але й виявляти потенційні,

які можуть здійснитися в майбутньому. Діагностика в системі фінансово-економічної безпеки – це процес розпізнавання загрози та визначення її, оцінювання ступеня вразливості до неї організації, тобто встановлення діагнозу ненормального стану. Процедури діагностування призначені для оцінювання фінансово-економічного стану суб'єкта господарювання з метою виявлення небезпечних і кризових зон та оцінювання масштабу прояву кризи. Діагностика дозволяє виявити, де та за якими індикаторами найсильніше проявляються загрози фінансово-економічній безпеці організації, попередити можливі негативні наслідки їх впливу та здійснити оцінювання впливу факторів загроз та їх значення для фінансово-економічної безпеки організації. Діагностична роль моніторингу є самостійною, водночас доповнюючи інформаційну. Виявлена в ході діагностики інформація досліджується в перспективі.

Аналітична роль моніторингу має не менш важливе значення. У ході аналізу відстежуються кількісні й якісні зміни індикаторів стану фінансово-економічної безпеки. Аналіз здійснюється за етапами на основі аналітичної обробки інформації. Результатом аналізу є оцінка стану захищеності фінансово-економічної безпеки організації. Ці аналітичні дані є джерелом інформації для прийняття управлінських рішень у сфері забезпечення фінансово-економічної безпеки. Аналітичній обробці підлягають не тільки дані про поточний стан, але й аналіз наслідків реалізації програм із забезпечення фінансово-економічної безпеки.

Моніторинг має бути результатом взаємодії всіх зацікавлених у фінансово-економічній безпеці підрозділів організації. Під час здійснення моніторингу повинний діяти принцип безперервності спостереження за станом об'єкта моніторингу з урахуванням фактичного стану та тенденцій розвитку його потенціалу, а також загального розвитку економіки, політичної обстановки та дії інших загальносистемних факторів.

6.2. Основні компоненти внутрішнього контролю організації

Контроль є необхідною частиною управління організацією та засобом досягнення її цілей, відіграючи ключову роль у запобіганні фінансово-економічним втратам.

Термін "контроль" найчастіше тлумачиться некоректно, в тому числі й керівниками. Саме слово "контроль", як і слово "влада", породжує перш

за все негативні емоції. Для багатьох людей контроль означає обмеження, примусовість, відсутність самостійності. Як наслідок, неправильність у поданні та розумінні даного процесу породжує хибність процесу його реалізації, а отже – зниження результативності. Основними функціями контролю є:

забезпечення підпорядкування (важлива функція, але не завжди головна);

координація діяльності;

мотивація персоналу;

забезпечення гнучкості в стратегії та тактиці компанії.

Внутрішній контроль здійснюється Радою директорів, менеджментом та іншим персоналом організації, спрямований на забезпечення розумної гарантії досягнення цілей за такими категоріями:

ефективність і результативність операцій компанії;

достовірність фінансової звітності;

дотримання відповідного законодавства, підзаконних актів і регламентів.

Внутрішній контроль – це процес, безперервна та повторювана послідовність взаємопов'язаних заходів, які зачіпають різні складові організації. Ці заходи відображають методи та підходи до управління, використовувані керівництвом, і повинні спрямовуватись на досягнення поставлених цілей. Внутрішній контроль повинен бути вбудований в систему управління компанією.

Комітет спонсорських організацій (COSO – Комісія Тредвея (https://www.coso.org) – випустив такі документи, як "Інтегровані основи внутрішнього контролю", "Ілюстративні інструменти для оцінювання ефективності системи внутрішнього контролю" та "Внутрішній контроль над зовнішньою звітністю: збірник підходів з прикладами". Ці документи визначають поняття системи внутрішнього контролю та надають інструменти, які організації можуть використовувати для проведення оцінювання своїх систем внутрішнього контролю (управління фінансово-економічною безпекою, ризик-менеджмент, внутрішній аудит тощо).

Згідно з концепцією COSO процес організації внутрішнього контролю складається з п'яти компонентів, які є складовою частиною процесу управління. Основні компоненти внутрішнього контролю наведено в табл. 6.1.

Таблиця 6.1

Основні елементи системи внутрішнього контролю

Елементи	Ключові характеристики	Опис
1	2	3
Контрольне середовище	Загальна характеристика компанії, політик і процедур щодо внутрішнього контролю	Розробляється керівництвом та включає: організаційну структуру внутрішнього контролю, у тому числі розподіл повноважень і відповідальності, а також підзвітність суб'єктів внутрішнього контролю; участь ради директорів і комітету з внутрішнього аудиту, включаючи оцінювання їх знань, досвіду, ступінь незалежності від керівництва, а також залученість у процес внутрішнього контролю; філософію та стиль управління організацією; кадрову політику; чесність і етичні якості людей, які створюють і оцінюють систему внутрішнього контролю, особливо це стосується компетентності та дій вищого виконавчого керівництва компанії та Ради директорів
Процес оцінювання ризику	Ідентифікація ризиків, значущих у підготовці фінансової звітності	Для найбільш ефективного досягнення своїх цілей компанія повинна ідентифікувати й аналізувати ризики, пов'язані з її діяльністю
Засоби контролю	Політика та процедури, контрольні заходи, які сприяють пом'якшенню ризиків, пов'язаних з досягненням цілей до прийнятного рівня	Такі засоби включають: порівняння фактичних даних з бюджетами, прогнозами та попередніми періодами; періодичну інвентаризацію та порівняння фактичних активів з сумами, відображеними в бухгалтерському обліку; обробку інформації щодо певних засобів контролю для гарантії того, що операції правомірні, відповідним чином санкціоновані, повною мірою й акуратно відображені; розподіл обов'язків зі санкціонування операцій, їх обліку та підтримка збереження відповідних активів з метою зниження ризиків приховування інформації та шахрайства. Фізичні засоби контролю за збереженням активів включають: фізичний розподіл і охорону активів, засоби захисту, що пов'язані з незалежними зберігачами (банки, депозитні комірки, сейфи, незалежні склади); авторизований доступ до активів і записів (наприклад, використання електронних кодів доступу, нумерація документів, а також необхідні підписи на документах з вибуття або руху активів)

Закінчення табл. 6.1

1	2	3
Інформація та комунікації	Методи, використовувані для класифікації та відображення операцій та повідомлення співробітників про їх ролі й обов'язки	Комп'ютерні мережі забезпечують ідентифікацію, зберігання й обмін інформацією у своєчасній і відповідній формі. Інформаційна система, використовувана для підготовки фінансової звітності, складається з процедур (як автоматичні, так і ручні) та облікових записів, розроблених для створення, фіксування, обробки й обліку операцій організації, а також ведення бухгалтерського обліку зобов'язань і капіталу. Засоби комунікації можуть бути письмовими (керівництва щодо політики та процедур, керівництва за підготовку фінансової звітності та меморандуми) або усними
Моніторинг	Процедури, необхідні для оцінювання якості системи внутрішнього контролю на постійній основі	Процес оцінювання організації системи внутрішнього контролю; структура та своєчасна робота суб'єктів контролю, а також прийняття рішень щодо здійснення необхідних коригувань. Процес моніторингу може включати: засоби поточного контролю, вбудовані в нормальні повторювані операції, включаючи регулярне залучення керівництва та контролерів; роботу комітету (служби) з внутрішнього аудиту й УФЕБ

Особливе місце в концепції COSO відведене ризику. Експерти COSO зазначають, що ризик не можна розглядати в якості потенційного обмеження або виклику для реалізації стратегії організації. Навпаки, те, як організація справляється з ризиком, передбачає стратегічні можливості. Ця теза є відповіддю на поліпшені практики, культуру та можливості, інтегровані з розробленням стратегій та їх виконанням.

Концепція управління ризиками, яка є основою "Управління ризиками підприємства" й "Управління ризиками шахрайства", включає такі складові.

1. Основи управління ризиками будуть складатися з п'яти компонентів, заснованих на двадцяти трьох принципах. П'ять взаємопов'язаних компонентів – це управління та культура; ризики, стратегія та постановка цілей; ризики в процесі виконання; ризики інформації та звітності; моніторинг системи управління ризиками.

2. Запропоновано нове визначення системи управління ризиками організації як "культури, здібностей і практик, інтегрованих зі стратегією

та виконанням, на які покладаються організації в управлінні ризиками створення, збереження та реалізації вартості".

3. Збільшено акцент на взаємозв'язку між ризиками та вартістю. Запропонована нова теза – "працюйте чітко". Вартість визначається як ключовий драйвер управління ризиками організації. Усе це важливо для стратегій організації управління ризиками, забезпечуючи можливості щодо створення та збереження вартості.

4. Управління ризиками є інтегрованою частиною системи менеджменту, а не окремим напрямом діяльності.

5. Дослідження ролі культури у виробничих процесах. Саме культура охоплює етичні цінності в організації, зразкові манери поведінки та, звісно, розуміння ризику. Взаємозв'язок між культурою та бізнес-контентом визначає, як саме будуть вибиратися та виконуватися стратегії.

6. Високе значення надане обговоренню стратегій. Фокусування на трьох концепціях: ризику того, що стратегія та цілі бізнесу не будуть відповідати місії організації, баченню та цінностям; впливі обраної стратегії; на ризиках виконання стратегії.

7. Покращений взаємозв'язок між управління ризиками та результатами діяльності. Тут мова йде про роль ризиків у визначенні ділових цілей.

8. Взаємозв'язок між управлінням ризиками та прийняттям рішень. Рішення, прийняті щодо вибору стратегій, визначення цілей і цільових показників діяльності, розподілу ресурсів і так далі, – мають бути більш обґрунтованими, базуючись на якнайповнішій інформації про ступінь і тип асоційованих ризиків.

9. Визначення схильності до ризику та допустимих відхилень у діяльності. Такі "допустимі відхилення" досить часто пов'язані саме з терпимістю до ризику. Схильність до ризику – це величина ризику, яку готова взяти на себе організація заради реалізації своєї стратегії та досягнення ділових цілей. Толерантність до ризику не є детальною варіацією схильності до ризику. Терпимість до ризику обертається навколо визначення величини ризику, допустимого за заданих рівнів результативності діяльності. Таким чином, ризик і результативність не розглядаються в якості статичних і незалежних величин – навпаки, вони постійно змінюються та впливають один на одного.

Отже, контроль покликаний виявити назрілі проблеми та скоригувати діяльність організації до того, як ці проблеми переростуть у кризу. У тій чи іншій його формі контроль і моніторинг діяльності завжди присутні в будь-якій системі управління організацією.

6.3. Аналіз стану фінансово-економічної безпеки організації

Для формулювання цілей та інструментарію аналізу фінансово-економічної безпеки організації необхідно сформулювати концепцію безпеки, основні параметри безпечної роботи організації, визначити коло заходів, які забезпечують реалізацію концепції.

Критерії фінансово-економічної безпеки можуть бути конкретизовані у вигляді груп показників.

Першу групу таких показників складають ті, що характеризують результати господарської діяльності організації, її платоспроможність, фінансову стійкість, ділову активність. Як правило, для цього використовують стандартні методики, застосовувані в процесі аналізу фінансової та господарської діяльності організації, у тому числі показники оперативного обліку.

Одним з популярних підходів до оцінювання рівня фінансово-економічної безпеки організації є розрахунок оцінних коефіцієнтів фінансового стану, серед яких виокремлюють: показники платоспроможності, структури капіталу, оборотності та рентабельності.

Показники платоспроможності (ліквідності) допомагають оцінити спроможність організації своєчасно розрахуватися за своїми поточними або короткостроковими зобов'язаннями через реалізацію найліквідніших або всіх ліквідних активів.

Показники структури капіталу (фінансової стійкості) оцінюють співвідношення окремих статей його активів і пасивів, зокрема, показують рівень фінансової незалежності від зовнішніх джерел фінансування, частку власного капіталу, вкладену в оборотні кошти та ін.

Показники оборотності (ділової активності) оцінюють швидкість обігу активів організації, відображають кількість оборотів, що здійснюють ті чи інші їх види протягом його ділового циклу, а також час одного повного обороту в днях.

Показники рентабельності характеризують здатність організації генерувати певний прибуток у процесі господарської діяльності, визначають загальну ефективність використання активів і вкладеного капіталу.

Перелік основних фінансових коефіцієнтів, які використовують для оцінювання рівня фінансово-економічної безпеки суб'єкта господарювання, формули їх розрахунку за даними балансу (форма 1) і звіту про фінансові результати (форма 2), а також рекомендовані значення (динаміка) достатньо повно описані в навчальній літературі з економічного та фінансового аналізу [23; 28].

Саме дані фінансової звітності є об'єктом аналізу та розпізнавання викривлення інформації в ній та виявлення ознак шахрайства [5]. У фінансовій звітності організації розкривається найбільш повна інформація про її діяльність. Але фінансова звітність недосконала, тому надання фінансової інформації (наприклад, відмінної від прогнозів аналітиків) може обернутися зниженням капіталізації компанії. Надання інформації, більш сприятливої порівняно з прогнозами аналітиків, може привести до зростання вартості акцій, а отже, до зниження вартості залучення позикових коштів та іншим позитивним для компанії результатам. У разі, якщо поліпшення досягнуто "штучним" шляхом, то рано чи пізно факт спотворення звітних даних стане загальновідомим, і тоді компанію чекають важкі часи. Прикладів судових справ і скандалів навколо загальновідомих компаній через викривлення інформації у фінансовій звітності чимало, хоча це світові бренди, які, як здавалось би, мають бездоганну репутацію. Саме тому даним фінансової звітності потрібно приділяти ретельну увагу. І професіонал з ФЕБ має бути компетентний в цьому питанні для того, щоб не допустити можливі негативні наслідки, будь то мале підприємство чи велика компанія.

Шахрайство у фінансовій звітності має чітко виражену структуру. За обсягами махінацій управлінське шахрайство набагато перевищує неуправлінське (рис. 6.1).

Рис. 6.1. **Структура шахрайства у фінансовій звітності**

Другу групу складають показники кадрової статистики, обліку та звітності з праці та заробітної плати персоналу. Неважко уявити, наприклад, що високий рівень плинності працівників і низька заробітна плата навряд чи свідчать про фінансово-економічну стабільність організації. Так, рівень плинності перевищує 10 %, з достатнім ступенем вірогідності вказує на існування серйозних проблем, що виникли з вини менеджменту організації.

Третю групу складають соціальні показники, що характеризують рівень соціального розвитку організації, стан соціально-психологічного клімату в колективі. До них відносять демографічні показники, професійно-кваліфікаційні параметри персоналу.

