МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МІСЬКОГО ГОСПОДАРСТВА імені О. М. БЕКЕТОВА

О. Ю. ЛИТОВЧЕНКО

КОНСПЕКТ ЛЕКЦІЙ
з дисципліни

«КОМПЛЕКСНЕ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ»

(для студентів денної і заочної форм навчання
освітнього рівня магістр
спеціальності 073 – Менеджмент)

Харків
ХНУМГ ім. О. М. Бекетова
2018

Литовченко О. Ю. Конспект лекцій з дисципліни «Комплексне забезпечення фінансово-економічної безпеки» (для студентів денної і заочної форм навчання освітнього рівня магістр спеціальності 073 – Менеджмент) / О. Ю. Литовченко ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2018. – 197 с.

Автор канд. екон. наук., доц. О. Ю. Литовченко

Рецензент д-р екон. наук, проф. Т. В. Момот

Рекомендовано кафедрою фінансово-економічної безпеки, обліку і аудиту, протокол № 10 від 03.04.2017.

ЗМІСТ

ВСТУП

Однією з найважливіших складових успіху економічної діяльності підприємств є стан їх фінансів, який значною мірою визначає конкурентні позиції підприємства, їх платоспроможність, відносини з партнерами, перспективи розвитку та здатність до подальшого успішного розвитку в цілому. Натомість, теперішній стан фінансів більшості вітчизняних підприємств є незадовільним. Багато керівників пояснюють таку ситуацію зовнішніми причинами: неплатоспроможністю партнерів, відсутністю необхідного попиту, недосконалістю законодавства, відсутністю інвесторів, а також застарілою матеріальною базою виробництва. До цього додаються численні економічні ризики господарської діяльності, що супроводжують ринкові відносини, у складі яких найбільш вразливими є фінансові ризики. Саме недостатня увага до них може призвести підприємства, навіть при високій прибутковості, до припинення його існування.

Забезпечення стабільності результатів діяльності підприємства, досягнення цілей, відповідних інтересам власників і суспільства, неможливі без підвищення їхньої уваги до питань забезпечення фінансово-економічної безпеки.

Проблеми забезпечення фінансово-економічної безпеки охоплюють аспекти управління фінансовими ресурсами, грошовими потоками компанії, фінансовою стійкістю та прибутковістю, шляхи зниження ризиків небажаних подій відносно фінансово-економічної сфери діяльності підприємства. Означене є одним з ключових елементів системи сучасного управління підприємством взагалі, та має особливе, пріоритетне значення для сьогоднішніх умов розвитку економіки.

Тому вкрай важливо, щоб майбутні фахівці з менеджменту оволоділи теорію комплексного забезпечення фінансово-економічної безпеки, а також вміли втілювати на практиці отримані теоретичні знання.

МОДУЛЬ 1 ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ, БАНКІВ ТА ФІНАНСОВИХ УСТАНОВ

ЗМ 1 Організація та управління системою фінансово-економічної безпеки

Тема 1 Теоретичні засади управління фінансово-економічною безпекою підприємства

План лекції

1.1 Сутність безпеки, її види та характерні ознаки

1.2 Сутність економічної безпеки та її рівні

1.3 Складові елементи економічної безпеки підприємства

1.4 Характеристика фінансово-економічної безпеки

1.1 Сутність безпеки, її види та ознаки

На сьогоднішній день слово «безпека» належить до понять часто вживаних і з плином часу воно використовується все частіше. Від безпеки характеру глобального, регіонального та локального, – до безпеки дорожнього руху, безпеки праці, тощо. Відсутність безпеки або процес зниження ступеня безпеки трактують як загрозу, явище та загрозливий процес для існування життя і його перспектив.

Безпека – це певний об’єктивний стан, заснований на відсутності загрози, відчутний суб’єктивно через одиниці чи угрупування. Під безпекою розуміють також стан без загрози, стан спокою, впевненості.

У широкому науковому сенсі під безпекою розуміється захищеність природно-фізіологічних, соціально-економічних, ідеально-духовних і ситуативних потреб у ресурсах, технологіях, інформації і моральних ідеалах, необхідних для життєдіяльності і розвитку населення.

Базовими ознаками, які відображені у визначенні поняття «безпека» є такі: *безпека* – це стан об’єкта; *безпека* – здатність об’єкта, явища або процесу зберегти власну сутність в умовах цілеспрямованого, руйнівного внутрішнього та зовнішнього впливу; *безпека* – властивість системи, побудованої на принципах структурної стійкості, самоорганізації, цілісності (кожна з цих властивостей є системоутворюючою, тобто руйнація будь-якої з них може призвести до колапсу всієї системи); *безпека* – гарантія, необхідна умова життєдіяльності особи, суспільства, держави, що дозволяє їм зберігати та збільшувати матеріальні, духовні та моральні цінності; *безпека* – відсутність небезпек та загроз для того чи іншого об`єкта.

Суть безпеки – постійне існування загрози і повсякденна необхідність управління нею.

Безпека – це гарантована конституційними, законодавчими і практичними заходами захищеність і забезпеченість життєво важливих інтересів об`єкта від зовнішніх і внутрішніх загроз. До життєво важливих інтересів відносять: економічну самостійність об`єкта; правове і соціальне благополуччя; системну цілісність; стабільне та ефективне функціонування та розвиток.

Спеціалізована пізнавальна діяльність, метою якої є об’єктивне пізнання та розуміння природної та суспільної дійсності, а також здатність до використання здобутих знань з метою перекваліфікації дійсності згідно з вимогами людини є *секьюрітологія* – наука про безпеку.

1.2 Сутність економічної безпеки та її рівні

Особливе місце серед різних видів безпеки (соціальної, екологічної, демографічної, політичної, військової, науково-технологічної, інформаційної, енергетичної, культурної, правової, генетичної, гуманітарної, психологічної) займає безпека *економічна*.

У загальному сенсі під *економічною безпекою* розуміють найважливішу якісну характеристику економічної системи, що визначає її здатність

підтримувати нормальні умови життєдіяльності населення, стійке забезпечення ресурсами розвитку народного господарства. Забезпечення економічної безпеки – це гарантія незалежності країни, умова стабільності й ефективної життєдіяльності суспільства, досягнення успіху.

Економічна безпека має складну внутрішню структуру, у якій можна виділити три її найважливіших *елементи*:

1. *Економічна незалежність – не носить абсолютного характеру*, адже міжнародний поділ праці сприяє взаємозалежності національних економік одна від одної.

2. *Стабільність і стійкість національної економіки* – передбачають захист власності у всіх її формах, створення надійних умов і гарантій для підприємницької активності, стримування факторів, здатних дестабілізувати ситуацію.

3. *Здатність до саморозвитку і прогресу* – створення сприятливого клімату для інвестицій і інновацій, постійна модернізація виробництва, підвищення професійного, освітнього і загальнокультурного рівня працівників стають необхідними й обов'язковими умовами стійкості і самозбереження національної економіки.

Таким чином, економічна безпека – це сукупність умов і факторів, що забезпечують незалежність національної економіки, її стабільність і стійкість, здатність до постійного відновлення і вдосконалення, здатність економіки забезпечувати ефективне задоволення суспільних потреб на національному і міжнародному рівнях.

На економічну безпеку суб'єкта будь-якого рівня впливають фактори внутрішнього і зовнішнього середовища.

У ринкових умовах господарювання підприємство, як відкрита система, функціонує у складному зовнішньому середовищі, що характеризується нестабільністю та постійною динамікою. Таке середовище змушує керівництво швидко адаптуватися до нових умов, потребує знання законів розвитку та пошуку шляхів виживання в ринковій економіці, врахування чинників

невизначеності та нестійкості економічного середовища. характеризують положення суб'єкта рівня економічної безпеки.

Внутрішні фактори пов'язані з господарською діяльністю підприємства, його персоналом і безпосередньо залежать від форм, методів та організації роботи на підприємстві. Вони обумовлені тими процесами, які виникають в ході виробництва та реалізації продукції, і можуть вплинути на результати бізнесу.

Економічна безпека розглядається та оцінюється на різних її *рівнях* (рис. 1.1).

Рисунок 1.1 – Ієрархія рівнів економічної безпеки

Глобальна економічна безпека – є сукупністю економічної безпеки регіонів та окремих держав.

На міжнародному рівні національну економічну безпеку розглядають через призму глобальних проблем сучасності, а саме: нерівномірності економічного розвитку, зростання зовнішньої заборгованості, циклічних коливань національної економіки та інших чинників функціонування світового господарства.

Економічна безпека держави – спроможність національної економіки забезпечувати вільний, незалежний розвиток і утримувати стабільність громадянського суспільства та його інститутів, а також достатній оборонний

потенціал країни до всіляких несприятливих умов і варіантів розвитку подій та здатність української держави до захисту національних економічних інтересів від зовнішніх та внутрішніх загроз. Найбільш важливими *факторами* економічної безпеки для України виступають: продовольча безпека, ресурсна залежність, технологічна залежність, енергетична безпека, інформаційна безпека. Економічна безпека держави охоплює три взаємозалежних *рівні*: рівень держави, рівень регіону (області), рівень підприємств (фірм). Економічна безпека на рівні держави досягається, коли є погоджені дії суб'єктів кожного її рівня. Кожний з них здійснює при цьому свої специфічні функції, забезпечуючи безпеку як свою, так і всіх інших.

Економічна безпека на рівні регіону (області). Стан економічної безпеки України в цілому знаходиться в залежності від забезпечення стійкого розвитку всіх її регіонів. З однієї сторони, забезпечення економічної безпеки регіонів визначає інтеграцію регіональної економіки з економікою держави, а з іншої – збереження регіональної незалежності.

Економічна безпеку на рівні підприємства (фірми) – передбачає стійкий розвиток (тобто збалансований і безупинний), що досягається за допомогою використання усіх видів ресурсів і підприємницьких можливостей, за якими гарантується найбільш ефективне їх використання для стабільного функціонування та динамічного науково-технічного й соціального розвитку, запобігання внутрішнім і зовнішнім негативним впливам (загрозам). Головна мета при цьому – гарантувати стабільне та максимально ефективне функціонування підприємства зараз і забезпечити високий потенціал розвитку в майбутньому.

1.3 Складові елементи економічної безпеки підприємства

Економічна безпека підприємства є достатньо складною системою, що включає певний набір внутрішніх характеристик, спрямованих на забезпечення ефективного використання матеріальних, трудових, інформаційних та

фінансових ресурсів. Розрізняють такі критерії визначення економічної безпеки підприємства: функціональний, статичний та ресурсний. *Функціональний* – характеризує захищеність економічних інтересів від зовнішніх і внутрішніх загроз (здатність їх виявити, усунути та нейтралізувати). *Статичний* – відображає стан економічного розвитку, який характеризується збалансованістю, стійкістю, стабільністю функціонування підприємства відповідно до його стратегічних цілей. *Ресурсний* – характеризує здатність економічної системи забезпечувати безперервне виробництво та відтворення достатнім обсягом матеріальних, трудових та фінансових ресурсів.

У межах підходу до економічної безпеки підприємства як стану, обумовленого впливом зовнішнього середовища, в науковій літературі виокремлюють *ресурсно-функціональний підхід, за яким* економічну безпеку розглядають як стан найбільш ефективного використання корпоративних ресурсів для запобігання загроз і забезпечення стабільного функціонування підприємств у даний час і майбутньому. Розрізняють сім функціональних складових економічної безпеки: фінансова, силова, інформаційна, техніко-технологічна, політико-правова, кадрова та інтелектуальна, екологічна (рис. 1.2).

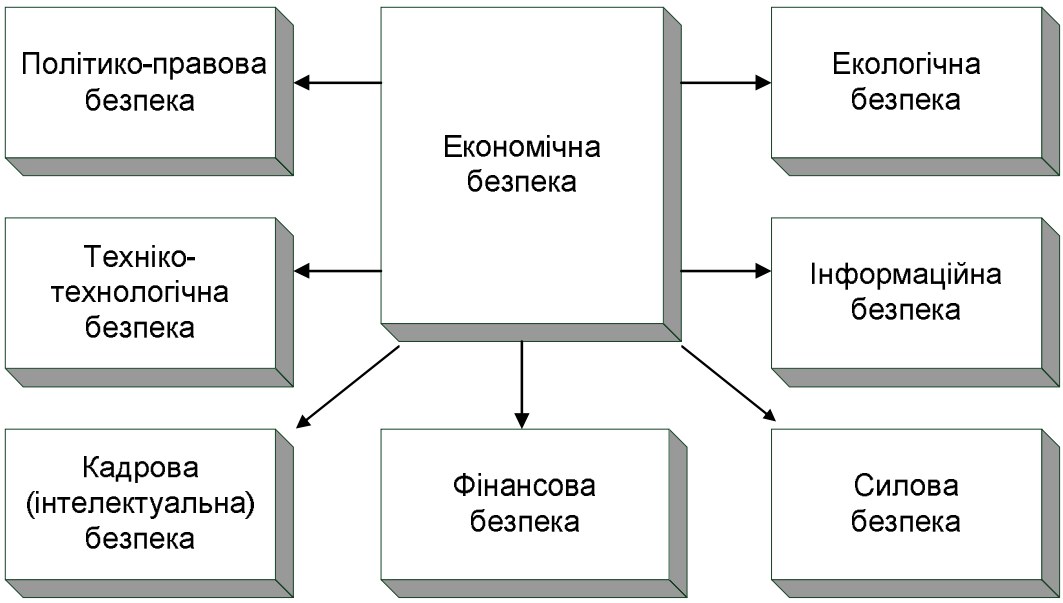

Рисунок 1.2 – Основні складові економічної безпеки підприємства

Фінансова складова – визначає і регулює питання фінансово-економічної заможності підприємства, стійкості до банкрутства. Вона вважається провідною й вирішальною, оскільки за ринкових умов господарювання фінанси є «двигуном» будь-якої економічної системи. Про її стан свідчить рівень рентабельності, частка ринку, доступ до кредитів, ліквідність коштів, курсова вартість цінних паперів, оптимальна структура капіталу тощо

Силова безпека – займається режимами, фізичною охороною об'єктів і особистою охороною керівництва, протидією криміналу, взаємодією із правоохоронними й іншими державними органами.