Найважливіше завдання, що стоїть перед організацією та визначає рівень її фінансово-економічної безпеки, полягає у виявленні повного спектра загроз. Аналіз можливих загроз за кожним з об'єктів захисту організації на практиці починають з фіксації стану цього об'єкта, що забезпечує його нормальне функціонування. Природно, будь-яке відхилення від цього стану може розцінюватися як можлива загроза в сьогоденні або майбутньому. Наступний крок – формалізація можливих відхилень, визначених як загрози фінансово-економічній безпеці. І на завершення – класифікація основних загроз фінансово-економічної безпеки організації за напрямами.

Ризик визначається як ймовірність настання несприятливого результату (реалізації загрози). Водночас **фінансово-економічний ризик** – це ймовірність фінансових втрат для організації через усвідомлену небезпеку через дії чи бездіяльність, виражену в різних варіантах економічної поведінки. Фінансові втрати організації можуть виникати в результаті безпосередньої фінансової діяльності, управління майном, комерційної діяльності, дії чинників інформаційної та кадрової безпеки.

Для оцінювання фінансово-економічного ризику виділяють зони, за якими він розрізняється з точки зору втрат і заповнення втрат:

безризикова зона, де втрати не очікуються;

зона допустимого ризику, яка перекривається прибутком;

зона критичного ризику, що покривається заповненням витрат;

зона катастрофічного ризику, що покривається всім майном.

Показник ступеня фінансово-економічного ризику в загальному вигляді (*Кр*) може визначатися відношенням максимально можливого збитку до суми власних коштів організації. Визначають оптимальний ризик – якщо *Кр* = 0,3; ризик банкрутства – якщо *Кр* = 0,7.

Майнові ризики – це ймовірність здійснення загроз, пов'язаних з повною або частковою втратою майна організації. Показниками, що використовуються для оцінювання майнового ризику, виступають: норми природного убутку під час зберігання, норми амортизації, страхові тарифи (нетто-ставки).

Комерційні ризики включають ризики, пов'язані з реалізацією, транспортуванням, прийманням товару, неплатоспроможністю покупця, ризики, пов'язані з форс-мажорними обставинами. Оцінити рівень комерційного ризику з достатнім ступенем достовірності можна, використовуючи такі показники, як: рівень дебіторської та кредиторської заборгованості; обсяги (індекси) реалізації продукції; рівень втрат під час транспортування продукції; індекси цін на продукцію.

Інформаційні ризики – це ризики, пов'язані зі втратою, спотворенням, розкраданням інформації в процесі її отримання, обробки, зберігання, передання. Особливо слід зазначити ризики асиметричної інформації, в основу яких закладена специфіка вимог учасників ділових відносин до повноти, своєчасності та достовірності переданої інформації. Показниками, використовуваними для оцінювання інформаційних ризиків, можуть виступати: вартісне оцінювання інформації, віднесеної до комерційної таємниці; суми витрат, пов'язаних з відновленням втраченої інформації; фінансові втрати та недоотриманий прибуток у результаті прийняття рішення, заснованого на недостовірній інформації.

Кадрові ризики – це ризики, пов'язані з ймовірністю реалізації антропогенних загроз, тобто загроз, що виходять від людей. Враховуючи, що людський фактор опосередковує всі сторони економічних відносин в організації, можна визначити кадрові ризики як комплексні, найважливішими з яких є ризики втрати конфіденційної інформації, комерційні ризики. Показниками, що використовують для узагальненого оцінювання кадрових ризиків, є рівень плинності персоналу, ступінь лояльності персоналу до адміністрації організації.

Організаційні ризики пов'язані із недоліками організації системи фінансово-економічної безпеки. До них можна віднести ризики неефективної координації робіт із забезпечення фінансово-економічної безпеки, втрата контролю за рухом товарно-матеріальних цінностей, невиконання персоналом посадових обов'язків належним чином, збільшення можливостей для знищення шахрайства серед персоналу, некомпетентні функції контролюючих підрозділів.

Комплаєнс-ризики – це недоліки в системі управління ризиками шахрайства та комплаєнс, які допомагають запобігати, виявляти, розслідувати та реагувати на випадки шахрайства. Це може бути виникнення/повторення випадків шахрайства (якщо не змінити організаційну систему, кадрову складову фінансово-економічної безпеки), неефективна координація внаслідок відсутності регламентів (положень, інструкцій) щодо забезпечення кадрової та фінансово-економічної безпеки, розкриття/просочування комерційної таємниці, втрата репутації й іміджу організації.

Аналіз ризиків забезпечує їх мінімізацію та включає оцінювання впливу факторів середовища, ймовірності прояву загроз, економічного збитку від реалізації загроз. Можливий економічний збиток (величина ризику) визначається добутком збитку від реалізації конкретної загрози, включаючи упущену вигоду, і ймовірності реалізації загрози. Мета аналізу ризику реалізації загроз полягає у виборі оптимального варіанту захисту за критерієм "ефективність/вартість".

Вибір конкретного методу дослідження й аналізу стану фінансово-економічної безпеки залежить від ситуативних обставин діяльності організації, проблемних напрямів діяльності та формування фінансових ресурсів, наявності джерел інформації та визначеності стратегій та потреб аналізу фінансово-економічної безпеки.

6.4. Витрати та джерела фінансування управління фінансово-економічною безпекою

Основним джерелом коштів, що спрямовуються на утримування СФЕБ, є внутрішні ресурси організації, хоча можливе залучення коштів із зовнішніх джерел. Основними джерелами фінансування, що виділяються на безпеку, зазвичай є:

власні фінансові кошти (прибуток, амортизаційні відрахування; страхові відшкодування, які виплачуються страховими компаніями; відсотки за акціями тощо);

засоби від продажу основних фондів (нерухомість, земля, майно, транспорт тощо);

кошти, отримані від продажу акцій, благодійні й інші внески; кошти, що виділяються фінансово-промисловими групами (ФПГ) на безоплатній основі; інші внески;

асигнування з місцевого бюджету;

іноземні інвестиції, надані у формі фінансової чи іншої участі в статутному капіталі спільних підприємств, а також у формі прямих грошових вкладень міжнародних організацій і фінансових інститутів, держав, підприємств різних форм власності, приватних осіб;

різні форми позикових коштів, у тому числі кредити, надані державою на оплатній основі, кредити іноземних інвесторів, облігаційні позики, векселі, кредити банків та інших інституційних інвесторів.

Складність вирішення організаційних і економічних завдань забезпечення ФЕБ організації зумовлена його комплексним характером. З одного боку, комплексний підхід до впровадження СФЕБ підвищує стабільність функціонування організації, що не може не вплинути на позитивну динаміку зростання її показників. З іншого – впровадження системи комплексної безпеки є досить витратним, часто обтяжливим для організації процесом.

Одним із принципів забезпечення безпеки є розумна достатність, визначити яку можна за допомогою методів та інструментів, що дозволяють оцінити величину витрат, плановану керівництвом організації для забезпечення безпеки свого бізнесу, а також той ефект, на який за цих умов можна розраховувати.

Створення СФЕБ організації поряд з визначенням переліку програмних заходів повинно враховувати також економічне оцінювання структури витрат на реалізацію запланованих заходів. Спочатку проводиться їх класифікація, що дозволяє організувати планування, облік і аналіз витрат і на цій основі вирішити завдання зниження собівартості впровадження системи безпеки.

Витрати класифікуються за такими ознаками (загальні підходи):

за економічними елементами;

за статтями калькуляції;

відносно до процесу виробництва;

за складом;

за способом віднесення на собівартість;

за роллю в процесі виробництва;

за можливістю охоплення плануванням;

відносно до обсягу виробництва;

за періодичністю виникнення;

відносно до готової продукції;

відносно до часу;

за місцем виникнення.

Основними складовими витрат на СФЕБ є:

витрати на підготовку програми – дослідження, аудит стану системи безпеки, планування заходів, вивчення досвіду забезпечення безпеки в аналогічних компаніях (маркетингові дослідження, організація та проведення тендерів, отримання, обробка й аналіз інформації);

вартість технічних пристроїв, виробів, матеріалів, комплектувальних, програмного забезпечення, використовуваних для створення системи безпеки;

вартість послуг сторонніх організацій, якщо вони задіяні у дослідженнях, експертних оцінюваннях, консультаціях, монтажі, пуско-налагоджувальних роботах, розрахунку основних показників та інших заходах;

заробітна плата адміністрації та робітників, задіяних в організації, контролі виконання робіт, монтажі, обслуговуванні, експлуатації та ремонті систем безпеки.

втрати від браку, упущень, технологічних збоїв; помилок роботи з системою в процесі монтажу, пуско-налагоджувальних робіт, експлуатації, технічного обслуговування та ремонту.

Для оцінювання економічної ефективності вкладень у забезпечення безпеки на практиці використовують ряд методів (моделей):

оцінювання сукупної вартості володіння системою безпеки *TCO* (total cost of ownership);

оцінювання повернення інвестицій *ROI* (return on investment);

стандартні методи оцінювання економічної ефективності інвестицій (віддача інвестицій);

віддача активів;

"ціна" акціонера;

оцінювання одноразових витрат на впровадження та закупівлю засобів захисту та ін.

Прикладом оцінювання витрат на СФЕБ може бути розрахунок сукупної вартості володіння службою ФЕБ, який характеризує загальну вартість володіння організації в цілому або його складової частини. Він є одним з найважливіших критеріїв у розгляді майбутніх проектів, оскільки визначає їх економічну обґрунтованість.

Основна мета розрахунку цього показника полягає в тому, щоб оцінити можливість повернення вкладених у безпеку коштів. Проте досить важко оцінити прямий економічний ефект від упровадження системи безпеки. Тому застосовують метод порівняння вартості володіння службою

ФЕБ (ВВСФЕБ) досліджуваної організації (наприклад, у перерахунку на одного співробітника) зі ВВСФЕБ інших аналогічних суб'єктів господарювання.

В основу моделі ВВСФЕБ покладені дві категорії витрат: прямі (бюджетні) та непрямі (рис. 6.2).

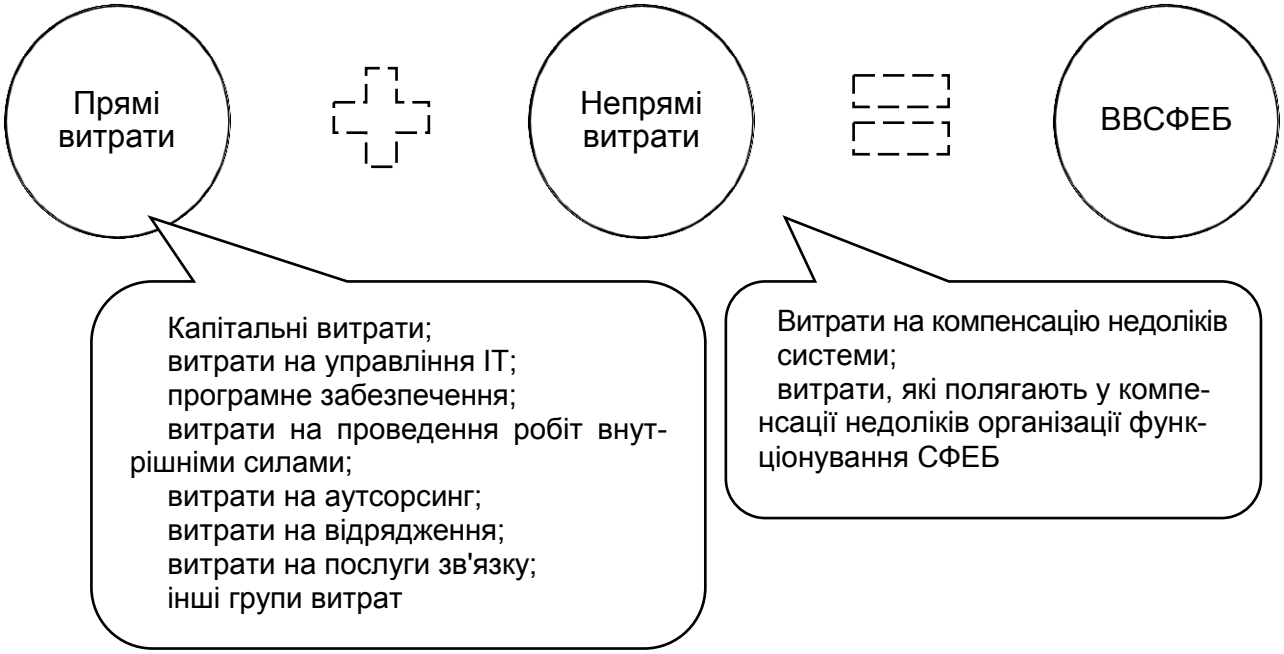

Рис. 6.2. **Структура витрат володіння службою ФЕБ організації**

ВВСФЕБ оцінюється з допомогою формул:

$$ВВСФЕБ = Пр + Кр1 + Кр2, \quad (6.1)$$

де *Пр* – прямі витрати;

Кр1 – непрямі витрати першої групи;

Кр2 – непрямі витрати другої групи.

$$Пр = Пр1 + Пр2 + Пр3 + Пр4 + Пр5 + Пр6 + Пр7 + Пр8, \quad (6.2)$$

де *Пр1* – капітальні витрати на обладнання приміщення та засобів служби ФЕБ (технічні та спеціальні пристрої);

Пр2 – витрати на управління ІТ (обслуговування та налагодження програмно-технічних засобів захисту; моніторинг процесів ІТ);

Пр3 – програмне забезпечення (оновлення програмного забезпечення);

Пр4 – витрати на проведення робіт внутрішніми силами (перевірка руху ТМЦ);

Пр5 – витрати на аутсорсинг (залучення зовнішніх фахівців, як то: експерти з кібербезпеки, незалежні аудитори, експерт з УФЕБ і перевірки контрагентів тощо);

Пр6 – витрати на відрядження (транспортні, добові);

Пр7 – витрати на послуги зв'язку (користування засобами зв'язку – мобільний зв'язок, рації);

Пр8 – інші групи витрат (робота з лояльними особами, агентурна робота).

Як правило, виділяють дві групи джерел виникнення непрямих витрат, пов'язаних зі створенням СФЕБ:

Кр1 – до першої групи належать витрати на компенсацію недоліків системи (наприклад, помилок проектування), що може викликати непродуктивне витрачання часу у користувачів і, як наслідок, втрати в бізнесі. Як правило, такі витрати важко визначити безпосередньо. Для цього слід розрізняти плановий і понаднормовий час непрацездатності;

Кр2 – до другої групи відносять такі витрати, які полягають у компенсації недоліків функціонування системи безпеки. Наприклад: унаслідок неналежної підтримки системи безпеки співробітники організації змушені особисто займатися роботою з відновлення працездатності технічних засобів, самонавчанням тощо, що, звісно, зменшує їх продуктивний час роботи.

Непрямі витрати можуть відігравати істотну роль в оцінюванні рішення за проектами. Для цього перша їх група може бути розглянута з використанням методу визначення виробничих втрат, а друга – за допомогою статистичних досліджень.

Показником, що дозволяє оцінити ефективність системи безпеки, є оцінка повернення інвестицій в інфраструктуру організації. Її визначають на основі моделі *ROI* (чиста приведена вартість), яка призначена для використання в якості способу обґрунтування необхідності вкладення коштів у систему безпеки організації. Така оцінка обчислюється шляхом розрахунку коефіцієнта повернення інвестицій в інфраструктуру організації.

Рекомендована література: [25; 29].

Практична частина

Контрольні запитання

1. Розкрийте змістовність моніторингу. Які завдання моніторингу в УФЕБ?

2. Розкрийте інформаційну роль моніторингу. Визначте класифікаційні ознаки інформації в УФЕБ.

3. Поясніть діагностичну роль моніторингу. У чому полягає відмінність аналітичної функції моніторингу від діагностики в УФЕБ?

4. Надайте визначення контролю та розкрийте змістовність внутрішнього контролю в організації.

5. Які основні елементи внутрішнього контролю організації, застосовувані в УФЕБ? Охарактеризуйте їх.

6. Яка міжнародна організація формує та розповсюджує стандарти організації внутрішнього контролю й управління ризиками в організації? У чому полягає значення її діяльності в питаннях УФЕБ?

7. Розкрийте концепцію управління ризиками організації COSO. Чому ризикам відводиться принципове значення в системах внутрішнього контролю?

8. Які критерії фінансово-економічної безпеки можуть бути застосовані для оцінювання УФЕБ організації?

9. Наведіть перелік основних фінансових коефіцієнтів, які використовують для оцінювання рівня фінансово-економічної безпеки організації. Поясніть їх.

10. Розкрийте структуру ознак шахрайства у фінансовій звітності організації. Надайте пояснення.

11. Наведіть кадрові та соціальні показники, які використовують для оцінювання фінансово-економічної безпеки організації.

12. Яким чином можна оцінити фінансово-економічний ризик? Розкрийте його змістовність.

13. Поясність і розмежуйте майнові, комерційні, інформаційні, кадрові, організаційні, комплаєнс-ризики організації.

14. Визначте структуру витрат на утримування СФЕБ організації.

15. Якими можуть бути джерела фінансування УФЕБ?

Тестові завдання

1. Спостереження за комплексом факторів фінансово-економічної безпеки, тобто тих, які створюють чи потенційно можуть створювати загрозу ФЕБ організації, з метою відстеження невідповідності стану початковим припущенням або бажаному результату – це компетенція:

а) організації;

б) контролю;

в) моніторингу;

г) аналізу.

2. Інформаційна роль моніторингу в СФЕБ полягає в:

а) оцінюванні фінансово-економічних ризиків, виявленні кризових явищ;

б) отриманні даних щодо стану ключових фінансово-економічних показників організації;

в) аналітичних процедурах обліку господарської діяльності організації;

г) усі відповіді правильні.

3. Організовані канали отримання інформації – це ті, які:

а) розміщені у відкритому доступі;

б) формуються й обслуговуються фахівцями СФЕБ;

в) здійснюються фахівцями підрозділу конкурентної розвідки з використанням не завжди законних методів отримання інформації;

г) усі відповіді правильні.

4. Інформація з обмеженим доступом – це інформація, яка:

а) вимагає проведення додаткових аналітичних розрахунків або оплати послуг сторонніх організацій;

б) не вимагає додаткових витрат;

в) передбачає не завжди законні дії та (або) вимагає значних витрат або залучення додаткових фахівців;

г) усі відповіді правильні.

5. Недостовірна інформація – це та, яка:

а) у повній мірі відображає реальний стан певного явища чи динаміку процесу;

б) поряд з достовірною інформацією містить і помилкову, зайву або дезінформацію;

в) не в повній мірі стосується об'єкта дослідження;

г) не відповідає реальному стану справ, є продуктом контррозвідки конкурентів або отримана з ненадійних джерел інформації і т. п.

6. Інформація, яка є комерційною таємницею, – це:

а) безкоштовна інформація, яка надходить через відкриті канали (телебачення, преса, Інтернет тощо);

б) інформація, отримання якої потребує організації інформаційного каналу, залучення фахівців (агентів), розроблення певного програмного забезпечення, визначених матеріальних, фінансових і трудових витрат;

в) інформація, яка має стратегічне значення для розвитку ринку, окремого сегмента або виду діяльності, отримання якої неможливе через відкриті канали інформації та вимагає істотних фінансових витрат;

г) правильної відповіді немає.

7. Процес розпізнавання загрози, її визначення, оцінювання вразливості до неї організації (наприклад, оцінювання фінансово-економічного стану підприємства) з метою виявлення небезпечних і кризових зон та оцінювання масштабу прояву кризи – це:

а) діагностика;

б) аналіз;

в) контроль;

г) усі відповіді правильні.

8. Відстеження кількісних та якісних змін індикаторів стану фінансово-економічної безпеки – це:

а) діагностика;

б) аналіз;

в) контроль;

г) усі відповіді правильні.

9. Загальна характеристика компанії, політики та процедур щодо внутрішнього контролю, розподіл відповідальності – це:

а) контрольне середовище;

б) оцінювання ризиків;

в) контрольні процедури;

г) інформація та комунікація.

10. Політика та процедури, контрольні заходи, які сприяють пом'якшенню ризиків, пов'язаних з досягненням цілей до прийнятного рівня, – це:

а) контрольне середовище;

б) оцінювання ризиків;

в) контрольні процедури;

г) інформація та комунікації.

11. Створення та використання актуальної, якісної інформації для підтримки функціонування СФЕБ, організація взаємодії з зовнішніми сторонами – це елементи:

а) контрольного середовища;

б) оцінювання ризиків;

в) контрольних процедур;

г) інформації та комунікації.

12. Імовірність фінансових втрат для організації через усвідомлену небезпеку дії чи бездіяльність в різних варіантах економічної поведінки – це ризик:

а) фінансово-економічний;

б) комерційний;

в) комплаєнс;

г) кадровий.

13. Ймовірність здійснення загроз, пов'язаних з повною або частковою втратою майна організації, – це ризик:

а) фінансово-економічний;

б) комерційний;

в) комплаєнс;

г) майновий.

14. Ризики, пов'язані з імовірністю реалізації антропогенних загроз, що виходять від людей, – це ризики:

а) фінансово-економічні;

б) комерційні;

в) комплаєнс;

г) кадрові.

15. Недоліки в системі управління ризиками шахрайства, які допомагають запобігати, виявляти, розслідувати та реагувати на випадки шахрайства, як то: виникнення/повторення випадків шахрайства (якщо не змінити організаційну систему, кадрову складову фінансово-економічної безпеки), неефективна координація внаслідок відсутності регламентів (положень, інструкцій) щодо забезпечення кадрової та фінансово-економічної безпеки, розкриття/просочування комерційної таємниці, втрата репутації й іміджу організації – це ризики:

а) фінансово-економічні;

б) комерційні;

в) комплаєнс;

г) кадрові.

Комплексні практичні завдання

Завдання 1

Мета – здійснити оцінювання організації фінансово-економічної безпеки компанії та розробити відповідні рекомендації.

Результати ревізійної перевірки, яка здійснюється один раз на рік, поставили під сумнів ефективність управління та стан справ у компанії "Soyuz" з боку американського учасника товариства – корпорації "Medina Inc.". Стали відомі такі факти.

1. У ході перевірки фінансової звітності компанії "Soyuz" були виявлені ознаки можливого викривлення інформації/шахрайства в фінансовій звітності: штучне завищення величини дебіторської заборгованості зі зниженням рівня продажів; списання безнадійної дебіторської заборгованості; зростання величини кредитного ризику, якому піддається компанія.

2. Ревізор отримав повідомлення з "гарячої лінії", а саме: заступник керівника салону-магазину компанії "Soyuz" займається замовленням комплектувальних для комп'ютерної техніки (збирання заявок від відділів, замовлення комплектувальних і оформлення актів на списання). Зазвичай керівник салону-магазину, в обов'язки якого входить санкціонування заявок, не перевіряє їх і підписує один раз в кінці місяця. Є підозра, що заступник керівника салону-магазину став завищувати замовлення, а надлишки списувати та привласнювати. Відомо, що він має власний магазин комплектувальних для комп'ютерної техніки. Крім того, номенклатура його магазину не відрізняється від номенклатури комплектувальних для комп'ютерної техніки компанії "Soyuz".

Надайте обґрунтовані відповіді на запитання

1. На основі наведеної інформації про компанію, її організаційну структуру (додаток Б), розподіл повноважень органів управління (додаток В), дайте оцінку організації фінансово-економічної безпеки компанії "Soyuz".

2. Надайте рекомендації щодо удосконалення/створення системи фінансово-економічної безпеки в компанії "Soyuz":

- назвіть організаційно-розпорядчі документи, які мають закріплювати обов'язки в системі фінансово-економічної безпеки компанії;

- кому має підпорядковуватися відділ/служба фінансово-економічної безпеки компанії: загальним зборам учасників, директорові чи ревізійній комісії? Визначте переваги вашої пропозиції та місце відділу/служби з фінансово-економічної безпеки в організаційній структурі компанії (наведіть схему);
- розкрийте основні принципи управління, за якими має бути організована відповідна служба/відділ;
- надайте рекомендації щодо компетенцій персоналу відділу/служби з фінансово-економічної безпеки компанії;
- визначте, які переваги матиме компанія від створення відділу/служби з фінансово-економічної безпеки.

Завдання 2

Мета – закріпити знання способів здійснення шахрайських дій серед персоналу підприємства й індикаторів їх розпізнавання.

Державне підприємство "Інженерні системи" (Підприємство-замовник) планує закупівлю послуг з охорони майна. Комітетом з конкурсних торгів ДП "Інженерні системи" відповідно до норм чинного законодавства заплановано й організовано процедуру відкритих торгів, у рамках якої буде укладено договір про закупівлю охоронних послуг з переможцем.

Специфіка діяльності ДП "Інженерні системи" вимагає з боку його посадових осіб ретельного підходу до вибору потенційного контрагента в частині забезпечення майнової безпеки.

На конкурс подано документи від ТОВ "Барс" (додаток Г) та ТОВ "Лео" (додаток Д), основна сфера діяльності яких – надання послуг з охорони власності та громадян.

Надайте обґрунтовані відповіді на запитання щодо оцінювання та відбору потенційного контрагента

1. Якими основними нормативно-правовими актами має керуватись ДП "Інженерні системи" для організації та проведення закупівлі даного виду послуг?

2. Яким кваліфікаційним критеріям згідно з чинним законодавством має відповідати учасник конкурсних торгів (суб'єкт охоронної діяльності)? Наведіть їх.

3. Надайте висновок щодо відповідності учасників торгів означеним критеріям. Необхідна інформація про суб'єктів охоронної діяльності додається: ТОВ "Барс" – додаток Г, ТОВ "Лео" – додаток Д.

4. За результатами розгляду визначте й обґрунтуйте вибір учасника-переможця.

5. Які документи може додатково вимагати Підприємство-замовник від учасників для підтвердження відповідності наведеним кваліфікаційним критеріям?

6. На якій підставі Підприємство-замовник може прийняти рішення про відмову суб'єкту охоронної діяльності в участі у процедурі закупівлі та відхилити його пропозицію?

7. Які документи мають надати суб'єкти охоронної діяльності в складі своїх пропозицій, щоб підтвердити доцільність своєї участі у відкритих торгах?

Завдання 3

Мета – закріпити знання способів здійснення шахрайських дій серед персоналу підприємства й індикаторів їх розпізнавання.

ТОВ "Альянс" входить у десятку найбільших бюджетоутворювальних компаній в області. Основними видами діяльності товариства є: оптова торгівля автомобільними деталями та приладдям; посередництво в торгівлі автомобільними деталями та приладдям; організація перевезення вантажів. В асортименті компанії продукція більше трьохсот виробників (30 одиниць товару в продуктовому портфелі), найбільший в Україні склад запасних частин і комплектувальних до вантажних і легкових автомобілів країн СНД і далекого зарубіжжя. Товариство має розгалужену партнерську мережу роздрібних магазинів з торгівлі автокомпонентів.

З метою усунення можливих чинників загроз діяльності та фінансово-економічному стану ТОВ "Альянс":

1) визначте, які найбільш розповсюджені дії менеджменту (способи шахрайства) призводять до викривлення інформації:

у розмірі виручки та прибутку підприємства;

про активи та пасиви підприємства;

у примітках до фінансової звітності;

2) за наведеними даними методикою розрахунку та значеннями фінансових індикаторів ТОВ "Альянс" (табл. 7.1) надайте їх інтерпретацію та вкажіть ознаки можливого викривлення інформації (шахрайства);

Таблиця 7.1

Значення фінансових індикаторів для ТОВ "Альянс"

Фінансові індикатори можливого шахрайства	Формула розрахунку індикатора	Значення за роками	
		попередній рік	звітний рік
Темп зміни виручки від реалізації продукції	В1/В0, де В1, В0 – виручка від реалізації продукції за звітний (попередній) період	1,54	1,12
Темп зниження частки маржинального доходу у виручці від реалізації	[(В0 - С0) / В0] / [(В1 - С1) / В1], де В1, В0 – виручка від реалізації продукції за звітний (попередній) період; С1, С0 – собівартість реалізованої продукції за звітний (попередній) період	1,0	1,09
Темп зміни якості активів	[(А1-ПА1-ОЗ1)/А1]/[(А0-ПА0-ОЗ0)/А0], де А1, А0 – сукупна величина активів на кінець звітного (попереднього) періоду; ПА1, ПА0 – величина оборотних (поточних) активів на кінець звітного (попереднього) періоду; ОЗ1, ОЗ0 – залишкова вартість основних засобів на кінець звітного (попереднього) періоду	0,48	1,25
Темп зміни оборотності дебіторської заборгованості	(365/(В1/ДЗ1) дн.)/(365/(В0/ДЗ0) дн.), де ДЗ1, ДЗ0 – дебіторська заборгованість на кінець звітного (попереднього) періоду; В1, В0 – виручка від реалізації продукції за звітний (попередній) період	0,47	0,61
Темп зміни частки витрат у виручці від продажу	(Р1/В1)/(Р0/В0), де Р1, Р0 – повна собівартість реалізованої продукції за звітний (попередній) період; В1, В0 – виручка від продажу за звітний (попередній) період	1,0	0,99
Темп зміни частки амортизаційних відрахувань	(А1/ПВ1)/(А0/ПВ0), де А1, А0 – сума амортизаційних відрахувань за звітний (попередній) період; ПВ1, ПВ0 – первісна вартість основних засобів на кінець звітного (попереднього) періоду	1,1	1,06
Темп зміни фінансового важелю	(ПК1/ВК1)/(ПК0/ВК0), де ПК1, ПК0 – величина позикового капіталу на кінець звітного (попереднього) періоду; ВК1, ВК0 – власний капітал на кінець звітного (попереднього) періоду	0,51	1,79

3) визначте посади працівників служби фінансово-економічної безпеки, які компетентні з питань попередження й усунення виявлених загроз. Розкрийте їх завдання й обов'язки.