Інформаційна складова – заснована не тільки на захисті власної інформації, у тому числі конфіденційної, але й передбачає ділову розвідку, інформаційно-аналітичну роботу з зовнішніми і внутрішніми суб'єктами тощо. Вона також опікується створенням системи економічної підтримки прийнятих рішень щодо заходів економічної безпеки.

Техніко-технологічна складова – передбачає створення і використання такої технічної бази, устаткування й основних засобів виробництва, таких технологій і бізнес-процесів, що підсилюють конкурентоспроможність підприємства. Про неї свідчить виробничий потенціал підприємства, ступінь оновлення виробничих фондів, рівень освоєння виробничої потужності тощо.

Політико-правова складова – передбачає всебічне юридичне забезпечення діяльності підприємства, правову роботу з контрагентами і владою, вирішення інших правових питань.

Кадрова та інтелектуальна складова – передбачає запобігання негативним впливам на економічну безпеку підприємства за рахунок ризиків і загроз, пов'язаних з персоналом, його інтелектуальним потенціалом і трудовими відносинами в цілому.

Екологічна складова – розглядає проблеми охорони екологічної безпеки суспільства від суб'єктів господарювання, що здійснюють виробничо-комерційну діяльність.

Залежно від поділу факторів економічної безпеки підприємств на зовнішні та внутрішні, їх поділяють на багато видів (рис. 1.3).

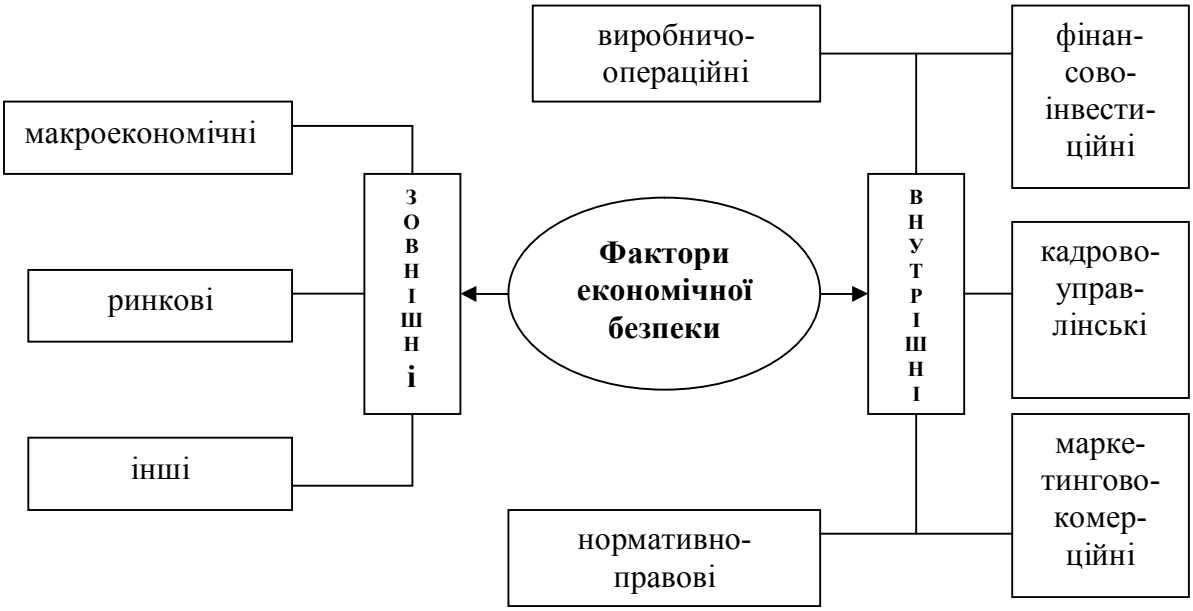

Рисунок 1.3 – Фактори економічної безпеки підприємства

Зовнішні фактори включають: макроекономічні, ринкові та інші.

Внутрішні фактори включають: виробничо-операційні, фінансово-інвестиційні, кадрово-управлінські, маркетингово-комерційні, нормативно-правові.

Рівень економічної безпеки залежить від ефективної діяльності служб підприємства, а саме: наскільки вдається запобігати загрозам й усувати збитки від їхніх негативних впливів на різні аспекти функціонування підприємства. Джерелами таких негативних впливів можуть бути: свідомі або несвідомі дії людей, організацій, у тому числі органів державної влади, міжнародних організацій або підприємств-конкурентів, а також збіг об`єктивних обставин – стан фінансової кон`юнктури на ринках підприємства, наукові відкриття і технологічні розробки, форс-мажорні обставини тощо.

1.4 Характеристика фінансово-економічної безпеки

Фінансова безпека (від англ. financial security) – складова економічної безпеки, яка характеризує стан захищеності життєво важливих (ключових) інтересів держави, регіонів, підприємницьких структур та громадян у фінансовій сфері від впливу широкого кола негативних чинників (загроз).

Об'єктом фінансової безпеки підприємства є фінансова діяльність підприємства, безпеку якої необхідно забезпечити. Фінансова діяльність – це процес, на який спрямовується функціонування підсистеми забезпечення фінансової безпеки. *Суб'єкти* фінансової безпеки – це керівництво підприємства і його персонал. *Предмет* фінансової безпеки підприємства – діяльність суб'єктів фінансової безпеки як реалізація принципів, функцій, стратегічної програми або конкретних заходів щодо забезпечення фінансової безпеки, яка спрямована на об'єкти фінансової безпеки.

Сутнісними характеристиками фінансової безпеки підприємства є наступні: *фінансова безпека* є одним з основних елементів економічної безпеки підприємства; *фінансова безпека* може бути охарактеризована за допомогою системи кількісних і якісних показників (вони повинні мати граничні значення, за допомогою яких можна зробити висновок про ступінь забезпечення фінансової безпеки підприємства); *фінансова безпека* підприємства повинна забезпечувати його розвиток і стійкість; *фінансова безпека* забезпечує захищеність фінансових інтересів підприємства.

З метою забезпечення фінансової безпеки підприємства потребують рішення наступні *задачі*: ідентифікація небезпек і загроз підприємству; визначення індикаторів фінансової безпеки підприємства; розробка системи моніторингу фінансової безпеки; розробка заходів, спрямованих на забезпечення фінансової безпеки підприємства, як у короткостроковому, так і в довгостроковому періоді; контроль за виконанням заходів; аналіз виконання заходів, їхня оцінка, коректування; ідентифікація небезпек і загроз

підприємству і коректування індикаторів у залежності від зміни стану зовнішнього середовища, цілей і задач підприємства.

На рівень фінансової діяльності підприємства і, відповідно, на стан його фінансової безпеки впливають внутрішні чинники (рівень операційного і стратегічного фінансового менеджменту) та зовнішні чинники (держава, ринок, конкуренція).

Функціональна структура фінансової безпеки підприємства – це сукупність елементів, її складових частин, які в комплексі забезпечують нормальне продуктивне функціонування підприємства. Вона базується на фінансових інтересах підприємства, до яких відносять забезпечення основним і оборотним капіталом для ефективного ведення комерційної діяльності; забезпеченість інвестиціями розвитку підприємства, включаючи максимізацію прибутку, оптимізацію відрахувань до бюджету, зростання ринкової вартості акцій тощо. До функціональної структури фінансової безпеки підприємства належать наступні елементи (рис.1.4).

Рисунок 1.4 – Структура фінансової безпеки підприємства та їх зміст

Вплив держави на стан фінансової безпеки підприємства реалізується через: політику держави: економічну, грошово-кредитну, бюджетну, податкову, інвестиційну; збалансованість національних фінансових інтересів та фінансових інтересів підприємств; функціонування секторів фінансово-кредитної сфери країни: бюджетного, грошово-кредитного, валютного, банківського, інвестиційного, фондового, страхового; національну Стратегію забезпечення фінансової безпеки держави; чинне законодавство у фінансово-кредитній сфері країни; контрольну функцію держави з боку Державної податкової адміністрації, Рахункової палати Верховної Ради України, Національного банку, Державного казначейства, Державної контрольно-ревізійної служби, Державної комісії з цінних паперів і фондового ринку, Державної комісії з регулювання послуг фінансових ринків, Державної митної служби, Пенсійного фонду.

1.5 Сутність системи фінансово-економічної безпеки підприємства

Комплексна система фінансово-економічної безпеки бізнесу – це комплекс взаємозв'язаних заходів організаційно-правового характеру, що здійснюються спеціальними органами, службами, підрозділами суб'єкта господарювання, спрямованих на забезпечення економічного зростання в майбутньому та захист життєво важливих інтересів особистості, підприємства і держави від протиправних дій з боку реальних або потенційних фізичних або юридичних осіб, що можуть призвести до істотних економічних втрат.

Головною метою забезпечення фінансово-економічної безпеки підприємства можна вважати досягнення максимальної стабільності його функціонування та створення умов для подальшого фінансово-економічного розвитку шляхом попередження внутрішніх і зовнішніх загроз. В свою чергу кожне підприємство потребує створення власної системи фінансово-економічної безпеки.

В основі розробки комплексної системи забезпечення фінансово-економічної безпеки підприємства повинна бути відповідна *концепція,* при створенні якої необхідно виходити з наступного:

1) кожне підприємство є системою, що включає різні, пов'язані між собою, складові елементи. На рівні внутрішніх і зовнішніх зв'язків системи (фірми) можуть утворюватися прогалини, через які реалізуються різні види загроз її економічної безпеки. Для забезпечення належного ступеня захисту від них необхідно протиставити діяльність, яка б носила системний характер;

2) система економічної безпеки не може бути однаковою в різних підприємствах, установах чи організаціях. Її відмінність та унікальність залежить від спеціалізації та структури виробничої діяльності та промислового потенціалу, місця суб'єкта господарювання на ринку, кваліфікації та дисциплінованості кадрів тощо;

3) система економічної безпеки окремого підприємства є відносно самостійною й відособленою по відношенню до аналогічних систем безпеки інших суб'єктів підприємницької діяльності, водночас, якщо виходити, наприклад, з адміністративно-територіального поділу, система економічної безпеки окремого підприємства є складовим елементом системи економічної безпеки міста, району, області, держави;

4) система економічної безпеки суб'єкта господарювання може бути тільки комплексною. Її забезпечення тісно пов'язано з рівнем забезпечення науково-технічної, кадрової, екологічної, інформаційної, фізичної безпеки та інших;

5) ефективне забезпечення економічної безпеки підприємства можливе за умови, коли вибір та застосування сил, засобів та охоронних заходів здійснюється на основі ретельно продуманої концепції.

Концепція системи забезпечення фінансово-економічної безпеки повинна включати мету, завдання, принципи діяльності, об'єкти та суб'єкти, стратегію та тактику.

Метою системи безпеки є своєчасне виявлення та запобігання як зовнішніх, так і внутрішніх небезпек і загроз, забезпечення захищеності діяльності підприємства та досягнення ним цілей бізнесу.

Організація, побудова та функціонування комплексної системи фінансово-економічної безпеки підприємства повинні відповідати наступним *принципам:*

1. Комплексність (системність) – необхідність створення такої системи безпеки, що забезпечила б захищеність всіх об'єктів захисту підприємства.

2. Пріоритет заходів запобігання (своєчасність) – раннє виявлення загроз та запобігання їх руйнівному впливу.

3. Безперервність – постійна дія системи.

4. Законність – робота із забезпечення безпеки повинна здійснюватися на основі діючого законодавства.

5. Плановість - діяльність щодо забезпечення безпеки організується на основі комплексної програми та конкретних планів щодо окремих напрямків безпеки.

6. Оптимальність – досягнення максимальної функціональної ефективності (віддачі) системи економічної безпеки за меншими витратами ресурсів на її забезпечення.

7. Взаємодія – погодженість діяльності всіх учасників системи, включаючи ділові контакти із зовнішніми організаціями, які забезпечують безпеку підприємств.

8. Поєднання гласності та конфіденційності – з одного боку система заходів з безпеки повинна бути відома всім працівникам підприємства, а з другого – цілий ряд засобів та методів забезпечення безпеки повинні бути відомі лише вузькому колу фахівців.

9. Компетентність – професіоналізм всіх учасників системи.

Система фінансово-економічної безпеки підприємства будується відповідно до політики та стратегії безпеки.

Політика фінансово-економічної безпеки являє собою систему поглядів, заходів, рішень, дій у галузі безпеки, що створюють умови та сприятливе середовище для досягнення цілей бізнесу.

Стратегія фінансово-економічної безпеки підприємства – це система забезпечення економічної безпеки підприємства в довгостроковому періоді, що являє собою сукупність взаємоузгоджених і взаємозумовлених складових, які об'єднує єдина глобальна мета – досягнення найвищого рівня прибутковості.

Одним з найважливіших елементів системи фінансово-економічної підприємства є *механізм її забезпечення*, що являє собою сукупність законодавчих актів, правових норм, спонукальних мотивів і стимулів, методів, заходів, сил і засобів, за допомогою яких суб'єкт впливає на об'єкт для досягнення цілей безпеки і розв'язання завдань, які стоять перед нею.

Тема 2 Чинники впливу на фінансово-економічну безпеку та адаптація підприємства

План лекції

2.1 Сутність чинників впливу на фінансово-економічну безпеку підприємства

2.2 Методи нейтралізації загроз фінансовій безпеці підприємства

2.3 Адаптація та адаптивна реакція підприємства до впливів оточуючого середовища

2.1 Сутність чинників впливу на фінансово-економічну безпеку підприємства

Провідним принципом у роботі будь-якого підприємства є прагнення до одержання якомога більшого прибутку, але воно обмежується можливістю зазнати збитків, оскільки у ринковій економіці різко посилюється фактор ризику, що впливає на діяльність підприємства.

В широкому сенсі під *ризиком* прийнято розуміти імовірність (загрозу) втрати підприємством частини своїх ресурсів, недоодержання доходів чи появи додаткових витрат у результаті здійснення певної виробничої і фінансової діяльності. Ризики, що супроводжують фінансову діяльність підприємства, виділяють в особливу групу ризиків, що мають назву фінансові ризики.