Глосарій професіонала з фінансово-економічної безпеки

Безпека організації – захищеність організації від негативного впливу зовнішніх і внутрішніх загроз, дестабілізаційних факторів, за умов чого досягається стале функціонування та розвиток організації.

Внутрішній контроль – здійснюється Радою директорів, менеджментом та іншим персоналом організації; спрямований на забезпечення поміркованої гарантії досягнення цілей за такими категоріями, як: ефективність і результативність операцій компанії; достовірність фінансової звітності; дотримання відповідного законодавства, підзаконних актів і регламентів.

Вразливість – слабкі місця в безпеці або процесі захисту організації.

Економічна безпека підприємства – система захисту бізнес-процесів і результатів господарської діяльності підприємства від небажаних змін.

Загроза – небезпека, пов'язана з: деклараціями наміру заподіяти шкоду; визначенням чогось поганого – знак або небезпека, що щось небажане може статися; ситуацією, коли хто-небудь або що-небудь здатні нанести шкоду або біль, наприклад: людина, тварина, який-небудь предмет.

Загрози фінансово-економічній безпеці підприємництва – потенційні або реально можливі події, процеси, явища або дії фізичних та юридичних осіб, що порушують стан захищеності суб'єкта підприємницької діяльності, його стійкість і розвиток і здатні призвести до припинення його діяльності або до фінансово-економічних втрат.

Інформаційні ризики – ризики, пов'язані зі втратою, спотворенням, розкраданням інформації в процесі її отримання, обробки, зберігання, передання. Особливо слід зазначити ризики асиметричної інформації, в основу яких закладена специфіка вимог учасників ділових відносин до повноти, своєчасності та достовірності переданої інформації.

Кадрова безпека – процес запобігання негативним впливам на корпоративну (економічну) безпеку організації через ризики та загрози, пов'язані з персоналом, його інтелектуальним потенціалом і трудовими відносинами у цілому.

Концепція фінансово-економічної безпеки організації – офіційний документ, який надає повне уявлення про систему сервісу та підтримки розвитку організації, захист активів, місце УФЕБ, її обґрунтованість.

Комерційні ризики – ризики, пов'язані з реалізацією, транспортуванням, прийманням товару, неплатоспроможністю покупця, форс-мажорними обставинами.

Комплаєнс-ризики – недоліки в системі управління ризиками від шахрайства та комплаєнс, які заважають запобігати, виявляти, розслідувати та реагувати на випадки шахрайства. До них відносять: виникнення/повторення випадків шахрайства (якщо не змінити організаційну систему та кадрову складову фінансово-економічної безпеки); неефективну координацію внаслідок відсутності регламентів (положень, інструкцій) щодо забезпечення кадрової та фінансово-економічної безпеки; розкриття/просочування комерційної таємниці; втрата репутації та іміджу організації.

Компоненти системи фінансово-економічної безпеки організації – це ті її елементи, блоки й одиниці організації, які виконують певні самостійні функції, а в поєднанні забезпечують виконання повного циклу функцій з УФЕБ.

Корпоративна безпека – захист корпоративних активів, тобто тих, які підтримують і сприяють веденню бізнесу та приносять прибуток.

Незалежність підрозділу ФЕБ – передбачає свободу від умов, які створюють загрозу здатності підрозділу неупереджено виконувати свої обов'язки.

Майнові ризики – ймовірність здійснення загроз, пов'язаних з повною або частковою втратою майна організації. Показниками, що використовуються для оцінювання майнового ризику, виступають: норми природного убутку під час зберігання, норми амортизації, страхові тарифи (нетто-ставки).

Механізми реалізації загрози – мотиви, засоби та способи здійснення загроз.

Можливість учинити шахрайство, приховати його та уникнути покарання – елемент "трикутника шахрайства", який розподіляють на чинники, пов'язані та не пов'язані з контролем.

Моніторинг – спостереження за комплексом факторів фінансово-економічної безпеки, тобто тих, які створюють чи потенційно можуть створювати загрозу ФЕБ організації, з метою відстеження невідповідності стану початковим припущенням або бажаному результату.

Мотивація, тиск – обставини, що змушують людину здійснити шахрайську дію.

Об'єкт ФЕБ – корпоративне середовище – все те, на що спрямовані зусилля щодо забезпечення ФЕБ.

Об'єктивність роботи підрозділу ФЕБ – уявна настанова, яка дає змогу професіоналам і фахівцям з ФЕБ виконувати завдання неупереджено – таким чином, щоб вони самі відчували відповідальність і довіру до результатів своєї роботи та не допускали компромісів щодо її якості.

Організаційний механізм УФЕБ – СФЕБ організації в дії.

Організаційні ризики – ризики, пов'язані з недоліками організації системи фінансово-економічної безпеки. До них можна віднести ризики неефективної координації робіт щодо забезпечення фінансово економічної безпеки, втрата контролю за рухом товарно-матеріальних цінностей, невиконання персоналом посадових обов'язків належним чином, збільшення можливостей для випадків шахрайства серед персоналу, некомпетентні дії контролюючих підрозділів.

Підрозділ ФЕБ – штатна структурна одиниця організації (компанії, акціонерного товариства, холдингу, корпорації, підприємства) з самостійними функціями, завданнями та відповідальністю.

Політика фінансово-економічної безпеки організації – містить опис загальних дій і орієнтирів для прийняття рішень, спрямованих на досягнення цілей УФЕБ і таких, що визначають відношення з людьми.

Ризик: 1) шанс, що щось піде не так (небезпека травми, руйнування або втрати, які можуть статися); 2) можливість інвестиційних втрат, спекуляції; 3) статистичні коефіцієнти загрози, ймовірність загрози від чогонебудь, як то: невдачі інженерних систем.

Система фінансово-економічної безпеки: 1) сукупність елементів, функціонування яких забезпечує ефективну діяльність у сфері захисту активів організації, здійснення бізнес-процесів і захисту результатів фінансово-господарської діяльності, спрямованих на досягнення мети, тобто планованого результату забезпечення ФЕБ; 2) комплекс професійних засобів і методів у сукупності з органами, до компетенції яких входить забезпечення ФЕБ організації (бізнесу, підприємства, компанії).

Суб'єкт ФЕБ – особи, підрозділи, служби, органи, відомства, установи, які безпосередньо виконують функції щодо забезпечення та підтримки безпечного стану діяльності.

Фінансово-економічна безпека (ФЕБ) – діяльність, здійснювана з метою надання об'єктивних гарантій і консультацій щодо створення

та захисту сталого та прибуткового функціонування, розвитку та вимогливого дотримання встановлених режимів (організаційних, юридичних, виробничих, фінансових тощо) організації, спрямована на вдосконалення діяльності; є невід'ємною частиною контролю та підтримки управлінських рішень на підприємстві.

Фінансово-економічний ризик – ймовірність фінансових втрат для організації через усвідомлену небезпеку, дії чи бездіяльність у різних варіантах економічної поведінки.

Шахрайство: 1) кримінальний обман; людина або річ, яка не є тим, чим себе подає (Оксфордський словник); 2) використання свого становища з метою особистого збагачення шляхом навмисного неефективного використання ресурсів або активів організації, яка наймає на роботу (Асоціації сертифікованих фахівців з розслідування шахрайства (ACFE); 3) навмисні дії одної або більше осіб серед керівництва, управлінського персоналу, працівників або третіх осіб, що полягають у використанні обману для отримання неправомірної або незаконної вигоди (Міжнародні стандарти аудиту ISA 240).

Рекомендована література

1. Андрощук Г. А. Экономическая безопасность предприятия: защита коммерческой тайны : [монограф.] / Г. А. Андрощук, П. П. Крайнев. – Киев : ИД "Ин Юре", 2000. – 400 с.

2. Бачинин В. А. Социология: Три курса лекций студентам-юристам : учеб. пособ. / В. А. Бачинин. – Харьков : Консум, 2003. – 567 с.

3. Берлач А. І. Безпека бізнесу / А. І. Берлач. – Київ : Ун-т "Україна", 2007. – 280 с.

4. Большой экономический словарь / под ред. А. Н. Азрилияна. – 5-е изд., доп. и перераб. – Москва : Ин-т новой экономики, 2002. – 1280 с.

5. Брюханов М. Мошенничество в финансовой отчетности на развивающихся рынках / М. Брюханов // Корпоративное управление. – 2006. – № 15 (318). – С. 48–52.

6. Васин С. М. Управление рисками на предприятии [Текст] : учеб. пособ. / С. М. Васин, В. С. Шутов. – Москва : КНОРУС, 2010. – 304 с.

7. Вечканов Г. С. Экономическая безопасность : учебник для вузов / Г. С. Вечканов. – Санкт–Петербург : Питер, 2007. – 384 с.

8. Гапоненко В. Ф. Экономическая безопасность предприятий. Подходы и принципы / В. Ф. Гапоненко, А. Л. Беспалько, А. С. Власков. – Москва : Изд. "Ось–89", 2007. – 208 с.

9. Гнилицкая Л. В. Теоретико-методологические и прикладные основы обеспечения экономической безопасности субъектов хозяйственной деятельности : монография / Л. В. Гнилицкая, А. И. Захарок, П. Я. Прыгунов. – Киев : Дорадо-Друк, 2001. – 290 с.

10. Дворский М. Н. Техническая безопасность объектов предпринимательства / М. Н. Дворский, С. Н. Палатченко. – Киев : А-ДЕПТ, 2006. – 304 с.

11. Духов В. Е. Экономическая разведка и безопасность бизнеса / В. Е. Духов. – Киев : ИМСО МО Украины, 1997. – 176 с.

12. Економіка підприємства : навч. посіб. / Є. В. Мішенін, Є. О. Балацький, О. М. Дутченко та ін.; за заг. ред. Є. В. Мішеніна, Є. О. Балацького. – Суми : Диса плюс, 2015. – 336 с.

13. Економічна безпека підприємств : підручник / В. Л. Ортинський, І. С. Керницький, З. Б. Живко та ін. ; за ред. В. Л. Ортинського. – Київ : Алерта, 2011. – 704 с.

14. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи / А. Б. Качинський. – Київ : Нац. академія Служби безпеки України, 2004. – 472 с.

15. Козаченко А. В. Экономическая безопасность предприятия: сущность и механизм обеспечения / А. В. Козаченко, В. Г. Пономарев, А. Н. Ляшенко. – Киев : Либра, 2003. – 280 с.

16. Крутов В. В. Від патріотичного виховання, боротьби з тероризмом … до недержавної системи національної безпеки / В. В. Крутов. – Київ : Вид. "Преса України", 2009. – 592 с.

17. Мак-Мак В. П. Служба безопасности предприятия (организационно-управленческие и правовые аспекты деятельности) / В. П. Мак-Мак. – Москва : Баярд, 2003. – 208 с.

18. Маслоу А. Мотивация и личность / А. Маслоу; пер. с англ. – 3-е изд. – Санкт-Петербург : Изд-во "Питер", 2008. – 352 с.

19. Механизм управления предприятием: стратегический аспект / В. С. Пономаренко, Е. Н. Ястремская, В. М. Луцковский и др. ; под ред. В. С. Пономаренко. – Харьков : Изд. ХГЭУ, 2002. – 252 с.

20. Минаев Г. А. Безопасность организации : учебник / Г. А. Минаев. – Киев : КНТ, 2009. – 440 с.

21. Мойсеєнко І. П. Управління фінансово-економічною безпекою підприємства : навч. посіб. / І. П. Мойсеєнко, О. М. Марченко – Львів : ЛьвДУВС, 2011. – 380 с.

22. Одинцов А. А. Защита предпринимательства. Экономическая и информационная безопасность / А. А. Одинцов. – Москва : Международные отношения, 2003. – 120 с.

23. Отенко І. П. Аналіз господарської діяльності : навч. посіб. / І. П. Отенко, З. Ф. Петряєва. – Харків : Вид. ХНЕУ ім. С Кузнеця, 2014. – 420 с.

24. Отенко І. П. Економічна безпека підприємства : навч. посіб. / І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Харків. : Вид. ХНЕУ, 2012. – 256 с.

25. Отенко І. Становлення теорії управління безпекою соціальних систем / І. Отенко, Н. Москаленко, Д. Комарков // Зб. наук. праць ЧДТУ. Серія: Економічні науки. – 2013. – Вип. 35. – Ч. ІІІ. – Т. 2. – С. 85–91.

26. Отенко І. П. Теорія управління безпекою соціальних систем : навч. посіб. / І. П. Отенко, Н. О. Москаленко. – Харків : Вид. ХНЕУ ім. С. Кузнеця, 2014. – 232 с.

27. Подольчак Н. Організація та управління системою фінансово-економічної безпеки : навч. посіб. / Н. Подольчак, В. Карковська. – Львів : М-во освіти і науки України; Нац. ун-т "Львівська політехніка", 2014. – 267 с.

28. Савицкая Г. В. Анализ эффективности и рисков предпринимательской деятельности: методологические аспекты [Текст] : учеб. пособ. / Г. В. Савицкая. – Москва : Инфра-М, 2010. – 272 с.

29. Система економічної безпеки: держава, регіон, підприємство : В 3 т. / Г. В. Козаченко, О. М. Ляшенко, Ю. С. Погорелов [та ін.] / за заг. ред. Г. В. Козаченко. – Луганськ : Елтон–2, 2010. – 281 с.

30. Скібіцький О. М. Організація бізнесу. Менеджмент підприємницької діяльності : навч. посіб. / О. М. Скібіцький, В. О. Матвєєв, Л. І. Скібіцька. – Київ : Кондор, 2011. – 912 с.

31. Соснин А. С. Менеджмент безопасности предпринимательства : учеб. пособ. / А. С. Соснин, П. Я. Прыгунов. – Киев : Изд. Европейского ун-та, 2002. – 357 с.

32. Ступаков В. С. Риск-менеджмент [Текст] : учеб. пособ. / В. С. Ступаков, Г. С. Токаренко. – Москва : Финансы и статистика, 2008. – 288 с.

33. Тумар Н. Б. Экономическая безопасность предприятия / Н. Б. Тумар. – Харьков : Харьковский ин-т бизнеса и менеджмента, 2006. – 160 с.

34. Філиппова С. В. Аналітичні інструменти системи економічної безпеки суб'єктів господарювання (на прикладі виноробних підприємств) : монографія / С. В. Філиппова, С. А. Нізяєва. – Донецьк : Ноулідж (Донец. відділення), 2012. – 179 с.

35. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення : монографія / Т. Г. Васильців , В. І. Волошин, О. Р.Бойкевич та ін.; за ред. Т. Г. Васильціва. – Львів : Ліга-Прес, 2012. – 386 с.

36. Экономическая безопасность предприятий интегрированной промышленной структуры / А. В. Козаченко, Ю. С. Погорелов, А. Н. Ляшенко и др. ; под общ. ред. А. В. Козаченко. – Луганск : НОУЛИДЖ, 2011. – 226 с.

37. Ярочкин В. И. Секьюритология – наука о безопасности жизнедеятельности / В. И. Ярочкин. – Москва : Ось-89, 2000. – 216 с.

38. Williams A. R. Corporate Manager's Security Handbook. / A. R. Williams. – AuthorHouse, 2012. – 84 p.

39. Hayes B. Corporate Security Organizational Structure, Cost of Services and Staffing Benchmark: Research Report / B. Hayes, G. Kane, K. Kotwica. – Elsevier, 2013. – 76 p.

40. Kovacich G. L. The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program / G. L. Kovacich, E. P. Halibozek. – Butterworth-Heinemann, 2003. – 463 p.

41. Moskalenko N. Approaches to enterprises' financial and economic security management / N. Moskalenko, O. Romanenko, T. Oliinyk // Economic Annals-XXI. – 2015. – № 7-8 (1). – Pp. 54–57.

42. Moskalenko N. Critical issues of economic security of organizations / N. Moskalenko // Economics of Development. – 2016. – № 1 (77). – Pp. 69–76.

43. Всесвітній огляд динаміки економічної злочинності. Звіт по Україні // PricewaterhouseCoopers, 2009 [Електронний ресурс]. – Режим доступу : https://www.pwc.com/ua/en/services/forensic/assets/gecs_2009_report_ukraine_ukr.pdf.

44. Довідник кваліфікаційних характеристик професій працівників. – Вип. 99 "Безпека господарської діяльності підприємства, установи, організації" [Електронний ресурс]. – Режим доступу : http://zakon.golovbukh.ua/regulations/1521/8196/8197/461210/.

45. Иващенко Г. В. О понятии "безопасность" / Г. В. Иващенко [Электронный ресурс]. – Режим доступа : http://www.portalus.ru /modules /philosophy/print.php?archive=0215&id=1108062853&start_from&subaction=showfull&ucat=1.

46. Косенко О. Правові аспекти здійснення державного нагляду (контролю) у сфері господарської діяльності / О. Косенко [Електронний ресурс]. – Режим доступу : http://old.minjust.gov.ua/24659.

47. Крутов В. В. Недержавний сектор безпеки як складова системи забезпечення національної безпеки України / В. В. Крутов, Г. П. Новицький // Радник. Український юридичний портал [Електронний ресурс]. – Режим доступу : http://radnuk.info/statti.html.

48. Національний класифікатор України: класифікатор професій ДК 003:2010 [Електронний ресурс]. – Режим доступу : http://hrliga.com/index.php?module=norm_base&op=view&id=433.

49. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом : Закон України № 1702-VII від 14.10.2014 р. // Відомості Верховної Ради. – 2014. – № 50–51 – Ст. 2057 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/1702-18.

50. Про основні засади державного нагляду (контролю) у сфері господарської діяльності: Закон України № 877-V від 05.04.2007 р. // Відомості Верховної Ради України (ВВР). – 2007. – № 29. – Ст. 389 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua /laws/show/877-16/page.

51. Тоффлер Э. Шок будущего / Э. Тоффлер ; пер. с англ. – Москва : ООО "Изд. АСТ", 2002. – 557 с. [Электронный ресурс]. – Режим доступу : http://www.chronos.msu.ru/old/RREPORTS/toffler_shok/toffler_shok.htm.

52. Україна: Всесвітній огляд економічних злочинів. Кіберзлочини в центрі уваги // PricewaterhouseCoopers, 2011. – 16 с. [Електронний ресурс]. – Режим доступу : https://www.pwc.com/ua/uk/press-room/assets /gecs_ukraine_ua.pdf.

53. Федерація роботодавців України [офіційний сайт]. – Режим доступу : http://reestr.fru.org.ua/.

54. Федулов М. Концепция безопасности бизнеса: правильная постановка вопросов / М. Федулов // Association of Certified Fraud Examiners – 2011 [Электронный ресурс]. – Режим доступа : http://www.acfe-rus.org /page.php?id=155.

55. Філиппова С. В. Система формування і забезпечення економічної безпеки підприємства / С. В. Філиппова, О. С. Дашковський // Економіка: реалії часу : наук. журнал. – 2012. – № 2 (3). – С. 17–21 ; [Електронний ресурс]. – Режим доступу : http://www.economics.opu.ua/n3.html.

56. Global Economic Crime Survey // PricewaterhouseCoopers. – 2016. – 56 p. [Electronic resource]. – Access mode : http://www.pwc.com /gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf.

57. Cybercrime: protecting against the growing threat // Pricewaterhouse-Coopers, 2011. – 40 p. [Electronic resource]. – Access mode : http://pwc.blogs.com/files/2011-global-economic-crime-survey-report.pdf.

58. Edwin H. Sutherland. Is "White Collar Crime" Crime? // American Sociological Review. – 1944. – Vol. 10, No 2. – Annual Meeting Papers (Apr., 1945), pp. 132 – 139. [Electronic resource]. – Access mode : http://faculty. washington.edu/matsueda/courses/371/Readings/White%20Collar%20Crime.pdf.

.

Додатки

Додаток А

Таблиця А.1

Опис основних посад персоналу підрозділу ФЕБ організації [44]

Найменування посад персоналу підрозділу ФЕБ	**Основні функціональні завдання й обов'язки**
1	2
Керівник (директор, начальник) підрозділу (служби, управління, департаменту) з фінансово-економічної безпеки	Контролює та координує напрями робіт з розроблення, запровадження та реалізації заходів із забезпечення фінансово-економічної безпеки. Відповідає за дотримання підрозділом усіх зобов'язань із фінансово-економічної секретності перед державними та приватними юридичними особами. Затверджує (візує) керівні документи, які стосуються організації діяльності системи фінансово-економічної безпеки підрозділу, механізмів управління та взаємодії. Організовує роботу й ефективну взаємодію всіх структурних підрозділів, які пов'язані з дотриманням норм фінансово-економічної секретності. Забезпечує виконання підрозділом програм, планів щодо впровадження новітніх технологій у сфері фінансово-економічної безпеки. Уживає заходів щодо забезпечення підрозділу працівниками з питань фінансово-економічної безпеки, найкращого використання їх знань і досвіду. Під час виявлення зовнішніх і внутрішніх загроз і ризиків у сфері фінансово-економічної безпеки підрозділу координує та контролює хід виконання відповідних процедур щодо їх усунення та зменшення. Вирішує питання щодо фінансово-економічної безпеки в межах наданих йому повноважень, доручає виконання окремих функцій іншим працівникам: своїм заступникам, керівникам відповідних структурних підрозділів. Затверджує правовий статус структури підрозділів фінансово-економічної безпеки. Координує роботи зі створення та впровадження нових технологій щодо зниження загроз і ризиків діяльності підрозділу, забезпечення фінансово-економічної безпеки.

Продовження табл. А.1

1	2
	У межах наданих йому повноважень надає всім категоріям посадових осіб інформацію, яка стосується діяльності із забезпечення фінансово-економічної безпеки. Установлює межі взаємодії інших керівників підрозділу фінансово-економічної безпеки з органами державної влади, іншими державними органами, підприємствами, установами й організаціями, громадськими об'єднаннями та громадянами під час проведення заходів щодо забезпечення безпеки. Контролює організацію підвищення кваліфікації працівників структурних підрозділів у галузі фінансово-економічної безпеки. Сприяє захисту фінансово-економічних інтересів підрозділу в суді, органах державної влади й управління, приватних і юридичних осіб. Забезпечує дотримання законності, активне використання правових засобів удосконалення управління та функціонування в ринкових умовах, зміцнення договірної, економічної та фінансової дисципліни.
Керівник (начальник) підрозділу (відділу, сектору, групи) з фінансово-економічної безпеки	Забезпечує організацію управління фінансово-економічним, майновим напрямами роботи підрозділу (відділу, сектору, групи). Організовує та координує напрями робіт з розроблення, запровадження та реалізації заходів із забезпечення фінансово-економічної безпеки. Забезпечує дотримання підрозділом (відділом, сектором, групою) всіх зобов'язань із фінансово-економічної секретності. Забезпечує виконання підрозділом (відділом, сектором, групою) програм, планів щодо впровадження новітніх технологій у сфері фінансово-економічної безпеки, оновлення відповідних програмних забезпечень. Уживає заходів щодо забезпечення підрозділу (відділу, сектору, групи) працівниками з питань фінансово-економічної безпеки, найкращого використання їх знань і досвіду. Під час виявлення зовнішніх і внутрішніх загроз і ризиків у сфері фінансово-економічної безпеки підрозділу (відділу, сектору, групи) спрямовує роботу на виконання відповідних процедур щодо їх усунення та зменшення. Вирішує питання щодо фінансово-економічної безпеки в межах наданих йому повноважень, доручає виконання окремих функцій підлеглим працівникам

Продовження табл. А.1

1	2
	Розроблює правовий статус структури підрозділів фінансово-економічної безпеки. Керує роботами зі створення та впровадження нових технологій щодо зниження загроз і ризиків діяльності підрозділу (відділу, сектору, групи), забезпечення фінансово-економічної безпеки. У межах наданих йому повноважень надає всім категоріям посадових осіб інформацію, яка стосується діяльності із забезпечення фінансово-економічної безпеки. Контролює забезпечення підвищення кваліфікації працівників підрозділу (відділу, сектору, групи) у сфері фінансово-економічної безпеки. Сприяє захисту фінансово-економічних інтересів підрозділу (відділу, сектору, групи) в суді, органах державної влади й управління, приватних і юридичних особах. Забезпечує дотримання законності, активне використання правових засобів удосконалення управління та функціонування в ринкових умовах, зміцнення договірної, економічної та фінансової дисципліни
Професіонал з фінансово-економічної безпеки	Розроблює, запроваджує та реалізує на практиці заходи із забезпечення фінансово-економічної безпеки. Визначає перспективність та ефективність інноваційної діяльності в галузі фінансово-економічної безпеки підприємства відповідно до встановлених стандартів (норм). Застосовує техніку та технології із забезпечення фінансово-економічної безпеки. Забезпечує підготовку керівних документів, які стосуються організації діяльності системи фінансово-економічної безпеки підприємства, механізмів управління та взаємодії. Розроблює проекти положень, наказів та інструкцій, що регламентують функціонування системи безпеки, а також діяльність підрозділу економічної безпеки підприємства та його взаємодію з іншими структурними підрозділами. Визначає зовнішні та внутрішні загрози та ризики у сфері фінансово-економічної безпеки підприємства. Сприяє здійсненню інформаційно-аналітичного забезпечення щодо оцінювання рівня реальних і потенційних загроз фінансово-економічній безпеці підприємства

Продовження табл. А.1

1	2
	Проектує систему підготовки керівного складу та персоналу підприємства щодо проведення ефективних заходів зі зниження рівня небезпек, загроз та ризиків. Розроблює плани щодо забезпечення фінансово-економічної безпеки й її удосконалення, проведення окремих спеціальних заходів щодо оперативного реагування на загрози, ризики, небезпеки для діяльності підприємства. Надає пропозиції щодо визначення правового статусу, структури підрозділу економічної безпеки підприємства та визначення його основних функцій. Бере участь у створенні та використанні нових технологій щодо зниження загроз і ризиків діяльності підприємства, забезпечення фінансово-економічної безпеки. Бере участь у розробленні стратегічної орієнтації підприємства з урахуванням вимог до забезпечення фінансово-економічної безпеки. Розроблює документи, що визначають стандарти безпеки, повноваження структурних підрозділів підприємства, види та напрями їх діяльності щодо запобігання загрозам, ризикам, небезпеці та забезпечення фінансово-економічної безпеки. У межах наданих йому повноважень надає всім категоріям працівників підприємства інформацію, яка стосується діяльності із забезпечення фінансово-економічної безпеки. Здійснює загальний контроль за діяльністю структурних підрозділів підприємства щодо забезпечення фінансово-економічної безпеки. Готує пропозиції щодо організації взаємодії керівників підприємства, підрозділу економічної безпеки з органами державної влади, іншими державними органами, підприємствами, установами й організаціями, громадськими об'єднаннями та громадянами під час проведення заходів щодо забезпечення безпеки діяльності підприємства. Готує пропозиції та надає рекомендації із взаємостосунків партнерами підприємства щодо розроблення антикризових заходів і забезпечення безпеки. Бере участь в апробації заходів із фінансово-економічної безпеки підприємства шляхом розроблення моделі економічної безпеки підприємства