Під *фінансовими ризиками* підприємства слід розуміти вірогідність виникнення несприятливих фінансових наслідків у формі втрати доходу або капіталу у ситуації невизначеності умов здійснення його фінансової діяльності.

Ключовими *ознаками* поняття «фінансові ризики» вважаються вірогідність, невизначеність, втрати, пов'язані з настанням ризикового випадку або імовірність несприятливого відхилення від цілей, для досягнення яких і приймалося певне рішення.

Фінансові ризики мають об'єктивні засади через невизначеність зовнішнього середовища стосовно до підприємства. Зовнішнє середовище містить об'єктивні економічні, соціальні і політичні умови, у межах яких підприємство проводить свою діяльність. Невизначеність зовнішнього середовища обумовлена тим, що не завжди можна точно передбачити пропозицію на товари, кошти, фактори виробництва, до того ж існує багатоваріантність сфер використання капіталів, різноманітність критеріїв переваги інвестування коштів, обмеженість інформації тощо.

Для фінансового менеджера ризик – це, в першу чергу, вірогідність небажаного результату. Саме тому ризиком можна і потрібно управляти, тобто використовувати різноманітні заходи, які дають змогу у визначеній мірі прогнозувати настання ризикового випадку та приймати заходи задля зниження ступеню ризику.

Ризик і невизначеність – поняття взаємопов'язані, але між ними є певні відмінності. Під *невизначеністю* слід розуміти неможливість передбачити напевно, що станеться у майбутньому. *Ризик* – це така невизначеність, яку доводиться враховувати при здійсненні тих чи інших дій, адже вона може помітно впливати на стабільність функціонування будь-якого суб'єкта. Тобто у

сучасній інтерпретації ризик означає не лише можливі збитки, котрі можуть виникнути у ході реалізації господарських рішень, а насамперед імовірність несприятливого відхилення від цілей, для досягнення яких і приймалося певне рішення. Отже, ризик являє собою невизначеність щодо здійснення тієї чи іншої події в майбутньому.

Економічні рішення в умовах невизначеності приймаються в межах так званої *теорії прийняття рішень* – аналітичного підходу до вибору найкращої дії (альтернативи) або послідовності дій.

Фінансовим ризикам притаманні такі характерні особливості:

1. Ризики виникають при виборі альтернативних управлінських рішень в умовах невизначеності (у який бізнес направити інвестиції, купувати обладнання або взяти його в оренду, який обрати метод амортизації).

2. Ризики підлягають кількісній і якісній оцінці перед ухваленням управлінського рішення.

3. Ризики пов’язані з фінансовими відносинами, фінансовим менеджментом і фінансовою безпекою підприємства, рівень якої оцінюється показниками фінансової стабільності підприємства, ліквідністю активів, платоспроможністю.

4. Ризики носять імовірнісний і суб’єктивний характер.

Основним параметром диференціації фінансових ризиків у процесі управління ними є *вид ризику* (рис. 2.1). При цьому слід зазначити, що поява нових фінансових технологій, використання нових фінансових інструментів і інші інноваційні фактори будуть породжувати й нові види фінансових ризиків.

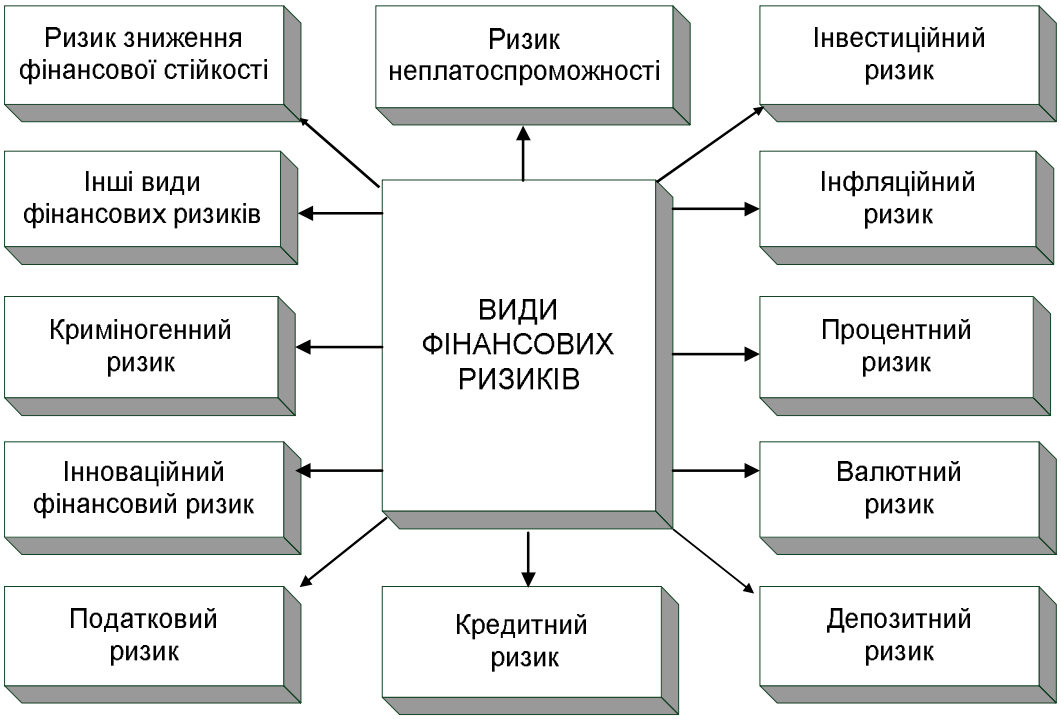

Рисунок 2.1 – Основні види фінансових ризиків підприємства

До основних видів фінансових ризиків підприємства відносять наступні:

а) *Ризик зниження фінансової стійкості* (або ризик порушення рівноваги фінансового розвитку) підприємства – генерується недосконалістю структури капіталу (надмірною часткою позикових засобів), що породжують незбалансованість позитивних і негативних грошових потоків підприємства. У складі фінансових ризиків за ступенем небезпеки (тобто здатністю генерувати загрозу банкрутства підприємства) цей вид ризику відіграє провідну роль.

б) *Ризик неплатоспроможності* (або ризик незбалансованої ліквідності) підприємства. Цей ризик генерується зниженням рівня ліквідності оборотних активів, що породжують розбалансованість позитивних і негативних грошових потоків підприємства у часі. За своїми наслідками цей вид ризику також відноситься до числа найнебезпечніших.

в) *Інвестиційний ризик.* Він характеризує можливість виникнення фінансових втрат у процесі здійснення інвестиційної діяльності підприємства.

Відповідно до видів цієї діяльності розділяються й види інвестиційного ризику – ризик реального інвестування й ризик фінансового інвестування.

г) *Інфляційний ризик.* В умовах інфляційної економіки він виокремлюється в самостійний вид фінансових ризиків. Цей вид ризику характеризується можливістю знецінення реальної вартості капіталу (у формі фінансових активів підприємства), а також очікуваних доходів від здійснення фінансових операцій в умовах інфляції.

д) *Процентний ризик.* Він складається в непередбаченій зміні процентної ставки на фінансовому ринку (як депозитної, так і кредитної). Причиною виникнення даного виду фінансового ризику є: зміна кон'юнктури фінансового ринку під впливом державного регулювання; зростання або зниження пропозиції вільних грошових ресурсів і інші фактори. Негативні фінансові наслідки цього виду ризику проявляються в емісійній діяльності підприємства (під час емісії акцій та облігацій), у його дивідендній політиці, у короткострокових фінансових вкладеннях і деяких інших фінансових операціях.

е) *Валютний ризик*. Цей вид ризику властивий підприємствам, що ведуть зовнішньоекономічну діяльність. Він виявляється в недоодержанні передбачених доходів у результаті безпосереднього впливу зміни обмінного курсу іноземної валюти, використовуваної в зовнішньоекономічних операціях підприємства, на очікувані грошові потоки від цих операцій.

є) *Депозитний ризик.* Цей ризик відбиває можливість неповернення депозитних внесків (непогашення депозитних сертифікатів).

ж) *Кредитний ризик.* Він має місце у фінансовій діяльності підприємств при наданні їм товарного (комерційного) або споживчого кредиту покупцям, формою. Його проявом є ризик неплатежу або несвоєчасного розрахунку за відпущену підприємством у кредит готову продукцію.

з) *Податковий ризик.* Цей вид фінансового ризику має ряд проявів: імовірність введення нових видів податків і зборів на здійснення окремих аспектів господарської діяльності; можливість збільшення рівня ставок діючих

податків і зборів; зміна строків і умов здійснення окремих податкових платежів; імовірність скасування діючих податкових пільг у сфері господарської діяльності підприємства.

и) *Інноваційний фінансовий ризик.* Цей вид ризику пов'язаний з провадженням нових фінансових технологій, використанням нових фінансових інструментів тощо.

і) *Криміногенний ризик*. У сфері фінансової діяльності підприємств він проявляється у формі оголошення його партнерами фіктивного банкрутства; підробки документів, що забезпечують незаконне привласнення сторонніми особами грошових і інших активів; розкрадання окремих видів активів власним персоналом і інші.

й) *Інші види ризиків*. До них відносять ризики стихійних лих і інші аналогічні «форс-мажорні ризики», ризик несвоєчасного здійснення розрахунково-касових операцій, ризик емісійний тощо.

Оскільки ризики характеризуються великою різноманітністю, тому з метою їх ефективного управління, їх прийнято класифікувати. Фінансові ризики підприємства *класифікують* за певними ознаками (табл. 2.1).

Під стратегією управління ризиком розуміють напрямки і способи використання засобів для досягнення поставленої мети. Кожному способу відповідає визначений набір правил і обмежень для ухвалення кращого рішення. Стратегія допомагає сконцентрувати зусилля на різних варіантах рішення, які не суперечать генеральній лінії стратегії і відкинути всі інші варіанти. Після досягнення поставленої мети дана стратегія припиняє своє існування, оскільки нові цілі висувають задачу розробки нової стратегії. Стратегія управління фінансовими ризиками реалізується через відповідну фінансову політику. *Тактика* – практичні методи і прийоми менеджменту для досягнення встановленої мети в конкретних умовах. Задачею тактики управління є вибір найбільш оптимального рішення і самих конструктивних у даній господарській ситуації методів і прийомів управління.

Таблиця 2.1 – Класифікація фінансових ризиків підприємства

№ п/п	Критерій класифікації	Види ризиків
1	За об'єктом, що характеризується	1. Ризик окремої фінансової операції 2. Ризик різних видів фінансової діяльності 3. Ризик фінансової діяльності підприємства в цілому
2	За сукупністю досліджуваних інструментів	1. Індивідуальний фінансовий ризик 2. Портфельний фінансовий ризик
3	За комплексністю	1. Простий фінансовий ризик 2. Складний фінансовий ризик
4	За сферою виникнення	1. Зовнішній або систематичний фінансовий ризик 2. Внутрішній або несистематичний ризик
5	За фінансовими наслідками	1. Ризик, що призводить до економічних втрат 2. Ризик, що призводить до втрачених вигод 3. Ризик, що призводить як до економічних втрат, так і до додаткових доходів
6	За характером прояву у часі	1. Постійний фінансовий ризик 2. Тимчасовий фінансовий ризик
7	За рівнем вірогідності реалізації	1. Фінансовий ризик з низьким рівнем імовірності реалізації 2. Фінансовий ризик із середнім рівнем імовірності реалізації 3. Фінансовий ризик з високим рівнем імовірності реалізації 4. Фінансовий ризик, рівень імовірності реалізації якого визначити неможливо
8	За рівнем фінансових втрат	1. Припустимий фінансовий ризик 2. Критичний фінансовий ризик 3. Катастрофічний фінансовий ризик
9	За здатністю передбачення	1. Прогнозований фінансовий ризик 2. Непрогнозований фінансовий ризик
10	За можливістю страхування	1. Ризик, що може бути застрахований 2. Ризик, що не може бути застрахованим

Управління фінансовими ризиками (ризик-менеджмент) містить наступні складові: якісний аналіз ризиків, виявлення ризикогенеруючих чинників; кількісну оцінку ризиків, яка передбачає визначення імовірності виникнення та розміру можливих збитків; розробку засобів оптимізації ризикових ситуацій шляхом мінімізації або нейтралізації ризиків.

Стратегія ризик-менеджменту – це мистецтво управління ризиком у невизначеній господарській ситуації, засноване на прогнозуванні ризику і прийомів його зниження. Ця стратегія включає правила, на основі яких приймаються ризикові рішення і способи вибору їхнього варіанту.

В системі методів управління фінансовими ризиками підприємства основна роль належить *внутрішнім механізмам їх нейтралізації, які* являють собою систему методів мінімізації їх негативних наслідків, що обираються і здійснюються в межах підприємства.

Система внутрішніх механізмів нейтралізації фінансових ризиків передбачає використання наступних основних *методів:*

відмова від здійснення фінансових операцій, рівень ризику за якими надмірно високий;

відмова від використання в високих об’ємах позичкового капіталу;

відмова від надмірного використання оборотних активів в низько ліквідних формах;

відмова від використання тимчасово вільних грошових активів в короткострокових фінансових вкладеннях.

Близьким до поняття «ризик» є терміни «загроза» та «небезпека».

Загроза – це ризик, який почав реалізовуватися за небажаним варіантом, або заздалегідь відомий сценарій несприятливого розвитку подій, що відповідно виходить за рамки поняття нормальної невизначеності умов господарської діяльності.

Загроза – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам об’єкту охорони.

Загроза – будь-які обставини або події, що можуть привести не тільки до порушення встановлених бізнесів-процесів, збитків або зменшення доходу але й до порушення політики безпеки підприємства.

Важливою передумовою формування системи фінансової безпеки підприємства є ідентифікація загроз їх реалізації. Від того, як точно і в повній мірі визначений склад загроз фінансовим інтересам, оцінено рівень інтенсивності їх проявлення та можливого збитку, залежить ефективність побудови всієї системи фінансової безпеки підприємства.

Усі *джерела фінансової загрози* підприємства поділяють на дві групи: *об'єктивні* (виникають в результаті форс-мажорних обставин) та *суб'єктивні*, які мають внутрішнє та зовнішнє походження. Таким чином, загроза фінансовим інтересам представляє собою форму вираження її протиріччя з фінансовим середовищем функціонування підприємства, що відображає реальну або потенційну можливість проявлення деструктивного впливу різних факторів та умов на їх реалізацію в процесі фінансового розвитку, що приводить до прямого або непрямого економічного збитку.