1	2
	Забезпечує підвищення кваліфікації працівників підпорядкованого структурного підрозділу в галузі фінансово-економічної безпеки
Аналітик з питань фінансово-економічної безпеки	Організовує аналітичні та методичні практики впровадження заходів із фінансово-економічної безпеки. Бере участь у розробленні, удосконаленні та реалізації теоретико-практичних методів забезпечення необхідною інформацією у сфері фінансово-економічної безпеки. Визначає перспективність та ефективність інноваційної діяльності з використанням інформаційних, облікових та аналітичних методів для удосконалення процесів фінансово-економічної безпеки в межах установлених стандартів і норм. Визначає індикатори економічної безпеки. Забезпечує підготовку документів, необхідних для прийняття управлінських рішень щодо діяльності підприємств в умовах реальних і потенційних загроз і небезпек, функціонування системи економічної безпеки, ефективної діяльності суб'єктів її забезпечення. Розроблює проекти наказів, положень, інструкцій щодо організації діяльності аналітиків з питань фінансово-економічної безпеки, їх взаємодії з іншими суб'єктами безпеки й інформаційно-аналітичного забезпечення функціонування системи економічної безпеки. Визначає й оцінює стан і рівень фінансово-економічної безпеки свого підприємства, партнерів (контрагентів) і конкурентів. Забезпечує визначення зовнішніх і внутрішніх ризиків і загроз у сфері фінансово-економічної безпеки підприємства. Забезпечує збереження та примноження матеріальної та фінансової бази підприємства, раціонального й ефективного використання його ресурсів, надання інформації, необхідної для прийняття управлінських рішень щодо доцільності діяльності підприємства з урахуванням виявлених загроз і небезпек, захист отриманої інформації, яка відноситься до комерційної таємниці підприємства, вивчає вплив внутрішніх і зовнішніх загроз на фінансовий результат підприємства. Сприяє здійсненню стратегічного управління підприємством і його фінансово-економічною безпекою. Здійснює всі види інформаційного, аналітичного й обліково-аналітичного забезпечення функціонування системи економічної безпеки підприємств. Бере участь у проведенні діагностики фінансово-господарського стану підприємства з метою попередження його банкрутства

Продовження табл. А.1

1	2
	Організовує проведення моніторингу оцінювання стану безпеки, надійності та рівня: економічного стану підприємства, потенційних партнерів підприємства, стратегії діяльності на ринку конкурентів, максимально повного інформаційного забезпечення функціонування системи економічної безпеки підприємства з метою мінімізації внутрішніх і зовнішніх загроз. Бере участь у розробленні заходів щодо мінімізації впливу загроз на діяльність підприємства, у розробленні стратегічної орієнтації підприємства з урахуванням вимог до забезпечення фінансово-економічної безпеки. Бере участь у плануванні із забезпечення фінансово-економічної безпеки, вдосконалення інформаційно-аналітичного процесу функціонування системи фінансово-економічної безпеки та плануванні окремих спеціальних заходів щодо оперативного реагування на загрози, ризики, небезпеки в діяльності підприємства. Розроблює аналітичні документи, за якими здійснюється оцінювання стану та надаються пропозиції щодо діяльності підприємства в умовах загроз і небезпек, рекомендації щодо їх зниження. Надає визначеним керівництвом підприємства особам аналітичну інформацію щодо фінансово-економічної безпеки на підприємстві. Бере участь у проведенні експертного оцінювання отриманої інформації, визначає рівень її достовірності. Надає пропозиції щодо здійснення заходів безпеки. Розроблює всі види аналітичних документів, які стосуються забезпечення фінансово-економічної безпеки на підприємстві. Бере участь у підвищенні кваліфікації працівників свого структурного підрозділу
Фахівець з фінансово-економічної безпеки	Бере участь у реалізації заходів із забезпечення фінансово-економічної безпеки підприємства, установи, організації. Застосовує техніку та технології із забезпечення фінансово-економічної безпеки. Здійснює підготовку документів, що стосуються організації діяльності підприємства, установи, організації. Розроблює проекти положень та інструкцій, що регламентують діяльність із забезпечення фінансово-економічної безпеки. Сприяє здійсненню інформаційно-аналітичного й обліково-аналітичного забезпечення щодо оцінювання рівня реальних і потенційних загроз фінансово-економічній безпеці підприємства, установи, організації

Закінчення табл. А.1

1	2
	Бере участь у розробленні планів (перспективних, квартальних, річних тощо) щодо забезпечення, вдосконалення системи фінансово-економічної безпеки та планів проведення окремих спеціальних заходів щодо оперативного реагування на загрози, ризики, небезпеки в діяльності підприємства, установи, організації. У межах своїх повноважень надає рекомендації щодо удосконалення діяльності структурного підрозділу фінансово-економічної безпеки підприємства, установи, організації та забезпечення виконання його основних функцій і завдань. Бере участь у створенні та використанні нових технологій щодо зниження загроз і ризиків діяльності підприємства, установи, організації, забезпечення їх фінансово-економічної безпеки. Сприяє наданню всім категоріям працівників підприємства, установи, організації інформації, яка стосується діяльності із забезпечення фінансово-економічної безпеки. Готує рекомендації та безпосередньо здійснює заходи щодо забезпечення компетентності працівників підприємства, установи, організації, їх морального та матеріального стимулювання. Бере участь у здійсненні загального контролю за діяльністю структурних підрозділів підприємства, установи, організації щодо забезпечення фінансово-економічної безпеки. Готує пропозиції та надає рекомендації стосовно взаємостосунків із партнерами підприємства, установи, організації щодо розроблення антикризових заходів і забезпечення безпеки. Бере участь в апробації заходів із фінансово-економічної безпеки підприємства, установи, організації шляхом розроблення моделі економічної безпеки підприємства, установи, організації

Додаток Б

Частина Б.1

Інформація про компанію "Soyuz"

Українсько-російсько-американська компанія "Soyuz" займається оптовою та роздрібною торгівлею комп'ютерною технікою, периферійних пристроїв і програмного забезпечення, комп'ютерним програмуванням, а також ремонтом і технічним обслуговуванням електронного обладнання й іншою діяльністю у сфері інформатизації та комп'ютерних систем. Управління компанією здійснюють: вищий орган управління – загальні збори учасників; виконавчий орган (одноособовий) – директор; контролюючий орган – ревізійна комісія. На рис. Б.1 наведений перелік повноважень органів управління компанії.

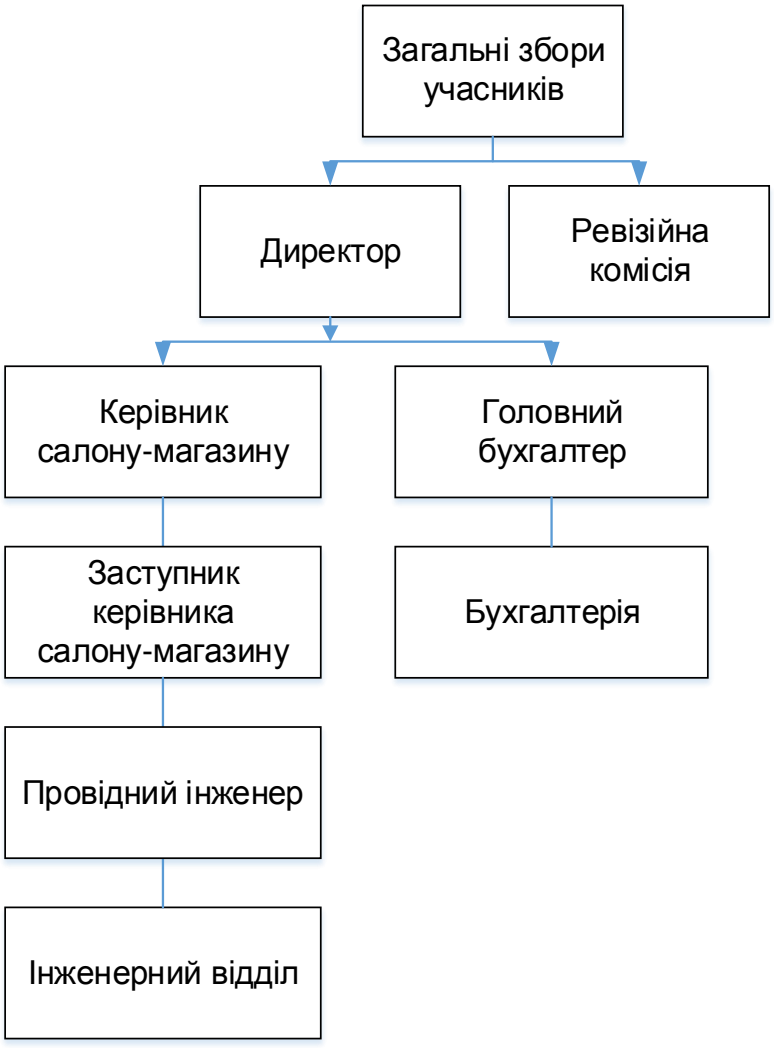

Рис. Б.1. **Організаційна структура управління компанії "Soyuz"**

Додаток В

Частина В.1

Розподіл повноважень органів управління компанії "Soyuz"

1. До виключної компетенції *ЗАГАЛЬНИХ ЗБОРІВ УЧАСНИКІВ* належить розгляд і прийняття рішень з таких питань;

а) визначення основних напрямів діяльності компанії, затвердження його планів та звітів про їх виконання;

б) внесення змін до Статуту Компанії;

в) виключення Учасника з Компанії;

г) обрання (призначення) та відкликання (звільнення) ДИРЕКТОРА Компанії та членів *РЕВІЗІЙНОЇ КОМІСІЇ,*

д) створення, реорганізація та ліквідація дочірніх підприємств, філій та представництв Компанії; затвердження їх статутів і положень про їх діяльність, внесення пропозицій щодо призначення та зміни керівників дочірніх підприємств, філій та представництв Компанії;

е) винесення рішень про притягнення до майнової відповідальності посадових осіб Компанії;

ж) визначення умов оплати праці *ДИРЕКТОРА* Компанії, керівників його дочірніх підприємств, філій та представництв;

з) прийняття рішень про зміну розміру Статутного капіталу Компанії;

и) установлення розміру, форми та порядку внесення учасниками додаткових внесків;

і) вирішення питання про придбання Компанією частки (вкладу) учасника;

ї) прийняття рішень про участь (засновника, учасника) Компанії в інших господарських товариствах, об'єднаннях, організаціях, структурах, установах і підприємствах;

к) прийняття рішень про припинення діяльності Компанії, призначення ліквідаційної комісії, затвердження ліквідаційного балансу.

2. *ДИРЕКТОР* Товариства:

а) вирішує всі питання діяльності Компанії, за винятком тих, які належать до виняткової компетенції *ЗАГАЛЬНИХ ЗБОРІВ УЧАСНИКІВ*;

б) організує виконання рішень ЗАГАЛЬНИХ ЗБОРІВ УЧАСНИКІВ;

в) представляє інтереси Компанії у відносинах з усіма підприємствами, організаціями, громадянами та державними органами;

г) у межах своєї компетенції розпоряджається майном і грошовими коштами Компанії, укладає угоди, контракти, видає довіреності з правом подальшої передовіри тощо.;

д) одноособово підписує зовнішньоекономічний договір (контракт) і має право уповноважувати на це інших осіб;

е) приймає на роботу та звільняє працівників Компанії;

ж) відкриває у банках поточний та інші рахунки Компанії, має право першого підпису розрахункових документів;

з) видає векселі, пред'являє векселі до оплати та виконує інші дії, пов'язані з обігом векселів;

и) формує колектив працівників Компанії (в т.ч. наймає заступників ДИРЕКТОРА за напрямами) та притягає їх до дисциплінарної та майнової відповідальності, організує їх працю;

к) дозволяє співробітникам відрядження у межах України та за кордон;

л) у межах своєї компетенції видає накази та дає вказівки, які є обов'язковими для працівників, затверджує посадові обов'язки працівників Компанії;

м) визначає склад і межі відомостей, що становлять комерційну таємницю Компанії, визначає порядок її захисту;

н) списує з балансу підприємства недостачі та втрати товарно-матеріальних цінностей, морально застарілого, зношеного та непридатного для подальшого використання устаткування, а також витрати на припинені та нездійснені робот, якщо інший порядок не передбачений чинним законодавством.

3. Перевірки діяльності *ДИРЕКТОРА* проводяться *РЕВІЗІЙНОЮ КОМІСІЄЮ* за дорученням *ЗАГАЛЬНИХ ЗБОРІВ УЧАСНИКІВ* з власної ініціативи або на вимогу учасника Компанії. *РЕВІЗІЙНІЙ КОМІСІЇ* повинні бути надані всі матеріали, бухгалтерські або інші документи й особисті пояснення службових осіб на її вимогу.

Додаток Г

ІНФОРМАЦІЯ ПРО СУБ'ЄКТА ОХОРОННОЇ ДІЯЛЬНОСТІ ТОВ "БАРС"

Частина Г.1

Інформація щодо відповідного обладнання та матеріально-технічної бази

Вих. № 57 від 22/12/2014 р.

ТОВ "Барс", засноване в 2003 р., зарекомендувало себе як підприємство з високим рівнем обслуговування своїх контрагентів. За для цього товариство має необхідну матеріально-технічну базу, центр обслуговування на території України: офіс з обслуговуючим персоналом, автомобілі, укомплектовані сучасними засобами зв'язку.

Групи реагування здійснюють цілодобове патрулювання об'єктів на автомобілях (у кількості двох машин: ВАЗ 21070, реєстраційний номер АХ 9999 АН; ВАЗ 21070, реєстраційний номер АХ 2785 АІ, які знаходяться у власності ТОВ "Барс"). Охоронники мають необхідну кваліфікацію, відповідний фізичний стан і забезпечені засобами активної оборони.

Копії технічних паспортів автомобілів надаються у складі пропозиції. Усі співробітники ТОВ "Барс" пройшли необхідну підготовку та медичний огляд.

Директор ТОВ "Барс" /підпис/

Продовження додатка Г

Частина Г.2

Довідка про досвід ТОВ "Барс" з виконання аналогічних договорів

Вих. № 52 від 19/12/2014 р.

ТОВ "Барс" вже багато років працює у сфері охоронних послуг, протягом останніх чотирьох років, з 2011 до 2014 рр., підприємство співпрацювало з такими контрагентами.

Номер і дата укладення договору	Предмет договору	Назви замовників	Адреси замовників	П. І. Б., номера телефонів контактних осіб
№ 269 від 01.04.2011 р.	Послуги, пов'язані з особистою безпекою (послуги фізичної охорони)	Товариство з обмеженою відповідальністю "ЕМІЛЬ"	м. Харків, вул. Серпова, ХХ	Людмила Іванівна Попова Тел.: (057)700-00-00
№ 223 від 01.02.2011 р.	Послуги охоронників	Товариство з обмеженою відповідальністю спеціалізована науково-виробнича фірма "Парус"	м. Харків, вул. Сумська, ХХ	Боровий Олег Іванович Тел.: (057)715-00-00

Директор ТОВ "Барс" /підпис/

Частина Г.3

Відгук
про надання охоронних послуг

ТОВ "Барс" згідно угод у період з 2011 р. до теперішнього часу здійснює охорону (послуги охоронників; послуги, пов'язані з особистою безпекою) об'єкта ТОВ СНВФ "Парус".