Близьким до терміну «загроза» за рівнем впливу на об'єкт загрози є поняття «небезпека».

Небезпека – це можливі або реальні явища, події і процеси, здатні завдати шкоду підприємству, закрити шляхи до розвитку або навіть знищити його. Вона може виступати у різних формах: у вигляді намірів, планів підготовки дій і самих дій, спрямованих на знищення, послаблення, ліквідацію об`єктів безпеки.

Основою для розмежування небезпек і загроз за їх видами є виділення класифікаційних ознак і віднесення небезпек і загроз до тієї чи іншої групи за східними ознаками.

Залежно від джерела походження чинники загрози поділяють на *зовнішні* і *внутрішні.*

Головні *зовнішні чинники загрози*, що впливають на втрату фінансової безпеки – це: скупка акцій, боргів підприємства партнерами; наявність значних фінансових зобов'язань у підприємства (як великої величини позикових

засобів, так і великих заборгованостей підприємству); нерозвиненість ринків капіталу і їхньої інфраструктури; недостатньо розвинута правова система захисту прав інвесторів і виконання законодавства; криза грошової і фінансово-кредитної систем; нестабільність економіки; недосконалість механізмів формування економічної політики держави.

До *внутрішніх чинників загроз*, що впливають на фінансову безпеку, відносяться навмисні або випадкові помилки менеджменту в сфері керування фінансами підприємства, пов'язані з: вибором стратегії підприємства; керуванням і оптимізацією активів і пасивів підприємства (розробка, впровадження і контроль керування дебіторською і кредиторською заборгованостями, вибір інвестиційних проектів і джерел їхнього фінансування, оптимізація амортизаційної і податкової політики).

За систематичністю прояву – чинники загрози поділяються на: *систематичні загрози*, котрі, водночас виникнувши, існують завжди (чи досить тривалий час) і завжди справляють свій вплив на діяльність підприємства. Дані загрози мають систематичний характер прояву, оскільки відображують реальні процеси, які відбуваються у ринковій економіці, а також закони розвитку ринку; *несистематичні загрози*, що справляють свій вплив на діяльність підприємства з визначеним періодом виникнення. До таких загроз можна віднести сезонні коливання попиту на продукцію, загрози стихійних лих, тимчасовий розрив відносин з постачальником або підрядником, нестабільність роботи дилерської мережі тощо.

За тривалістю впливу на функціонування і розвиток підприємства чинники загрози поділяють на довго-, середньо- і короткострокові.

За можливістю локалізації менеджментом підприємства наслідків загроз їх поділяють на керовані і некеровані.

Залежно від ступеня кризи, викликаної дією того чи іншого дестабілізуючого фактора, загрози класифікуються на такі, що викликають певні ускладнення, значні та катастрофічні.

2.2 Методи нейтралізації загроз фінансовій безпеці підприємства

Процес забезпечення фінансової складової економічної безпеки підприємства може бути визначений сукупністю робіт щодо забезпечення максимально високого рівня платоспроможності підприємства та ліквідності оборотних коштів, найбільш ефективної структури капіталу підприємства, підвищення якості планування та здійснення фінансово-господарської діяльності за всіма напрямами стратегічного та оперативного планування та управління технологічним та кадровим потенціалом підприємства, його основними та оборотними активами з метою максимізації прибутку та підвищення рентабельності бізнесу, а також підвищення курсової вартості цінних паперів підприємства.

Господарська практика виробила систему заходів, спрямованих на зменшення ризику виникнення загроз до мінімально можливого рівня, що мають різні форми та зміст. При цьому застосовуються наступні *групи методів:* технічні, правові, організаційно-економічні.

Технічні методи засновані на впровадженні різних технічних засобів, наприклад, систем протипожежного контролю, банківських електронних розрахунків, охоронної сигналізації тощо.

До групи *економічних методів* відносяться: страхування, застава, неустойка (штраф, пеня), гарантія, задаток.

Організаційні методи включають комплекс розпорядницьких заходів, спрямованих на запобігання втрат від ризику у випадку настання несприятливих обставин, а також на їх компенсацію у випадку виникнення втрат. Вони, зазвичай, реалізуються за допомогою різних управлінських регламентів.

Найбільш розповсюдженими *методами зниження ризику* на підприємстві є:

1. Страхування. У комплексі з іншими методами дозволяє істотно знизити рівень господарського ризику при плануванні і реалізації стратегії

підприємства. Страхування є системою відшкодування збитків страховиками при настанні страхових випадків зі спеціальних страхових фондів, сформованих за рахунок страхових внесків, що сплачуються страхувальниками. Страхування може здійснюватися в *двох формах*: *обов'язкове і добровільне.*

Крім страхування може застосовуватися перестрахування і співстрахування. *Перестрахування* – це страхування, відповідно до якого страховик передає частину відповідальності по ризиках іншим страховикам, (перестрахувальникам). Мета такої операції полягає у створенні стійкого і збалансованого «страхового портфеля» для забезпечення стабільної і рентабельної роботи страхових організацій. *Співстрахування* – метод вирівнювання і розподілу великих ризиків між декількома страховиками. При цьому кожний з них укладає зі страхувальником окремий договір. При цьому визначається страховик, що бере на себе функції організатора страхування.

2. Поручительство. Даний вид передбачає, що при недостатності засобів у боржника поручитель несе відповідальність за його зобов'язаннями перед кредитором. При цьому існує солідарна відповідальність поручителя і боржника. За допомогою такого прийому забезпечується зворотність кредитів, виданих банками.

3. Застава. Даний метод стосується забезпечення виконання зобов'язань, за яким кредитор (заставоутримувач) має право одержати задоволення своєї вимоги з вартості закладеного майна переважно перед іншими кредиторами у випадку невиконання боржником (заставником) забезпеченого заставою зобов'язання. Предметом застави може бути будь-яке майно: будинок, споруди, устаткування, цінні папери, грошові кошти, майнові права, що можуть бути відчужені.

4. Розподіл ризику. Найчастіше цей спосіб застосовується у випадку розробки і реалізації проекту декількома виконавцями (інвесторами, проектувальниками, будівельниками, замовниками). При цьому кожен учасник виконує запланований проектом обсяг робіт і несе відповідну частку ризику у випадку невиконання проекту, але найбільшому ризикові піддається інвестор.

5. Резервування засобів. Створення резервів ресурсів на покриття непередбачених витрат дозволяє компенсувати ризик, що виникає у процесі реалізації планів підприємства, і тим самим ліквідувати різні збої у роботі.

Для забезпечення належного рівня фінансово-економічної безпеки підприємства насамперед виявляються причини, фактори виникнення відповідних загроз, здійснюється їх моніторинг і прогнозується їх вплив. *Моніторинг* фінансово-економічної безпеки підприємства – це інформаційно-аналітична, постійно діюча система спостережень за динамікою показників, що характеризують її рівень. Метою моніторингу є одержання інформації керівництвом підприємства про рівень ефективності і результативності діяльності підприємства на основі якісного і кількісного аналізу і оцінювання відповідних показників та оцінки виникнення або існування можливих загроз та ризиків. Предметною областю моніторингу рівня фінансово-економічної безпеки є визначення інтегрального показника економічної безпеки підприємства за виділеними функціональними складовими. Однією із умов, якою повинен відповідати алгоритм проведення моніторингу є можливість кількісної оцінки всіх досліджуваних показників для визначення рівня фінансово-економічної безпеки підприємства.

2.3 Адаптація та адаптивна реакція підприємства до впливів оточуючого середовища

Фінансово-економічну безпеку підприємства слід розглядати як *ступінь гармонізації* у часі та просторі фінансових інтересів підприємства з інтересами складових оточуючого середовища – держави, ринку, конкурентів. Звідси – підприємство тільки тоді знаходиться у належному стані безпеки, якщо його фінансові інтереси певною мірою узгоджені з інтересами суб’єктів зовнішнього середовища: споживачів, постачальників, конкурентів, інвесторів, держави.

У системі адаптації підприємства до впливів зовнішнього середовища виділяються дві складові адаптації: *адаптивна реакція підприємства* і власне

процес адаптації. Під адаптивною реакцією підприємства на вплив зовнішнього середовища розуміють зміну стратегічних цілей діяльності підприємства або способів досягнення цілей, що істотно впливають на взаємини підприємства з зовнішнім середовищем. У свою чергу, процес адаптації варто розуміти як процес внесення змін у функціонуванні внутрішніх систем і діяльність підрозділів підприємства, що супроводжують адаптивну реакцію.

Адаптивна реакція підприємства з'являється під впливом факторів зовнішнього середовища.

За оточенням та періодичністю впливу на підприємство, зовнішнє середовище поділяється на: середовище найближчого оточення; віддалене середовище організації.

Відповідно до функціонального розподілу, стан зовнішнього середовища розподіляється за їх природою на: соціальне, економічне, політичне та технологічне.

Середовище підприємства поділяють на такі групи елементів-факторів: зовнішнє середовище: макросередовище та мікросередовище; внутрішнє середовище.

Макросередовище складається з елементів-факторів непрямої дії, тобто вони переважно прямо не пов'язані з конкретним підприємством, проте створюють певне сприятливе або несприятливе середовище для його господарської діяльності. До факторів макросередовища, що здійснюють вплив на підприємство: стан економіки країни; політико-правові відносини; ефективність державного регулювання економіки; рівень НТП; рівень соціального розвитку; стан культури, ціннісних орієнтацій в суспільстві; дієвість профспілок, партій і громадських організацій; демографія; природні умови, екологія; міжнародне становище; надзвичайні обставини (форс-мажорні).

Мікросередовище – це середовище безпосереднього впливу на підприємство, тобто це учасники ринку, які безпосередньо контактують з

підприємством. Фактори мікросередовища: конкуренти і конкурентне середовище в цілому; покупці; постачальники; партнери; місцеві органи профспілок, партій, громадських організацій; місцеві органи влади тощо.

Метою адаптації підприємств до факторів впливу зовнішнього середовища є забезпечення фінансово-економічної безпеки підприємства за допомогою підвищення ефективності використання економічних та фінансових ресурсів, забезпечення балансу економічних інтересів із суб'єктами зовнішнього середовища, зміцнення або збереження його ринкових позицій для забезпечення конкурентоспроможності продукції. Адаптація підприємства до впливу зовнішнього середовища являє собою багатоступеневий процес (рис. 2.2).

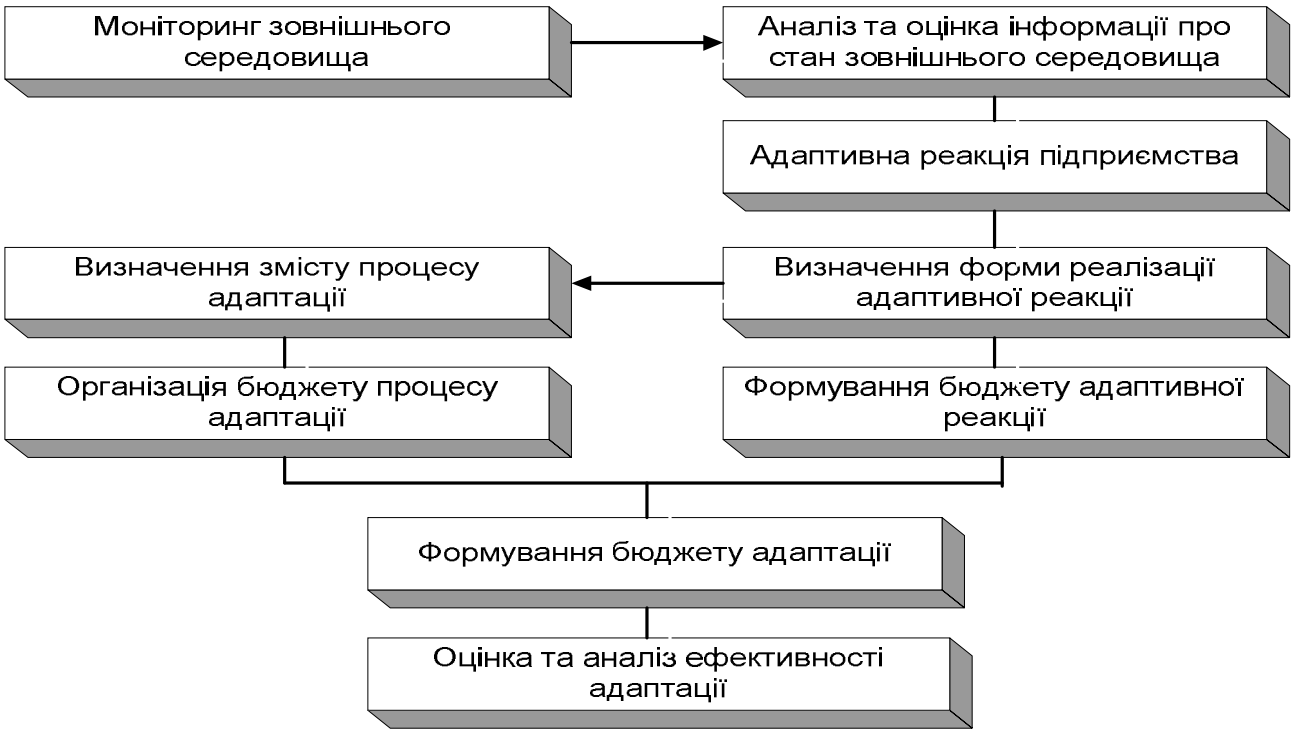

Рисунок 2.2 – Схема адаптації підприємства до змін у зовнішньому середовищі

Адаптація підприємства до змін у зовнішньому середовищі і пов'язаними з ними впливами факторів зовнішнього середовища може бути параметричною і структурною.

Параметрична адаптація припускає зміну параметрів внутрішніх систем підприємства, наприклад, освоєння виробництва нової продукції або нової технології, зміну ринків збуту або цінової політики підприємства.

Структурна адаптація передбачає зміну самої структури внутрішньої системи підприємства, появу нових внутрішніх систем, реорганізацію або ліквідацію існуючих.

У залежності від ролі і значення адаптаційних елементів, а також готовності до адаптивної реакції можна виділити три моделі поводження підприємств, кожна з яких визначає його готовність до адаптації: *модель активного, консервативного і змішаного поводження*.

Активна модель поводження підприємства є найбільш адаптованою до ринкових впливів. Вона припускає розробку різних моделей адаптивної реакції в залежності від характеру прогнозованих змін і ступеня їхньої важливості для діяльності підприємства.

У *консервативній моделі* поводження адаптивна реакція носить змушений і локальний характер, тобто зміни в діяльності підприємства відбуваються лише тоді, коли воно поставлено перед вибором: або збитки аж до банкрутства, або перетворення, але лише за окремими аспектами діяльності або в окремих підрозділах підприємства, що не робить істотного впливу на діяльність усього підприємства.

У *змішаній моделі* поводження підприємства розроблена не модель адаптації, а тільки її загальні принципи і підходи до поводження підприємства в ринкових умовах, а сама адаптація залежить від виду і ступеня інтенсивності впливу факторів зовнішнього середовища: при інтенсивному впливі загальні принципи адаптації певним чином реалізуються в діяльності підприємства, а при невисокій інтенсивності – реалізація принципів адаптації носить поверхневий і несистемний характер.

У залежності від факторів, що впливають, сукупність адаптивних заходів підприємства можна поділити на такі групи: адаптація підприємства до

нововведень; адаптація підприємства до змін кон'юнктури ринку; адаптація підприємства до соціально-культурних і політико-правових умов.

Адаптивна реакція підприємства потребує фінансової підтримки, яка може бути надана як за рахунок витрат виробництва, так і за рахунок інвестиційних ресурсів. Так, вартість живої праці, короткострокових позикових ресурсів включається переважно у витрати підприємства. До витрат, фінансованих за рахунок інвестиційних ресурсів, відносяться: розширення обсягу оборотних коштів, підвищення кваліфікації, підготовка і навчання персоналу, залучення фінансових ресурсів на довгостроковій основі, організація просування продукції, консультації експертів і фахівців тощо.

Усі витрати, що пов'язані з прийняттям і реалізацією рішень з адаптації підприємства, поділяються на *дві групи:* витрати на розробку рішень з адаптації і витрати на реалізацію цих рішень. Збалансованість витрат на адаптацію підприємства є одним з інструментів керування адаптацією підприємства, зокрема, її ресурсним забезпеченням.

На відміну від витрат на процес адаптації, витрати на реалізацію адаптивної реакції підприємства відшкодовуються переважно за рахунок інвестиційних ресурсів, оскільки більшість видів адаптивної реакції підприємства передбачають різного роду зміни, пов'язані з виробничою базою (розширення виробничої бази, підвищення її технічного рівня, її зміна відповідно до обраного критерію), організаційною структурою підприємства і його структурою керування. Тільки окремі види витрат на реалізацію адаптивної реакції підприємства можуть відшкодовуватися за рахунок витрат виробництва. Реалізація практично усіх видів адаптивної реакції підприємства вимагає значних інвестицій, джерелами яких можуть бути власні, позикові або притягнуті засоби. Сума витрат на адаптацію називається *бюджетом адаптації.*

Тема 3 Механізм управління фінансово-економічною безпекою підприємства

План лекції

3.1 Сутність механізму управління фінансово-економічною безпекою підприємства

3.2. Складові елементи механізму управління фінансово-економічною безпекою підприємства

3.1 Сутність механізму управління фінансово-економічною безпекою підприємства

Під управлінням фінансово-економічною безпекою підприємства розуміють систему принципів і методів розроблення та реалізації управлінських рішень, які пов'язані із забезпеченням захисту його пріоритетних фінансово-економічних інтересів від внутрішніх і зовнішніх загроз. Процес оцінювання загроз фінансово-економічній безпеці підприємства, розроблення та реалізація методів нейтралізації негативного впливу цих загроз вимагають побудови адекватного механізму управління фінансово-економічною безпекою.

Механізм управління фінансово-економічної безпекою підприємства представляє собою сукупність економічних, мотиваційних, організаційних і правових процедур прийняття управлінських рішень щодо забезпечення захисту фінансових інтересів, які дозволяють узгоджувати інтереси взаємодіючих сторін, об'єктів і суб'єктів управління.

На практиці в основу механізму забезпечення фінансово-економічної безпеки покладено вдосконалену принципову схему, яка передбачає наявність *трьох базових компонентів:* інтереси підприємства у фінансовій сфері, загрози як чинники, що створюють небезпеку реалізації означених інтересів, а також

систему заходів, направлених на усунення загроз, їх прогнозування, своєчасне попередження і профілактику.

Фінансові інтереси підприємства виступають носіями суперечностей фінансової діяльності і тому вони нерозривні між собою. Інтереси, як і суперечності, водночас є джерелами і рушіями розвитку фінансової діяльності підприємства і забезпечення його фінансово-економічної безпеки.

Класифікація фінансових інтересів в залежності від різних критеріїв наведена на рис. 3.1.

Рисунок 3.1 – Система фінансових інтересів підприємства

Головним фінансовим інтересом в умовах ринкової трансформації економіки виступає *зростання ринкової вартості підприємства.* Крім того, до основних інтересів можна віднести наступні: забезпечення основним і оборотним капіталом для ефективного ведення комерційної діяльності;

забезпеченість інвестиціями для розвитку підприємства, включаючи його фінансову систему; максимізація прибутку; оптимізація відрахувань до бюджету та ін. З метою управління фінансово-економічною безпекою доцільно розвернути цю сукупність фінансових інтересів підприємства у «дерево» інтересів шляхом їхньої конкретизації і перетворення у певні цілі.

Алгоритм практичної реалізації фінансових інтересів підприємства представлено на рис. 3.2.

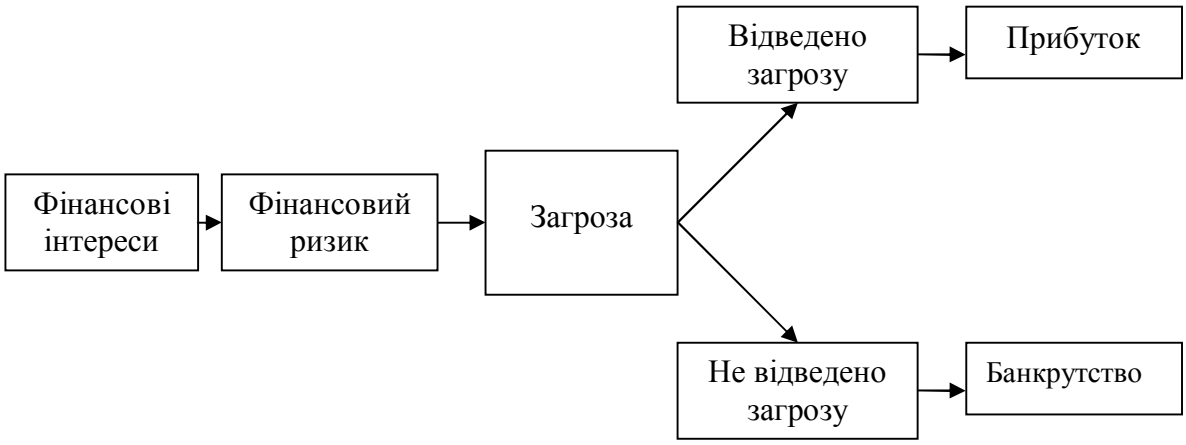

Рисунок 3.2 – Схема взаємозв’язку основних категорій фінансово-економічної безпеки підприємства

В основу забезпечення фінансово-економічної безпеки підприємства покладено концепцію системного поєднання функцій контролю, планування, зворотного зв’язку та інформаційного забезпечення.

3.2 Складові елементи механізму управління фінансово-економічною безпекою підприємства

Механізм управління фінансово-економічної безпеки підприємства являє собою єдність процесу управління і системи управління.

До структури (складу) механізму управління відносить такі складові елементи: об’єкт та суб’єкт управління, функції управління, принципи і методи управління, організаційну структуру, управлінський персонал, техніку і

технології управління, фінансові інструменти, критерії оцінки рівня фінансово-економічної безпеки.

Усі наведені елементи пов'язані між собою і складають єдиний механізм (рис. 3.3).

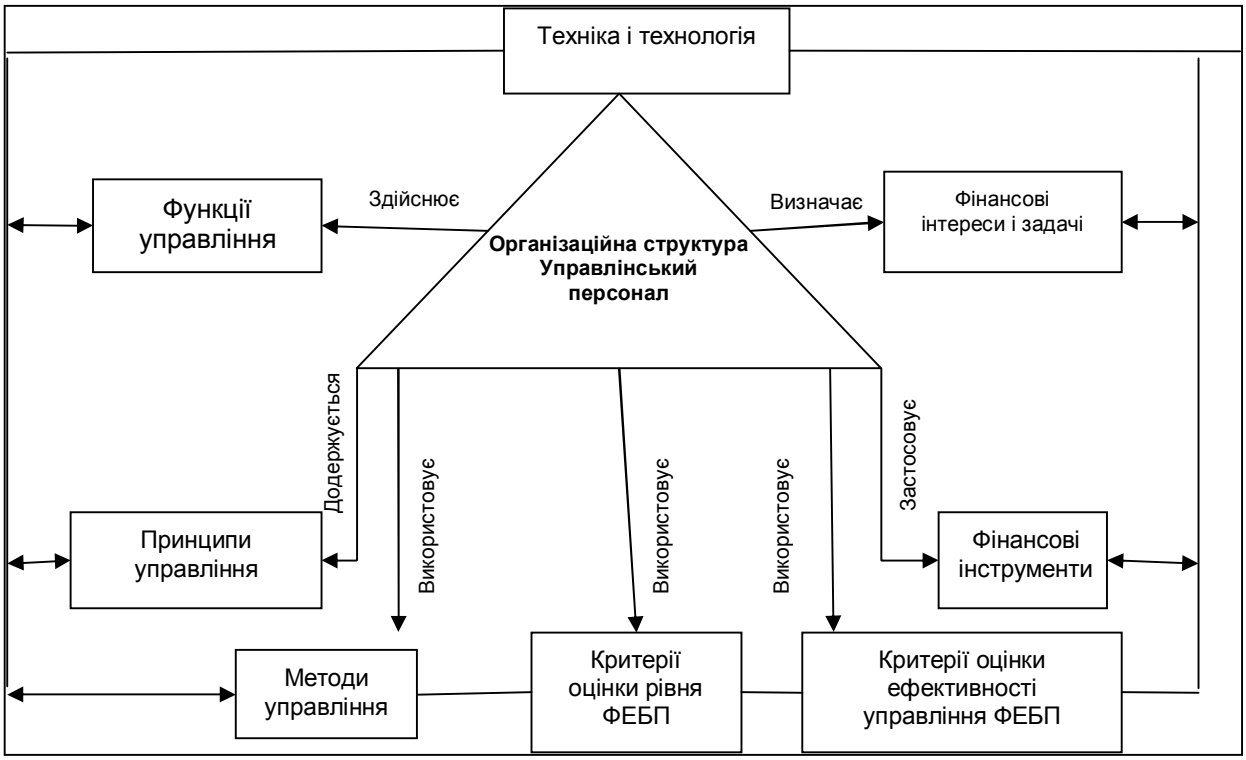

Рисунок 3.3 – Елементи механізму управління фінансово-економічною безпекою підприємства

Суб'єктів фінансово-економічної безпеки підприємства можна класифікувати: *за приналежністю:* власні служби безпеки, що входять у структуру суб'єктів господарювання і повністю утримуються за їхні кошти; самостійні комерційні чи державні організації, що наймаються суб'єктом господарювання для виконання функцій щодо забезпечення окремих або всіх аспектів його безпеки; *залежно від безпосередньої участі в забезпеченні безпеки підприємства:* спеціальні суб'єкти, створені виключно для виконання функцій щодо забезпечення безпеки фірми, як її власна служба безпеки, так і залучена на умовах договору; напівспеціальні суб'єкти, до безпосередніх функцій яких входить низка таких, що спрямовані на забезпечення безпеки підприємства; решта персоналу та структурні підрозділи, участь яких у

здійсненні заходів щодо забезпечення безпеки підприємства має винятковий характер; *залежно від форми власності та підпорядкування:* державні органи – здійснюють повноваження щодо безпеки суб'єктів фінансово-господарської діяльності, до структури яких вони входять, або ж надають послуги стороннім фірмам на умовах укладених договорів; недержавні органи (представлені охоронними організаціями, аналітичними центрами, інформаційними та консалтинговими службами, які за відповідну плату на умовах договору надають послуги щодо охорони об'єктів, здійснюють захист інформації, комерційної таємниці тощо); *залежно від правової основи функціонування (легітимності суб'єктів):* офіційні органи, що функціонують у межах чинного законодавства України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України; нелегітимні структури, діяльність яких відбувається поза правовим полем України.

До складу основних функцій управління фінансово-економічною безпекою можна віднести, базуючись на теорії управління, наступні: планування (включаючи програмування і прогнозування), організацію і регулювання, стимулювання, контроль (у вигляді обліку, аналізу і аудиту).

У процесі *планування* розробляються оперативні та щорічні фінансові плани, концепції, стратегічні програми і прогнози забезпечення фінансово-економічної безпеки. У процесі *організації і регулювання* суб'єкт управління застосовує фінансові інструменти і технології. У такому разі суб'єктом управління виступає сукупність організаційних, фінансових і правових методів управління, завдяки використанню яких реалізуються управлінські рішення щодо забезпечення фінансової безпеки підприємства. Суб'єктом управління в процесі стимулювання виступає сукупність економічних і соціально-психологічних методів управління. *Контроль* у вигляді обліку, аналізу і аудиту уявляє собою зворотний зв'язок між фінансовими цілями і ступенем їхньої реалізації.