Охоронники мають відповідний фізичний стан і несуть службу у форменому одязі. ТОВ СНВФ "Парус" не має зауважень до ТОВ "Барс" стосовно виконання обумовлених з ним завдань. Усі умови з охорони майна на об'єкті виконуються у повному обсязі й якісно.

Генеральний директор /підпис/

Продовження додатка Г

Таблиця Г.1

Інформація щодо співробітників ТОВ "Барс"
для надання послуг, пов'язаних з особистою безпекою

№ п\п	П. І. Б.	Посади	Досвід роботи на посаді	Освіта	Диплом, сертифікати посвідчення тощо
1	Король Ігор Анатолійович	директор	7 років	вища	у наявності
2	Поліщук Галина Миколаївна	головний бухгалтер	1 рік	вища	у наявності
3	Журавська Ольга Віталіївна	інспектор з кадрів	6 років	вища	у наявності
4	Усата Тетяна Юріївна	оператор пульту керування	5 місяць	вища	у наявності
5	Білобородов Сергій Леонідович	водій АТЗ	2 роки	середня	у наявності
6	Віслогузов Андрій Володимирович	водій АТЗ	5 місяць	середня	у наявності
7	Баранов Анатолій Анатолійович	водій АТЗ	1 рік	професійно-технічна	у наявності
8	Карлов Микола Васильович	водій АТЗ	6 місяць	професійно-технічна	у наявності
9	Багач Тетяна Олександрівна	охоронник	3 роки	професійно-технічна	у наявності
10	Балюк Тетяна Михайлівна	охоронник	3 роки	базова вища	у наявності
11	Білокінь Віталій Петрович	охоронник	4 роки	професійно-технічна	у наявності
12	Болдижева Ірина Федорівна	охоронник	2 роки	середня	у наявності
13	Гапонов Володимир Сергійович	охоронник	5 років	вища	у наявності
14	Гладка Тетяна Василівна	охоронник	3 роки	середня	у наявності
15	Головань Володимир Якович	охоронник	2 роки	середня	у наявності
16	Кнюпа Ігор Борисович	охоронник	3 роки	базова вища	у наявності
17	Котляров Олександр Сергійович	охоронник	1 рік	середня	у наявності

Директор ТОВ "Барс" /підпис/

Продовження додатка Г

Таблиця Г.2

Фінансовий звіт
суб'єкта малого підприємництва
ТОВ "Барс"

1. Баланс на 30 вересня 2014 р. Форма 1-м

Активи	Код рядка	На початок звітного року, тис. грн	На кінець звітного року, тис. грн
1	2	3	4
1. Необоротні активи			
Незавершені капітальні інвестиції	1005	-	-
Основні засоби:	1010	1,0	1,0
первісна вартість	1011	8,7	8,7
знос	1012	(7,7)	(7,7)
Довгострокові біологічні активи:	1020		
довгострокові фінансові інвестиції	1030	56,5	56,5
інші необоротні активи	1090	-	-
Усього за розділом 1	1095	73,9	73,9
II. Оборотні активи			
Запаси:	1100	2,3	4,3
у тому числі готова продукція	1103		-
Поточні біологічні активи	1110	-	-
Дебіторська заборгованість за товари, роботи, послуги:	1125	55,2	54,9
дебіторська заборгованість за розрахунками з бюджетом	1135	2,5	3,6
у тому числі з податку на прибуток	1136	0,1	0,1
інша поточна дебіторська заборгованість	1155	769,9	711,5
Поточні фінансові інвестиції	1160	-	-
Гроші й їх еквіваленти	1165	8,7	10,9
Витрати майбутніх періодів	1170	-	-
Інші оборотні активи	1190	0,5	0,5
Усього за розділом II	1195	839,2	785,8
III. Необоротні активи, утримувані для продажу, та групи вибуття	1200	-	-
Баланс	1300	931,1	857,7

Продовження табл. Г.2

Пасив	Код рядка	На початок звітного року, тис. грн	На кінець звітного року, тис. грн
1	2	3	4
1. Власний капітал			
Зареєстрований (пайовий) капітал	1400	18,5	18,5
Додатковий капітал	1410	-	-
Резервний капітал	1415	-	-
Нерозподілений прибуток (непокритий збиток)	1420	794,3	704,3
Неоплачений капітал	1425		
Усього за розділом 1	1495	812,8	722,8
II. Довгострокові зобов'язання, цільове фінансування та забезпечення	1595		
III. Поточні зобов'язання			
Короткострокові кредити банків	1600		
Поточна кредиторська заборгованість за: довгостроковими зобов'язаннями	1610		
товари, роботи, послуги	1615		
розрахунками з бюджетом	1620	4,8	6,0
у тому числі з податку на прибуток	1621		
розрахунками зі страхування	1625	4,9	8,8
розрахунками з оплати праці	1630	12,4	15,0
Доходи майбутніх періодів	1665		
Інші поточні зобов'язання	1690	61,6	90,8
Усього за розділом III	1695	83,7	120,5
IV. Зобов'язання, пов'язані з необоротними активами, утримуваними для продажу, та групами вибуття	1700		
Баланс	1900	896,5	843,3

Закінчення табл. Г.2

2. Звіт про фінансові результати Форма 2-м

Стаття	Код рядка	За звітний період, тис. грн	За аналогічний період попереднього року, тис. грн
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2000	302,7	300,5
Інші операційні доходи	2120		
Інші доходи	2240		
Разом доходи (2000 + 2120 + 2240)	2280	302,7	300,5
Собівартість реалізованої продукції (товарів, робіт, послуг)	2050	(245,3)	(213,3)
Інші операційні витрати	2180	(147,4)	(239,9)
Інші витрати	2270		
Разом витрати (2050 + 2180 + 2270)	2285	(392,7)	(453,2)
Фінансовий результат до оподаткування (2280 - 2285)	2290	-90,0	-152,7
Податок на прибуток	2300		
Чистий прибуток (збиток)	2350	-90,0	-152,7

Керівник / підпис /
Головний бухгалтер / підпис /

Продовження додатка Г

Таблиця Г.3

Спрощений фінансовий звіт
суб'єкта малого підприємництва
ТОВ "Барс"

1. Баланс на 31 грудня 2013 р. Форма 1-мс

Актив	Код рядка	На початок звітного року, тис. грн	На кінець звітного року, тис. грн
1	2	3	4
I. Необоротні активи			
Основні засоби:			
залишкова вартість	030	1,0	1,0
первісна вартість	031	8,7	8,7
знос	032	(7,7)	(7,7)
Інші необоротні активи	070	56,5	56,5
Усього за розділом 1	080	57,5	57,5
II. Оборотні активи			
Запаси	100	1,2	2.3
Поточна дебіторська заборгованість	210	1036,7	827,4
Грошові кошти та їх еквіваленти:			
в національній валюті	230	60,3	8,7
у тому числі в касі	231	-	-
в іноземній валюті	240	-	-
Інші оборотні активи	250	0,5	0,5
Усього за розділом II	260	1098,7	839,0
Баланс	280	1156,2	896,5
Пасив	Код рядка	На початок звітного року, тис. грн	На кінець звітного періоду, тис. грн
I. Власний капітал			
Капітал	300	18,5	18,5
Нерозподілений прибуток (непокритий збиток)	350	964,8	794,3
Усього за розділом 1	380	983,3	812,8
II. Цільове фінансування	430	-	-
III. Довгострокові зобов'язання	480	-	-

Закінчення табл. Г.3

1	2	3	4
IV. Поточні зобов'язання			
Короткострокові кредити банків	500	-	-
Кредиторська заборгованість за товари, роботи, послуги	530	-	-
Поточні зобов'язання за розрахунками:			
з бюджетом	550	6,2	4,8
зі страхування	570	5,6	4,9
з оплати праці*	580	10,3	12,4
Інші поточні зобов'язання	610	150,8	61,6
Усього за розділом IV	620	172,9	83,7
Баланс	640	1156,2	896,5

2. Звіт про фінансові результати

Форма 2-мс

Статті	Код рядка	За звітний період, тис. грн	За аналогічний період попереднього року, тис. грн
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2000	401,4	443,4
Інші доходи	2160		
Разом доходи (2000 + 2240)	2280	401,4	443,4
Собівартість реалізованої продукції (товарів, робіт, послуг)	2050	(287,0)	(342,6)
Інші витрати	2165	(284,9)	(436,2)
Разом витрати (2050 + 2165)	2285	(571,9)	(778,8)
Фінансовий результат до оподаткування (2280 – 2285)	2290	-170,5	-335,.4
Податок на прибуток	2300	( )	( )
Витрати (доходи), які зменшують (збільшують) фінансовий результат після оподаткування	2310		
Чистий прибуток (збиток) (2290 – 2300 – (+) 2310)	2350	-170,5	-335,4

Керівник / підпис /
Головний бухгалтер / підпис /

Частина Г.4

Вих. 40 від 22/12/2014 р.

ФОРМА "ПРОПОЗИЦІЯ"

Товариство з обмеженою відповідальністю "Барс"

Уважно вивчивши комплект документації конкурсних торгів, цим надаємо свою пропозицію конкурсних торгів щодо участі у відкритих торгах на закупівлю послуг, пов'язаних з особистою безпекою (послуги охоронників):

1. Повне найменування учасника:

Товариство з обмеженою відповідальністю "Барс".

2. Місцезнаходження учасника: 61166, Харківська область, м. Харків, Київський р-н, вул. Сумська, буд. ХХ

3. Загальна вартість (ціна) пропозиції конкурсних торгів, що зазначена цифрами та літерами:

1 441 020,00 грн (один мільйон чотириста сорок одна тисяча двадцять грн 00 коп) (з урахуванням ПДВ, якщо ПДВ передбачено). ПДВ не передбачено (без ПДВ) грн.

4. Телефон, факс: (057)705-00-00; факс (057)705-00-00.

5. Код за ЄДРПОУ/реєстраційний номер облікової картки платника податків: ХХХХХХХХ.

6. Правовий статус; організаційно-правова форма учасника-юридичної особи: юридична особа; товариство з обмеженою відповідальністю.

7. Банківські реквізити: Р/р ХХХХХХХХХХХХ у ПАТ "БАНК "ГІГАНТ" м. Харкова МФО № ХХХХХХ.

8. Індивідуальний податковий номер – для учасника, який є платником податку на додану вартість: *-//-*.

9. Відомості про керівника учасника-юридичної особи:

(П.І.Б., посада, контактний телефон): Король Ігор Анатолійович, директор, тел.: (057)705-00-00.

10. П.І.Б., зразок підпису, для юридичної особи – посада особи (осіб), уповноваженої (уповноважених) підписувати пропозицію конкурсних торгів від імені учасника: Король Ігор Анатолійович – директор.

11. П.І.Б., зразок підпису, для юридичної особи – посада особи (осіб), уповноваженої (уповноважених) підписувати договір про закупівлю за результатами процедури закупівлі.

Директор ТОВ "Барс" /підпис/

Додаток Д

ІНФОРМАЦІЯ ПРО СУБ'ЄКТА ОХОРОННОЇ ДІЯЛЬНОСТІ ТОВ "ЛЕО"

Частина Д.1

ТОВ "Лео"
61000, м. Харків, пул. Сумська, ХХ, кв. Х, тел.: 707 00 00
Р/р ХХХХХХХХХХХХ у ПАТ "БАНК " АВЕРС " м. Харкова МФО № ХХХХХХ, код ЄДРПОУ ХХХХХХХХ

Довідка, складена в довільній формі, що містить інформацію про наявність у ТОВ "Лео" відповідного обладнання та матеріально-технічної бази, необхідних для надання послуг, що є предметом закупівлі

Товариство з обмеженою відповідальністю "Лео" для надання послуг, пов'язаних з особистою безпекою (послуги охоронників) має в розпорядженні: достатню кількість охоронників, пульт централізованого спостереження, групи реагування, а саме: у власності ТОВ "Лео" знаходяться транспортні засобі (у кількості двох одиниць), уніформа охоронників, засоби активної оборони, засоби індивідуального захисту – шоломи, бронежилети. Є в наявності ПЦС, розташований в орендованому офісному приміщенні (центр обслуговування з працюючим персоналом, який спостерігає за станом систем передавання тривожних сповіщень). За необхідності, з метою посилення охорони об'єктів на допомогу охороннику висилається група реагування. Також здійснюється постійний цілодобовий контроль за несенням служби всіма постами охорони. На кожному об'єкті охороннику видаються спецзасоби (засоби спорядження охоронників – такі, як: газові балончики "Терен", бронежилети). Усі співробітники мають мобільні засоби зв'язку. Співробітники одягнені у чорну форму, відповідно: влітку – сорочка та чорна бейсболка, взимку – чорна куртка, шапка та берці. ТОВ "Лео" має у розпорядженні групи реагування на двох автомобілях з засобами зв'язку, які здійснюють цілодобове патрулювання об'єктів, контроль за несенням служби охоронниками та виїзд на сигнали "Тривога" з ПЦС, а також доставку представників підприємства у нічний час для з'ясування причин спрацювання засобів сигналізації. Це дозволяє забезпечити цілодобове реагування на будь-які події в термін від 5 хвилин (у нічний час) до 10 хвилин (денний час).

Датовано 19/12/2014 р.

Директор ТОВ "Лео" /підпис/

Продовження додатка Д

Частина Д.2

ТОВ "Лео"
61000, м. Харків, пул. Сумська, ХХ, кв. Х, тел.: 707 00 00
Р/р ХХХХХХХХХХХХ у ПАТ "БАНК " АВЕРС " м. Харкова МФО № ХХХХХХ, код ЄДРПОУ ХХХХХХХХ

Інформація в довільній формі, складена в табличному вигляді, про досвід виконання аналогічних договорів із зазначенням номеру та дати укладення договору, предмету договору; назви, адреси замовників і П. І. Б., номеру телефону контактних осіб замовників, яким здійснювалось надання послуг.