Управління фінансово-економічною безпекою підприємства повинно базуватися на наступних *принципах*:

законності – передбачає дотримання основ чинного законодавства під час забезпечення фінансово-економічної безпеки підприємства;

комплексності – створення цілісної системи фінансово-економічної безпеки, направленої на забезпечення захисту інтересів підприємства від різного роду небезпек під час реалізації його фінансово-економічної стратегії;

безперервності – полягає в постійному, безперервному процесі управління фінансово-економічною безпекою підприємства;

системність побудови – усі елементи системи управління фінансово-економічною безпекою підприємства мають бути взаємопов'язані та взаємоузгоджені між собою;

інтегрованість із загальною системою менеджменту – система управління фінансово-економічною безпекою підприємства має бути складовою системи менеджменту підприємства;

інтегрованість із системою управління безпекою підприємства;

спрямованість на стратегічні цілі фінансово-економічного розвитку підприємства – прийняті управлінські рішення не повинні суперечити загальній стратегії фінансово-економічного розвитку підприємства;

своєчасності та адекватності – передбачає побудову такої система фінансової безпеки, яка б могла на ранніх стадіях виявляти різноманітні загрози та вживати заходи щодо попередження їх негативного впливу на діяльність підприємства;

оперативність та динамічність управління – система управління фінансово-економічною безпекою має забезпечувати швидку реакцію підприємства на появу реальних та потенційних загроз та своєчасне прийняття відповідних управлінських рішень;

плановості – передбачає організацію діяльності спрямовану на забезпечення фінансово-економічної безпеки підприємства на основі комплексних програм і планів;

об’єктивність – управлінські рішення мають розроблятися з урахуванням об’єктивних економічних законів, на основі глибокого аналізу ситуації з застосуванням наукових методів пізнання;

комплексний характер управлінських рішень – прийняті управлінські рішення мають бути збалансованими, несуперечливими;

варіативність підходів до розробки окремих управлінських рішень – розробка декількох альтернативних варіантів управлінських рішень у сфері фінансово-економічною безпеки на основі визначених критеріїв;

безперервності моніторингу зовнішнього середовища підприємства – передбачає здійснення постійного контролю для своєчасного виявлення та ідентифікації загроз фінансово-економічним інтересам підприємства;

адекватність реагування на окремі загрози фінансовим інтересам – розробка заходів щодо реагування на загрози фінансово-економічним інтересам підприємства відповідно до визначених критеріїв, пріоритетної реакції потребують загрози з високою ймовірністю реалізації та (або) з великим обсягом можливої шкоди підприємству;

гнучкість (адаптивність) управління – система управління фінансово-економічною безпекою підприємства повинна адаптуватися та коригуватися відповідно до змін факторів зовнішнього та внутрішнього середовища підприємства;

ефективність прийняття управлінських рішень – витрати на заходи з ліквідації, нейтралізації чи мінімізації загроз фінансово-економічним інтересам підприємства мають бути меншими, ніж можливі збитки від їх реалізації;

стимулювання та відповідальність персоналу і керівництва за стан фінансово-економічної безпеки підприємства – розробка дієвої і ефективної системи стимулів та відповідальності посадових осіб за стан фінансово-економічної безпеки підприємства.

Організаційна складова управління фінансово-економічної безпеки підприємства передбачає склад і підпорядкованість різних елементів, ланок і рівнів управління фінансово-економічною безпекою та наявність необхідного персоналу, наділеного відповідними повноваженнями щодо здійснення діяльності із захисту фінансово-економічної безпеки. *Організаційна структура* – це сукупність органів, осіб та служб (відділів), що задіяні у забезпеченні фінансово-економічної безпеки на рівні підприємства.

Організація управління фінансово-економічною безпекою на підприємстві включає в себе необхідність формування організаційної схеми управління фінансово-економічною безпекою, встановлення центрів відповідальності за виконанням його завдань; визначення прав, обов'язків, відповідальності керівників та працівників окремих структурних підрозділів за рівень фінансово-економічної безпеки підприємства; організація постійного моніторингу рівня фінансово-економічної безпеки.

Забезпечення всебічної безпеки підприємства потребує створення спеціального підрозділу з метою реалізації захисних заходів – служби безпеки. Служба безпеки підприємства створюється залежно від величини самого підприємства. Як правило, в основному вона створюється на великих підприємствах, але за наявності можливості – на середніх. У всіх інших випадках безпеку малим і середнім підприємствам забезпечують місцеві органи внутрішніх справ або при державній службі безпеки. У залежності від цілей забезпечення безпеки можуть створюватися різні варіанти структури служби безпеки (рис. 3.4).

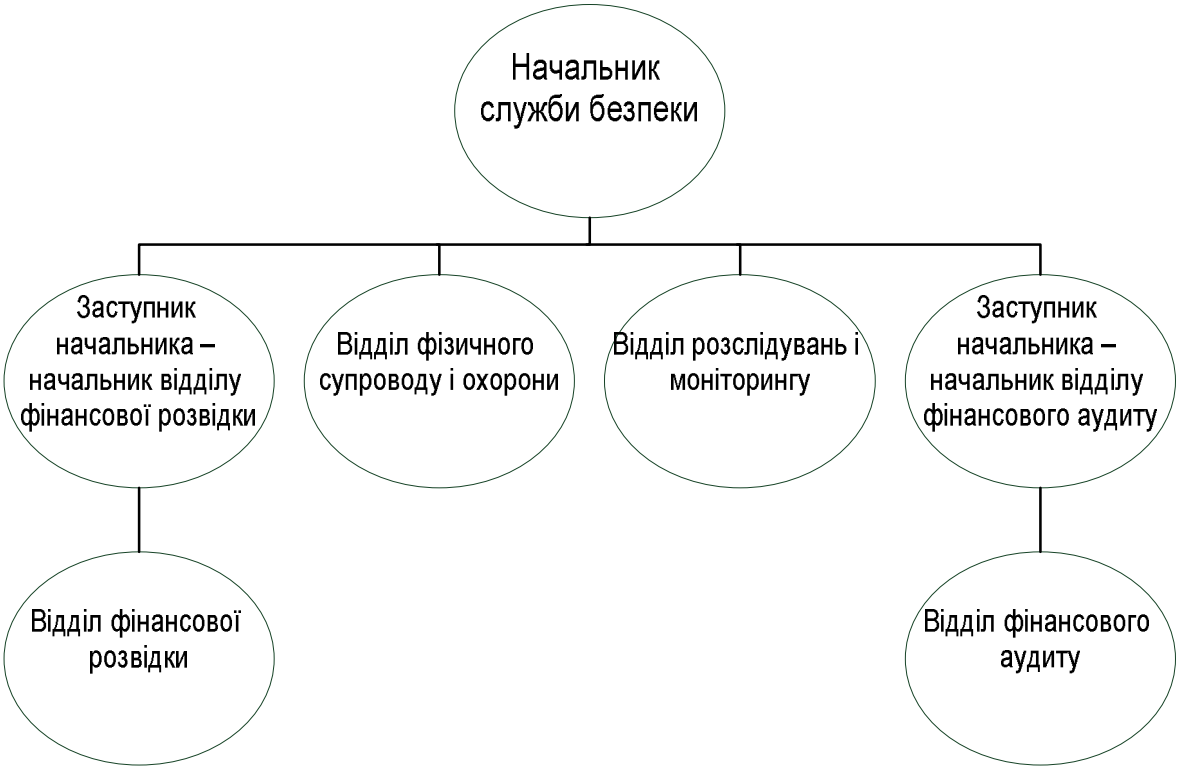

Рисунок 3.4 – Приклад структура служби фінансово-економічної безпеки підприємства

Функції забезпечення фінансово-економічної безпеки покладено на відділи фінансової розвідки і фінансового аудиту. Підрозділи служби безпеки взаємодоповнюють один одного, оскільки перший орієнтований на виявлення зовнішніх загроз фінансовим інтересам, а другий концентрує увагу на внутрішньому середовищі підприємства.

Управлінський персонал. Існуючий поділ управлінської праці в організації є основою класифікації її управлінського персоналу. Міжнародна організація праці розглядає управлінський персонал як частину категорії працівників, до якої, крім менеджерів, входять й інші фахівці-професіонали. Підставою для цього вважається тісний зв’язок у роботі менеджерів і фахівців. Вони залежать один від одного і спільно забезпечують запланований розвиток організації.

Найбільш поширений підхід, згідно з яким управлінський персонал поділяють на *керівників, фахівців, службовців* (технічних виконавців).

Аналіз рівня фінансово-економічної безпеки підприємства передбачає: аналіз зовнішнього та внутрішнього середовища з метою виявлення загроз його фінансово-економічним інтересам; оцінку загроз та їх можливих наслідків для підприємства; розрахунок та оцінку основних показників-індикаторів рівня фінансово-економічної безпеки суб'єктів господарювання. На основі проведеного аналізу рівня фінансово-економічної безпеки підприємства здійснюється стратегічне, поточне, оперативне планування фінансово-економічної безпеки підприємства. Результатом стратегічного планування має бути стратегія забезпечення фінансово-економічної безпеки підприємства. Поточне планування включає розробку поточних фінансових планів підприємства, а оперативне – короткострокових фінансових планових документів.

Контроль за реалізацією прийнятих управлінських рішень у сфері фінансово-економічної безпеки підприємства передбачає здійснення попереднього, поточного та підсумкового контролю за ходом реалізації рішень у сфері фінансово-економічної безпеки підприємства, і включає, зокрема, вибір контрольних показників, виявлення розмірів відхилень по кожному з них та встановлення їх причин, прийняття рішень про ліквідацію розбіжностей.

Методичне забезпечення фінансово-економічної безпеки підприємства може включати такі методи дослідження як: техніко-економічні розрахунки, балансовий, економіко-статистичний, економіко-математичний, експертних оцінок, реінжинірингу, логістики, оптимізації тощо.

Інструментарій, спрямований на забезпечення ефективного управління фінансово-економічною безпекою поділяється на дві групи: фінансово-економічні методи (управління прибутком, витратами, капіталом, фінансовий облік, фінансовий аналіз, фінансове планування, фінансове регулювання, страхування тощо); економічні важелі – прибуток, дохід, фінансові санкції, дивіденди, ціна, фінансове стимулювання, заробітна плата та інші.

Нормативно-правове забезпечення управління фінансово-економічною безпекою займає вагоме місце в механізмі управління підприємства, і

передбачає наявність концепції забезпечення фінансово-економічної безпеки, яка виступає основою для розробки та реалізації стратегії фінансово-економічної безпеки та прийняття управлінських рішень у цій сфері. Концепція забезпечення фінансово-економічної безпеки конкретного підприємства має довільну форму, але вміщує головні положення щодо формування та організації управління фінансово-економічною безпекою підприємства.

Важливим елементом механізму управління фінансово-економічної безпеки підприємства є *інформаційно-аналітичне забезпечення,* яке має містити наступні дані: якісні і кількісні значення індикаторів фінансово-економічної безпеки, наявність або потенційність ризиків і загроз, формалізовані фінансові інтереси і стан їхньої реалізації, стратегічний план забезпечення фінансово-економічної безпеки підприємства, якісні і кількісні параметри використання фінансових ресурсів, обсяг останніх, а також джерела їх надходження, фінансовий план (бюджет).

Діагностика діяльності підприємства в системі фінансово-економічної безпеки – це системний аналіз середовища його функціонування за допомого взаємозалежних та взаємодоповнюючих показників, які відображають стан використання потенціалу підприємства та оцінку рівня безпеки. Результати діагностики є основою прийняття відповідних управлінських рішень.

Технологія і техніка управління. Технологія управління – це безупинний творчий процес підтримки стійкого режиму функціонування системи шляхом прийняття і реалізації господарських рішень. До цього процесу зводиться вся діяльність менеджера організації як суб’єкта управління своєї системи. Сукупність різних технічних засобів, призначених для оснащення розумової праці з керування виробництвом, являє собою *техніку управління.*

Найважливішим завданням проектування технічного забезпечення служби управління є вибір технічних засобів з урахуванням витрат на їхнє придбання і використання для виконання конкретного виду робіт (однофункціональні і багатофункціональні технічні засоби).

Тема 4 Нормативно-правове та інформаційно-аналітичне забезпечення фінансово-економічної безпеки підприємства

План лекції

4.1 Нормативно-правове забезпечення фінансово-економічної безпеки підприємства

4.2 Інформаційно-аналітичне забезпечення фінансово-економічної безпеки підприємства

4.1 Нормативно-правове забезпечення фінансово-економічної безпеки підприємства

За сучасних умов правове регулювання безпеки підприємницької діяльності набуває важливого значення. Нормативно-правова база системи безпеки фірми представлена різними інституціональними рівнями: міжнародним, національним, локальним:

міжнародний – міжнародні нормативні акти і угоди, прийняті міжнародними організаціями, союзами держав і нарадами (ООН, ЄС, СНД, ін.), міждержавні угоди (Україна і інші країни), нормативні акти окремих держав;

національний – кодекси та закони України, укази президента України, постанови Верховної Ради України, постанови Кабінету Міністрів України, нормативні акти місцевих органів влади;

локальний – статут фірми, положення фірми, які регулюють режим її діяльності, накази і розпорядження президента (директора) фірми, службові інструкції тощо.

З точки зору послідовного застосування принципу законності, в організації системи безпеки підприємства вирішальне значення має *національне законодавство*. Підприємство для захисту власних економічних інтересів може використовувати велику низку законів та інших державних нормативних актів. Передусім це – Конституція України, норми якої є нормами прямої дії. З точки

зору економічної безпеки, важливе значення має ст. 13 Конституції України, яка гарантує рівність прав суб'єктів права власності і господарювання, а ст. 42 забезпечує захист конкуренції у підприємницької діяльності, обмежує монопольну діяльність.

Широке коло питань економічної безпеки суб'єкта господарювання забезпечується Кодексами України: Цивільним, Кримінальним, Господарським, Податковим, Про працю, Морським, Повітряним та ін.

Більшість положень Конституції України і кодексів більш детально визначено окремими законами. З точки зору економічної безпеки фірми, в першу чергу, важливе значення мають наступні Закони України: Про власність; Про захист економічної конкуренції; Про зовнішньоекономічну діяльність; Про інформацію; Про науково-технічну інформацію; Про авторське право і суміжні права; Про охорону прав на знаки для товарів і послуг; Про охорону прав на промислові зразки; Про охорону прав на винаходи і корисні моделі тощо.

Основними функціями держави в контексті регулювання питань фінансово-економічної безпеки суб'єктів підприємництва в Україні є: захист прав власності, забезпечення вільного підприємництва, стимулювання ділової активності, боротьба з монополістичними тенденціями, забезпечення законності та правопорядку в господарській сфері, регулюванні грошового обігу, зовнішньоекономічній діяльності. Окрім указаних вище функцій, пов'язаних з питаннями фінансово-економічної безпеки суб'єктів підприємництва, держава виконує ще сертифікацію, стандартизацію, патентування, квотування, тощо.

З метою системного підходу до захисту економічних інтересів у 1997 р. Верховною Радою України було прийнято *Концепцію національної безпеки України*. У прийнятій Концепції розглядалися основи національної безпеки України, об'єкти та принципи забезпечення національної безпеки, загрози національній безпеці, основні напрями державної політики національної безпеки України та система національної безпеки України. Ця концепція не

здійснює прямого впливу на фінансово-економічну безпеку суб'єктів підприємництва, але опосередкований вплив має.

Також, Верховна Рада України ухвалила *Закон України «Про основи національної безпеки України»*, який набрав чинності з 30 липня 2003 року. Окремо фінансову безпеку цей Закон не визначає, однак наведено деякі ознаки утворення рівня фінансової безпеки суб`єктів підприємництва, а саме: критичний стан основних виробничих фондів у провідних галузях промисловості, агропромисловому комплексі.

Деякі аспекти, що стосуються фінансової безпеки суб'єктів підприємництва висвітлює *Господарський кодекс України*. Забезпечення фінансової безпеки держави, підприємства визначається V розділом Бюджетного кодексу України – «Контроль за дотриманням бюджетного законодавства та відповідальність за бюджетні правопорушення».

Окремі питання регулювання фінансової безпеки підприємств висвітлені у *Податковому кодексі України*.

Суспільні відносини, пов'язані з забезпеченням безпеки бізнесу, регулюють також Закони України: «Про цінні папери і фондову біржу», «Про захист від недобросовісної конкуренції», «Про інвестиційну діяльність», «Про підприємства в Україні» та ін.

З існуючих законодавчих актів найбільше уваги приділяється питанням банкрутства підприємств. Нині з урахуванням усіх поправок та змін *Закон України «Про відновлення платоспроможності боржника або визнання його банкрутом»* встановлює умови, порядок відновлення платоспроможності суб'єкта підприємницької діяльності-боржника або визнання його банкрутом і застосування ліквідаційної процедури, повного або часткового задоволення вимог кредиторів. Цей закон дає визначення ряду термінів: неплатоспроможність, боржник, банкрутство, суб'єкт банкрутства (банкрут), кредитор, конкурсні кредитори, поточні кредитори, грошове зобов'язання, безспірні вимоги кредиторів, досудова санація, розпорядження майном

боржника, розпорядник майна, санація, реструктуризація підприємства, керуючий санацією, арбітражний керуючий, мирова угода.

Держава здійснює найбільш помітний і значний вплив на формування фінансово-економічної безпеки підприємства. Використовуючи прямі і непрямі важелі втручання, вона створює і регулює економічні умови діяльності підприємств, які призначені для захисту економічних інтересів держави і його національної економіки. *Метою державного регулювання* є досягнення ефективного механізму взаємодії підприємств, фірм – міжфірмові відносини повинні сприяти зростанню випуску, встановленню прийнятної ціни на товар, підвищенню якості товару і відповідної продуктової диференціації, стабільності ринку.

Право підприємства на забезпечення економічної безпеки, захист комерційної таємниці повинно бути відображено в *Статуті.* У вступу до Статуту фірми, або спеціальній частині, треба оголосити, що фірма на підставі Господарського кодексу України (ст. 20.2; 44), Цивільного кодексу України (ст. 19) здійснює комплекс заходів для захисту власних інтересів, майна і працівників. Особливим пунктом повинно бути визначено право фірми на захист комерційної таємниці, згідно зі статтею 36 Господарського кодексу України. Ці статутні положення конкретизуються спеціальними *Положеннями про систему безпеки фірми.* В цьому документі визначаються завдання системи безпеки фірми, її функціональна і організаційна структура, субординація працівників системи безпеки, їх функції, права і обов’язки та відповідальність згідно з чинним законодавством країни.

Положення про систему безпеки фірми має більш конкретний характер, ніж Статут, але воно також не охоплює усіх особливості захисту від небезпек за окремими напрямками. Структура Положення про систему безпеки фірми має наступні складові частини: загальні положення, основні задачі системи безпеки, функції системи безпеки фірми, права і обов’язки працівників системи безпеки фірми, структура системи безпеки, режим безпеки фірми. відповідальність. Для регулювання процесу захисту згідно з структурою системи безпеки (наприклад,

охорона майна, персональна охорона, технологічний захист, комп'ютерний захист тощо) працівниками визначених структурних підрозділів розробляються окремі документи, що регулюють процес захисту. Це можуть бути окремі внутрішні нормативні акти.

4.2 Інформаційно-аналітичне забезпечення фінансово-економічної безпеки підприємства

Для того щоб оцінити рівень фінансово-економічної безпеки підприємства та якісно нею управляти, необхідно перш за все мати достовірну інформацію щодо фінансово-економічної діяльності підприємства. Тому постає проблема інформаційно-аналітичного забезпечення фінансово-економічної безпеки підприємства. Достовірні інформаційно-аналітичні матеріали дають можливість: по-перше, налагодити постійний моніторинг стану фінансово-економічної безпеки підприємства; по-друге, оцінювати рівень фінансово-економічної безпеки; по-третє, аналізувати та визначати чинники впливу на той чи інший стан фінансово-економічної безпеки.

Інформаційна база фінансово-економічної безпеки, яка існує на підприємстві, становить систему показників, вірогідність, періодичність поновлення. Її повнота й автоматизація забезпечує якість прийнятих управлінських рішень.

Інформаційне забезпечення фінансової діяльності відображає інформацію про стан суб'єкта господарювання на будь-який момент часу і з будь-яким ступенем деталізації, а також враховує показники зовнішнього середовища підприємства. Основними властивостями інформації є: повнота, вірогідність, цінність, актуальність та зрозумілість.

Створення раціонального потоку інформації про фінансово-економічну безпеку підприємства повинне опиратися на такі принципи: *уніфікованості* – припускає те, що аналітики повинні прагнути до того, щоб проектні рішення, які ними пропонуються, підходили до якомога ширшого кола завдань, які

вирішуються; *системності* – припускає встановлення порядку функціонування всієї системи аналітичної інформації в цілому і її динамічних тенденцій; *принцип вирішення нових завдань* – дозволяє виявляти й вирішувати нові завдання, які ставляться перед підприємством у зв'язку з ускладненням зовнішнього середовища; *принцип першого керівника* – заснований на безпосередньому керівництві аналітичною роботою на підприємстві першим керівником у зв'язку з тим припущенням, що він буде постійно націлювати аналітичний відділ на рішення нових більш складних завдань і намагатися вивести підприємство на лідируючі положення в конкурентному середовищі; *принцип розвитку* – розроблений комплекс вирішення аналітичних завдань повинен створюватися з урахуванням можливості поповнення й постійної актуалізації без порушення його функціонування; *принцип сумісності* – при створенні системи повинні бути реалізовані інформаційні інтерфейси, завдяки яким вона може взаємодіяти з іншими системами відповідно до встановлених правил; *принцип стандартизації* – припускає, що при створенні аналітичних комплексів повинні бути раціонально застосовані типові уніфіковані й стандартизовані елементи, проектні рішення, пакети прикладних програм, зокрема такі, які дозволяють займатися побудовою економіко-математичних моделей; *принцип ефективності* – полягає у досягненні раціонального співвідношення між витратами й цільовими ефектами, включаючи кінцеві результати автоматизації; *принцип єдиної інформаційної бази* – припускає, що вихідна інформація один раз вводилась в систему й могла бути використана багаторазово.

До збору, накопичення й систематизації інформації висуваються певні вимоги: інформація повинна бути повною й своєчасною, достовірною, корисною й зручною для сприйняття й подальшого використання.

Для аналітичної обробки отриманих даних щодо індикаторів фінансово-економічної безпеки підприємства і чинників, що впливають на її стан, використовуються *методи економічного аналізу*, а саме, кореляційного та регресійного аналізу, прямих розрахунків показників тощо.

Для поглиблення аналізу впливу на стан фінансово-економічної безпеки підприємства чинників або загроз, особливо нових, потрібна додаткова інформація, яка потребує нетрадиційних джерел та її аналітична обробка. Такими джерелами можуть бути *спеціальні обстеження фінансової діяльності* конкретного підприємства, проведення зовнішніми спеціалізованими фірмами *аудиту* його комерційної діяльності, дані результатів *соціологічного обстеження* тощо.

Метою інформаційно-аналітичного забезпечення фінансової безпеки підприємства є її підтримання на належному рівні, а завданнями – наведені у постановці проблеми.

Система показників для проведення фундаментальних аналітичних досліджень економічної безпеки повинна враховувати такі *вимоги до їх формування:* у систему повинні входити декілька окремих показників і один узагальнюючий, залежний від окремих; загальнотеоретична інтерпретація, взаємозв'язок і цілеспрямованість як окремих показників, їх груп, так і всієї системи в цілому; для системи повинна бути характерною інтегрованість, що дозволяє застосовувати її у програмно цільовому управлінні економічною безпекою й будувати «дерево» цілей економічного й соціального розвитку підприємства; можливість регуляції значень величини показників залежить від досягнутого рівня економічної безпеки та наявності потенціалу її досягнення в майбутньому; наявність достатньої кількості показників для оцінки окремих функціональних складових економічної безпеки підприємства; усі показники в системі повинні бути реальними й динамічними; можливість одержання прогнозу про спрямованість динаміки показників; показники повинні бути значущими (найбільш важливими для дослідження економічної безпеки); у системі показників, які використовуються при проведенні оцінки та аналізу економічної безпеки підприємства, необхідно враховувати галузеві особливості підприємства, його конкурентну стратегію та стадію життєвого циклу, на якому воно знаходиться.

Процес підготовки матеріалу до аналізу фінансово-економічної безпеки підприємства включає також приведення показників у порівняльний вид і спрощення цифрового матеріалу. Найпоширенішими прийомами приведення показників у порівняльний вид є: нейтралізація ціннісного фактора шляхом відображення різних видів об'ємних показників у єдиних цінах; нейтралізація кількісного фактора при аналізі ефективності використання будь-якого виду ресурсу за допомогою розрахунку ряду умовних показників, де незмінним залишається об'ємний показник і послідовно змінюється величина ресурсу, що витрачається; нейтралізація впливу на рівень кількісних і якісних показників методик їх розрахунку. Сукупність однорідних планових, звітних і облікових показників повинна мати єдину методику визначення; вирахування середніх величин при вивченні ряду однорідних показників; заміна абсолютних величин відносними, коли це найбільш доцільно, для більшої наочності, доступності й сприйняття.

Слід використовувати *дві групи показників* фінансово-економічної безпеки підприємства: перша – характеризує власне стан фінансово-економічної безпеки станом на певний час; друга – характеризує сукупність чинників, котрі впливають на рівень фінансово-економічної безпеки.

Джерелами інформації для визначення і моніторингу стану фінансово-економічної безпеки підприємства є дані бухгалтерського, оперативного та статистичного обліку і звітності.

Для аналізу впливу зовнішніх чинників на стан фінансово-економічної безпеки слід використовувати дані управлінського і маркетингового аналізу, які мають проводитися на кожному підприємстві, інформацію спеціалізованих консалтингових фірм, статистичні дані по регіонах, країні в цілому, вибіркові статистичні та аналітичні дослідження по галузях і групах підприємств, котрі проводяться органами державної статистики.

Формування системи інформаційного забезпечення є цілеспрямованою дією, що пов`язана з підбором інформативних показників для аналізу, планування та управління фінансовою діяльністю. Такі показники формуються

із використанням зовнішніх та внутрішніх джерел інформації, що представлені на рис. 4.1.

Рисунок 4.1 – Складові інформаційної бази фінансової діяльності

Ці показники мають досить великий вплив на ефективність регулювання і управління фінансовою діяльністю підприємства, на якість інформаційної бази, але, мають бути доповнені певними показниками *статистичної і податкової звітності*.

Статистичні показники – характеризують інноваційну діяльність підприємства. До них відносяться: рівень освоєння нових видів інноваційної продукції у загальній кількості видів продукції, рівень впровадження нових

технологічних процесів, структура витрат за типами інновацій, питома вага витрат на технологічні інновації, рівень прогресивності реалізованої прогресивної продукції. Зіставлення запропонованих показників за періодами надає змогу виявляти тенденції їх динаміки й приймати управлінські рішення щодо інноваційного розвитку підприємства. *Показники податкової звітності* використовуються для планування податків. Наприклад, показники для розрахунку сум податків, які підлягають сплаті в плановому періоді, та показники податкового планування, що дозволять мінімізувати суми податків засобами, що не суперечать законодавству. *Показники управлінської звітності* мають нерегламентований характер, але впливають на прийняття управлінських рішень, повинні наочно представляти їх динаміку за окремими напрямами.

Інформаційна база підприємства формується не тільки на основі інформації про показники діяльності, але й інших інформаційних ресурсів. Необхідним є пошук додаткових, *нетрадиційних джерел інформації* та її аналітична обробка. Такими джерелами є: спеціальні обстеження фінансової діяльності конкретного підприємства; проведення зовнішніми спеціалізованими фірмами аудиту його комерційної діяльності; дані результатів соціологічного обстеження; науково-технічна інформація (власні і цільові дослідження, конференції, ярмарки); Інтернет-ресурси – Інтернет-торгівля, Інтернет-реклама, Інтернет-Біржі, Інтернет-банкінг, Інтернет-інвестування.

Доцільно також систему інформаційно-аналітичного забезпечення доповнити *прогнозуванням*, що сприяє розв’язанню таких задач: визначення фінансової складової місії та завдань підприємства, а також пов’язаних з цим фінансових інтересів на певний період; оцінка цілей забезпечення фінансово-економічної безпеки підприємства; передбачення можливих шляхів розвитку внутрішніх і зовнішніх загроз безпеці підприємства та їхніх негативних наслідків; оцінка можливого рівня впливу позитивних і негативних чинників на майбутній розвиток фінансової діяльності підприємства тощо. Наявність прогнозування у складі системи інформаційно-аналітичного забезпечення

дозволяє більш системно забезпечити необхідний рівень фінансової діяльності підприємства в поточному та перспективному періодах.