№ п/п	Назва замовника	Номер та дата \укладення договору; предмет договору	Адреса замовника	П. І. Б., номер телефону контактних осіб
1	Науково-виробниче об'єднання "Гідротехпроект"	№ 200-04/11 від 01.04.2011 р.; охоронні послуги (послуги, пов'язані з особистою безпекою; послуги охоронників)	61ХХХ, Україна, м. Харків, вул. Кірова, ХХ	Генеральний директор Кравець С. В., 057- ХХХ-ХХ-ХХ
2	Товариство з обмеженою відповідальністю "Міжвідомчий центр інженерних досліджень"	№ 299 від 01.03.2012 р.; охоронні послуги (послуги, пов'язані з особистою безпекою; послуги охоронників)	62ХХХ, Україна, Харківська обл. Харківський р-н, м. Балаклея, вул. Горького, ХХХ	Заступник генерального директора Осадчий С. Д., 057-ХХ-ХХ-ХХХ

Датовано 12/12/2014 р.

Директор ТОВ "Лео" /підпис/

Частина Д.3

Відгук
про надання охоронних послуг
(послуги, пов'язані з особистою безпекою)
ТОВ "Лео"

Товариство з обмеженою відповідальністю "Лео" надає охоронні послуги ТОВ "Гідротехпроект" з 2011 року та до теперішнього часу. Охоронний персонал ТОВ "Лео" завжди у форменому одязі, несуть службу згідно з дислокаціями. Охорона виконує свої обов'язки задовільно та в повному обсязі. Охоронники мають досвід служби, відповідну фахову підготовку. Порушень договірних обов'язків з боку ТОВ "Лео" за цей період не було.

Директор НВО "Гідротехпроект" /підпис/

Продовження додатка Д

Частина Д.4

ТОВ "Лео"
61000, м. Харків, пул. Сумська, ХХ, кв. Х, тел.: 707 00 00
Р/р ХХХХХХХХХХХХ у ПАТ "БАНК " АВЕРС " м. Харкова МФО № ХХХХХХ, код ЄДРПОУ ХХХХХХХХ

Довідка, складена в довільній формі в табличному вигляді, що містить інформацію про наявність у учасника кількості працівників, достатньої для надання послуг, що є предметом закупівлі, відповідної кваліфікації, необхідних знань і досвіду; із зазначенням кількості співробітників, П.І.Б., їх посад, досвіду роботи на цих посадах, рівня освіти; наявності дипломів, посвідчень, сертифікатів, медичних довідок про проходження обов'язкових попереднього та періодичного психіатричних оглядів та сертифікати про проходження профілактичного наркологічного огляду (які є дійсними на дату розкриття пропозицій конкурсних торгів).

№ п/п	П. І. Б.	Посада	Рівень освіти	Стаж роботи: працює на посаді з:			Наявність дипломів, посвідчень, сертифікаті в тощо	Свідоцтво про підвищення кваліфікації (охоронник 1 розряду, охоронник 3 розряду)	Наявність медичних довідок
1	Бабаєва Ганна Сергіївна	головний бухгалтер	вища	01	07	2010	у наявності	немає	у наявності
2	Білоус Віталій Миколайович	охоронник	вища	01	03	2013	у наявності	ТА 43893000	у наявності
3	Вашатко Галина Віталіївна	інспектор з кадрів	вища	01	11	2012	у наявності	немає	у наявності
4	Глушко Сергій Миколайович	охоронник	повна середня	02	04	2013	у наявності	ТА 47158000	у наявності
5	Греков Віктор Володимирович	охоронник	повна середня	15	04	2014	у наявності	ТА 44060000	у наявності
6	Губін Микола Володимирович	охоронник	повна середня	01	09	2014	у наявності	ТА 47678000	у наявності
7	Гуляєв Олександр Іванович	охоронник	повна середня	14	09	2012	у наявності	ТА 44060000	у наявності
8	Зозуля Олександр Сергійович	охоронник	повна середня	01	09	2014	у наявності	ТА 47678000	у наявності
9	Коляда Олександр Миколайович	охоронник	повна середня	16	05	2014	у наявності	ТА 45851000	у наявності
10	Копил Олександр Володимирович	охоронник	повна середня	18	03	2013	у наявності	ТА 44380000	у наявності

Директор ТОВ "Лео" /підпис/

Таблиця Д.1

Штатний розклад
ТОВ "Лео"
на 2014 рік

№ п/п	Посада	Код професії	Кількість штатних одиниць	Посадовий оклад, грн	Фонд оплати праці, грн
1	Директор	1210.1	1	1 545,0	1 545,0
2	Заступник директора	1210.1	0,1	1 495,0	149,5
3	Головний бухгалтер	1231	0,1	1 445,0	144,5
4	Інспектор з кадрів	3423	0,1	1 355,0	135,5
5	Інженер	2149.2	1	1 350,0	1 350,0
6	Оператор пульту управління	8112	4	1 335,0	5 340,0
7	Електромонтер охоронно-пожежної сигналізації	7244.2	1	1 330,0	1 330,0
8	Охоронник	5169	35	1 320,0	46 200,0
9	Водій автотранспортних засобів	8322	4	1 325,0	5 300,0
	Всього	46,3			61 494,5

Директор ТОВ "Лео" /підпис/

Продовження додатка Д

Таблиця Д.2

ФІНАНСОВИЙ ЗВІТ
суб'єкта малого підприємництва
ТОВ "Лео"

Баланс на 30 вересня 2014 р. Форма 1-м

Активи	Код рядка	На початок звітного року, тис. грн	На кінець звітного року, тис. грн
1	2	3	4
1. Необоротні активи			
Незавершені капітальні інвестиції	1005	13,2	16,9
Основні засоби:	1010	0,7	3,9
первісна вартість	1011	99,9	103,8
знос	1012	(99,2)	(99,9)
Довгострокові біологічні активи:	1020	–	–
Довгострокові фінансові інвестиції	1030	–	–
Інші необоротні активи	1090	–	–
Усього за розділом 1	1095	13,9	20,8
2. Оборотні активи			
Запаси:	1100	47,7	78,2
у тому числі готова продукція	1103	–	–
Поточні біологічні активи	1110	–	–
Дебіторська заборгованість за товари, роботи, послуги:	1125	34,6	68,6
Дебіторська заборгованість за розрахунками з бюджетом	1135	2,0	2,3
у тому числі з податку на прибуток	1136	–	–
Інша поточна дебіторська заборгованість	1155	216,2	360,2
Поточні фінансові інвестиції	1160	–	–
Гроші й їх еквіваленти	1165	38,6	156,3
Витрати майбутніх періодів	1170	–	–
Інші оборотні активи	1190	2,5	–
Усього за розділом II	1195	341,6	665,5

Продовження табл. Д.2

1	2	3	4
3. Необоротні активи, утримувані для продажу, та групи вибуття	1200	–	–
Баланс	1300	355,6	686,4
Пасив	Код рядка	На початок звітного року, тис. грн	На кінець звітного року, тис. грн
1. Власний капітал			
Зареєстрований (пайовий) капітал	1400	52,5	52,5
Додатковий капітал	1410	–	–
Резервний капітал	1415	-	-
Нерозподілений прибуток (непокритий збиток)	1420	135,3	345,8
Неоплачений капітал	1425		
Усього за розділом 1	1495	187,8	398,3
II. Довгострокові зобов'язання, цільова фінансування та забезпечення	1595	–	–
III. Поточні зобов'язання			
Короткострокові кредити банків	1600	--	--
Поточна кредиторська заборгованість за: довгостроковими зобов'язаннями	1610	–	–
товари, роботи, послуги	1615		
розрахунками з бюджетом	1620	28,9	33,4
у тому числі з податку на прибуток	1621		
розрахунками зі страхування	1625	5,4	12,4
розрахунками з оплати праці	1630	14,2	22,8
Доходи майбутніх періодів	1665		
Інші поточні зобов'язання	1690	119,3	219,5
Усього за розділом III	1695	167,8	288,1
IV. Зобов'язання, пов'язані з необоротними активами, утримуваними для продажу, та групами вибуття	1700		
Баланс	1900	355,6	686,4

Закінчення табл. Д.2

2. Звіт про фінансові результати
за 9 місяців 2014 р.

Форма 2-м

Статті	Код рядка	За звітний період, тис. грн	За аналогічний період попереднього року, тис грн
1	2	3	4
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2000	1 854,5	1 490,1
Інші операційні доходи	2120	1,3	11,6
Інші доходи	2240		
Разом доходи (2060 + 2120 + 2240)	2280	1 855,8	1 501,7
Собівартість реалізованої продукції (товарів, робіт, послуг)	2050	(266,8)	(243,1)
Інші операційні витрати	2180	(1 378,5)	(1 267,5)
Інші витрати	2270		
Разом витрати (2050 + 2180 + 2270)	2285	(1 645,3)	(1 510,6)
Фінансовий результат до оподаткування (2280 - 2285)	2290	210,5	-8,9
Податок на прибуток	2300		
Чистий прибуток (збиток) (2290 - 3300)	2350	210,5	-8,9

Керівник /підпис/
Головний бухгалтер /підпис/

Продовження додатка Д

Таблиця Д.3

СПРОЩЕНИЙ ФІНАНСОВИЙ ЗВІТ
суб'єкта малого підприємництва
ТОВ "Лео"

1. Баланс на 31 грудня 2013 р. Форма 1-мс

Актив	Код рядка	На початок звітного року, тис. грн	На кінець звітного періоду, тис. грн
1	2	3	4
I. Необоротні активи			
Основні засоби:			
залишкова вартість	030	24,0	13,9
первісна вартість	031	103,4	113,1
знос	032	(79,4)	
Інші необоротні активи	070		
Усього за розділом I	080	24,0	13,9
II. Оборотні активи			
Запаси	100	18,0	47
Поточна дебіторська заборгованість	210	70,9	252,9
Грошові кошти й їх еквіваленти:			
в національній валюті	230	121,6	38,6
у тому числі в касі	231		
в іноземній валюті	240		
Інші оборотні активи	250	0,7	2,0
Усього за розділом II	260	211,2	340,5
Баланс	280	235,2	355,6
Пасив	Код рядка	На початок звітного року, тис. грн	На кінець звітного періоду, тис. грн
1. Власний капітал			
Капітал	300	52,5	52,5
Нерозподілений прибуток (непокритий збиток)	350	48,7	135,3
Усього за розділом 1	380	101,2	187,8

Закінчення табл. Д.3

1	2	3	4
II. Цільове фінансування	430		
III. Довгострокові зобов'язання	480		
IV Поточні зобов'язання			
Короткострокові кредити банків	500		
Кредиторська заборгованість за товари, роботи, послуги	530		
Поточні зобов'язання за розрахунками:			
з бюджетом	550	23,4	28,9
зі страхування	570	4,9	5,4
з оплати праці*	580	14,7	14,2
Інші поточні зобов'язання	610	91,0	119,3
Усього за розділом IV	620	134.0	167.8
Баланс	640	235.2	355.6

2. Звіт про фінансові результати

Форма 2-мс

Статті	Код рядка	За звітний період,, тис. грн	За попередній період, тис. грн
1	2	3	4
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	030	2 059,9	1 303,0
Інші доходи	040	11,6	18,1
Разом доходи (030 + 040)	070	2 071,5	1 321,1
Собівартість реалізованої продукції (товарів, робіт, послуг)	080	(683,9)	(247,9)
Інші витрати	100	(1 301,0)	(1 041,8)
Разом витрати (080 + 100)	120	(1 984,9)	(1 289,7)
Фінансовий результат до оподаткування (070 – 120)	130	86,6	31,4
Податок на прибуток	140		
Витрати (доходи), які зменшують (збільшують) фінансовий результат після оподаткування	145		
Чистий прибуток (збиток) (130 – 140 – (+) 145)	150	86,6	31,4

Керівник /підпис/

Головний бухгалтер /підпис/

Частина Д.5

ФОРМА "ПРОПОЗИЦІЯ"

ТОВ "Лео"

Уважно вивчивши комплект документації конкурсних торгів, цим надаємо свою пропозицію конкурсних торгів щодо участі у відкритих торгах на закупівлю послуг, пов'язаних з особистою безпекою (послуги охоронників):

1. Повне найменування учасника: Товариство з обмеженою відповідальністю "Лео".

2. Місцезнаходження учасника: 61022, Харківська обл., м. Харків, Шевченківський район, вулиця Сумська, буд. ХХ, квартира 5.

3. Загальна вартість (ціна) пропозиції конкурсних торгів, що зазначена цифрами та літерами: 1 349 040,00 грн. (один мільйон триста сорок дев'ять тисяч сорок грн, 00 коп.), без ПВД, ПДВ не передбачено.

4. Телефон, факс: 057-707-46-49, 057-707-46-49.

5. Код за ЄДРПОУ/реєстраційний номер облікової картки платника податків: 30000006.

6. Правовий статус; організаційно-правова форма учасника юридичної особи: юридична особа, товариство з обмеженою відповідальністю.

Банківські реквізити: Р/р 260000000077 у ПАТ "БАНК " АВЕРС " м. Харкова МФО № 8350000, код ЄДРПОУ 35982856.

7. Індивідуальний податковий номер – для учасника, який є платником податку на додану вартість: не платник ПДВ, платник єдиного податку.

8. Відомості про керівника учасника-юридичної особи:

(П.І.Б., посада, контактний телефон):

Кухар Михайло Михайлович,

директор, 057-707-46-49

9. П.І.Б., зразок підпису, для юридичної особи – посада особи (осіб), уповноваженої (уповноважених) підписувати пропозицію конкурсних торгів від імені учасника:

Кухар Михайло Михайлович – директор.

Директор /підпис/

НАВЧАЛЬНЕ ВИДАННЯ

Отенко Ірина Павлівна
Москаленко Наталя Олександрівна

ОРГАНІЗАЦІЯ ТА УПРАВЛІННЯ СИСТЕМОЮ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ

Навчальний посібник

Відповідальний за видання *І. П. Отенко*

Відповідальний редактор *М. М. Оленич*

Редактор *Н. І. Ганцевич*

Коректор *Н. І. Ганцевич*

План 2016 р. Поз. № 4-НП.
Підп. до друку 08.12.2016 р. Формат 60×90 1/16. Папір офсетний. Друк цифровий.
Ум. друк. арк. 14,0. Обл.-вид. арк. 17,5. Тираж 400 пр. Зам. № 286.

Видавець і виготовлювач – ХНЕУ ім. С. Кузнеця, 61166, м. Харків, просп. Науки, 9-А

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру
ДК № 4853 від 20.02.2015 р.