Для розробки ефективно функціонуючої системи інформаційно-аналітичного забезпечення фінансово-економічної безпеки підприємства слід визначитися з її критеріями та показниками, на основі яких здійснювати якісну та кількісну оцінку стану фінансової безпеки підприємства, а також чинників, що впливають на її стан.

Критерієм фінансово-економічної безпеки є основний фінансовий результат діяльності підприємства, що відображає всі сторони його функціонування: науково-технічну, виробничу, маркетингову, інформаційну, кадрову тощо (наявність прибутку). Обґрунтування критеріальних вимог до фінансово-економічної безпеки діяльності підприємств має бути визначеним у системі певних *індикаторів*, тобто елементів, які віддзеркалюють кількісні й якісні характеристики стану та ходу процесу об'єкта спостережень.

Індикатори фінансово-економічної безпеки підприємства мають бути водночас показниками стану фінансової діяльності підприємства, тобто входити до її складу, оскільки відображають певний стан фінансово-економічної безпеки і повністю базуватися на показниках фінансово-економічної діяльності. Для більшості таких показників можуть бути визначені критичні та нормальні значення. *Критичне значення* визначає мінімально припустимий рівень безпеки, подолання якого означає перехід підприємства в зону діяльності, що характеризується неефективним використанням корпоративних ресурсів і виникненням негативних впливів різного типу.

Теоретично характеристики індикаторів фінансово-економічної безпеки мають відповідати таким *ознакам:* вимірюваності (піддаватися кількісному вимірюванню); обґрунтованості віддзеркалення оцінюваного параметра; однозначності (наявності чіткого, загальноприйнятого визначення); стабільності у часі (наявність динамічних зрізів даних за індикатором);

доступності даних, необхідних для розрахунку (традиційних джерел інформації).

Вибір індикаторів для оцінювання фінансової безпеки підприємства – складний процес і, крім узагальнених вимог, має відповідати особливостям функціонування підприємства: стратегічній меті підприємства; стадії життєвого циклу підприємства; специфічним й індивідуальним особливостям загроз фінансовій безпеці з боку кожного окремого підприємства.

В практичній діяльності підприємств застосовують такі наукові підходи до оцінки фінансової безпеки підприємства:

1) індикаторний – передбачає порівняння фактичних значень показників фінансової безпеки з пороговими значеннями індикаторів її рівня. Під пороговими значеннями індикаторів фінансової безпеки розуміють їх граничні величини, недотримання яких призводить до формування негативних тенденцій (виникнення загроз) у сфері фінансової безпеки. За такого підходу найвищий рівень фінансової безпеки підприємства досягається за умови, що вся сукупність індикаторів знаходиться в межах порогових значень, а порогове значення кожного з індикаторів досягається не на шкоду іншим. Недоліком у використанні цього підходу є те, що оцінка фінансової безпеки залежить від визначення порогових значень, котрі, у свою чергу, є плинними в залежності від стану зовнішнього середовища, до якого підприємство має пристосовуватися і на який майже не може впливати.

2) ресурсно-функціональний – передбачає оцінку стану фінансової безпеки на основі оцінки рівня використання фінансових ресурсів, а також оцінку рівня виконання функцій – забезпечення фінансової ефективності діяльності підприємства, його фінансової стійкості та незалежності. Такий підхід є найбільш вживаним, адже фінансова безпека оцінюється на базі сукупного критерію, що визначається з урахуванням усієї діяльності підприємства. Порядок визначення показників фінансової безпеки підприємства за її окремими функціональними підсистемами (складовими) такий:

а) рівень безпеки за бюджетною складовою $\mathbf{I_{бж}}$ можна оцінити такими показниками:

часткою податків і зборів, які сплачуються з прибутку підприємства у сумі прибутку – $\mathbf{К_{п.з}}$:

$$К_{п.з} = (П_р - ПЗ) : П_р,$$

де: $П_р$ – прибуток підприємства;

ПЗ – сума сплачених з прибутку податків і зборів.

Тоді – ($П_р$ – ПЗ) – це чистий прибуток підприємства. Цей коефіцієнт при зменшенні ПЗ прямує до 1;

часткою бюджетних кредитів (бюджетного фінансування) у сумі оборотних коштів (власних і позикових) – $\mathbf{К_{б.к.}}$:

$$К_{б.к} = (ОК - БК) : ОК,$$

де: ОК – сума оборотних коштів (власних і позикових);

БК – величина бюджетних кредитів (бюджетного фінансування).

Коефіцієнт $\mathbf{К_{б.к}}$ за умови зменшення величини бюджетних кредитів (бюджетного фінансування) прямує до 1.

відношенням кредиторської заборгованості бюджету з податків і зборів – $\mathbf{К_{з.б}}$**:**

$$К_{зб} = (ОК - ЗБ) : ОК,$$

де: ЗБ – величина кредиторської заборгованості бюджету.

Коефіцієнт $\mathbf{К_{зб}}$ за умови зменшення кредиторської заборгованості бюджету також прямує до 1.

Математичне виведення загального індикатора $\mathbf{I_{бж}}$ через часткові коефіцієнти передбачає врахування їхніх вагових часток **а** за формулою:

$$I_{б.ж} = К_{п.з} \times a_{п.з.} + К_{б.к} \times a_{б.к} + К_{з.б} \times a_{з.б.}.$$

Вагові частки кожного з коефіцієнтів можна визначати експертним шляхом з врахуванням їхньої пріоритетності.

б) рівень безпеки за грошово-кредитною складовою $\mathbf{I_{г.к.}}$ можна оцінювати за такими показниками:

часткою короткострокових кредитів (у тому числі в іноземній валюті у перерахунку в національну) у покритті нестачі власних оборотних коштів – $\mathbf{К_{кр}}$:

$$К_{кр} = [ОК_п - (ОК_п - ОК_{кр})] : (ОК_п - ОК_в),$$

де: $ОК_п$ – потреба підприємства в оборотних коштах для здійснення операційної діяльності,

$ОК_{кр}$ – сума отриманих короткострокових кредитів для поповнення відсутніх для здійснення операційної діяльності оборотних коштів,

$ОК_в$ – наявність власних оборотних коштів;

наявністю заборгованості заробітної плати працівникам – $\mathbf{К_{зп}}$:

$$К_{з.п} = (Ф_{о.п.} - З_{з.п.}) : Ф_{о.п.},$$

де: $Ф_{о.п.}$ – фонд оплати праці,

$З_{зп}$ – заборгованість з заробітної плати;

співвідношенням кредиторської та дебіторської заборгованості (чиста заборгованість) – $\mathbf{К_{с.к.д.}}$:

$$К_{с.к.д} = [КЗ - (КЗ - ДЗ)] : КЗ,$$

де: КЗ – обсяг кредиторської заборгованості,

ДЗ – обсяг дебіторської заборгованості.

Цей індикатор показує рівень непокриття кредиторської заборгованості підприємства дебіторською.

Формула має економічний сенс лише за умови КЗ > або = ДЗ.

При КЗ < ДЗ коефіцієнт $К_{с.к.д}$ приймається рівним 1.

Загальний індикатор $\mathbf{I_{г.к.}}$ визначається через часткові коефіцієнти і передбачає врахування їхніх вагових часток **а** за формулою:

$$I_{г.к.} = К_{кр} \times а_{кр} + К_{з.л} \times а_{зп} + К_{с.к.д} \times а_{с.к.д.} .$$

Вагові частки кожного з коефіцієнтів також доцільно визначати з врахуванням їхньої пріоритетності експертним шляхом;

в) рівень безпеки за валютною підсистемою $\mathbf{I_{в.}}$ можна визначати за такими показниками:

часткою обсягу продажів за рахунок експортно-імпортних операцій у загальному обсязі продажів – $\mathbf{К_{е\text{-}і}}$:

$$К_{е\text{-}і} = ОП_{е\text{-}і} : ОП,$$

де: $ОП_{е\text{-}і}$ – обсяг продажів з експортно-імпортних операцій,

ОП – загальний обсяг продажів.

співвідношенням кредиторської та дебіторської заборгованості з експортно-імпортних операцій – $\mathbf{К_{к.д.е\text{-}і}}$:

$$К_{к.д.е\text{-}і} = [КЗ_{е\text{-}і} – (КЗ_{е\text{-}і} - ДЗ_{е\text{-}і})] : КЗ_{е\text{-}і},$$

де: $КЗ_{е\text{-}і}$ – обсяг кредиторської заборгованості з експортно-імпортних операцій,

$ДЗ_{е\text{-}і}$ – обсяг дебіторської заборгованості з експортно-імпортних операцій.

Цей індикатор показує рівень непокриття кредиторської заборгованості підприємства дебіторською.

Формула має економічний сенс лише за умови $\mathbf{КЗ_{е\text{-}і}}$ > **або** = $\mathbf{ДЗ_{е\text{-}і}}$.

При $\mathbf{КЗ_{е\text{-}і}}$ < $\mathbf{ДЗ_{е\text{-}і}}$ коефіцієнт $\mathbf{К_{к.д.е\text{-}і}}$ приймається рівним 1.

Загальний індикатор $\mathbf{І_в}$ визначається через часткові коефіцієнти і передбачає врахування їхніх вагових часток **а** за формулою:

$$І_{в.} = К_{е\text{-}і} \times а_{е\text{-}і} + К_{к.д.е\text{-}і} \times а_{к.д.е\text{-}і},$$

Вагові частки кожного з коефіцієнтів також можна визначати експертним шляхом з врахуванням їхньої пріоритетності;

г) рівень безпеки за банківською складовою $\mathbf{І_{б.н}}$ можна визначати за співвідношенням обсягів кредитів і депозитів по даному підприємству:

$$І_{б.н} = Д_п : К_р,$$

де: $Д_п$ – обсяг внесених підприємством у банк депозитів,

$К_р$ – загальний обсяг отриманих з банку кредитів (коротко- і довгострокових). Якщо $Д_п > К_р$ то значення показника $І_{б.н}$ приймається рівним **1**;

д) рівень безпеки за інвестиційною складовою $\mathbf{I_i}$. можна визначити за відношенням капітальних вкладень (інвестицій) до обсягу основного капіталу підприємства:

$$I_i = КВ : К_о,$$

де: КВ – капітальні вкладення у розвиток підприємства,

$К_о$ – основний капітал;

ж) рівень безпеки за фондовою підсистемою $\mathbf{I_ф}$ доцільно розраховувати за формулою:

$$I_Ф = В_а : К_о \text{ x } К_а : К_0,$$

де: $В_а$ – обсяг випущених акцій з метою зростання основного капіталу,

$К_а$ – обсяг придбаних акцій для зростання основного капіталу.

з) рівень безпеки за страховою складовою $\mathbf{I_c}$ доцільно визначати за такими показниками:

часткою застрахованого майна в основному капіталі – $К_{с.м}$:

$$К_{с.м} = М_с – К_о,$$

де: $М_с$ – обсяг застрахованого майна.

часткою застрахованого прибутку в загальному прибутку – $К_{с.п}$:

$$К_{с.п} = П_с : П_з,$$

де $П_с$ – обсяг застрахованого прибутку,

$П_з$ – загальний обсяг прибутку.

співвідношенням страхових платежів по страхуванню від нещасних випадків і захворювань до фонду оплати праці – $К_{сн}$:

$$К_{с.н} = Б_с : ФОП,$$

де: $Б_с$ – обсяг страхових платежів по нещасних випадках і захворюваннях,

ФОП – фонд оплати праці підприємства.

Загальний індикатор $\mathbf{I_c}$ визначається через часткові коефіцієнти і передбачає врахування їхніх вагових часток **а** за формулою:

$$I_c = К_{с.м} \text{ x } а_{см} + К_{с.п} \text{x } а_{сп} + К_{с.н} \text{ x } а_{сн}.$$

Вагові частки кожного з коефіцієнтів можна визначати з врахуванням їхньої пріоритетності експертним шляхом.

Інтегральний показник фінансової безпеки підприємства можна розраховувати за наступною формулою:

Іфбп=Ібж х bбж + Ігк х bгк + Ів х bв + Ібн х bбн + Іі х bі + Іф х bф + Іс х bс,

де: bбж, bгк**,** bв, bбн, bі, bф, bс – вагові коефіцієнти відповідно бюджетної, грошово-кредитної, валютної, банківської, інвестиційної, фондової і страхової складових фінансової безпеки підприємства. Їхня сума має дорівнювати **1**.

На конкретних підприємствах у той чи інший час можуть бути включені до фінансової діяльності не всі наведені вище функціональні підсистеми або їхні частки. У такому разі індикатор по цій складовій або її частці буде дорівнювати **0**;

3) за критерієм мінімізації сукупного збитку, який наноситься безпеці – передбачає застосування експертних оцінок і обмежений складними розрахунками через відсутність необхідних для оцінки фінансової безпеки підприємства бухгалтерських і статистичних даних, адже потребує ведення додаткового обліку;

4) за критерієм достатності оборотних коштів для здійснення господарської діяльності – має досить обмежене використання для оперативної оцінки фінансової безпеки підприємства.

Для оперативних цілей здійснення моніторингу стану фінансової безпеки підприємства (щоденного, тижневого, декадного аналізу) доцільно ввести і використовувати таке поняття як *діапазон (оперативний резерв) фінансової безпеки.* Його можна розраховувати за наступною формулою:

$$Р_{Ф.Б} = (ОП_{П} – ОП_{Т.БЗ}) : ОП_{П},$$

де: $ОП_{П}$ – прогнозований обсяг продажів,

$ОП_{ТБЗ}$ – обсяг продажів, який відповідає точці беззбитковості.

Окрім цього, для оцінки фінансово-економічної безпеки використовуються *комплексні моделі* оцінки її рівня.

Для експрес-аналізу рівня фінансової безпеки підприємства можна використати підхід із використанням бальних оцінок, так званий *метод балів.*

Оскільки рівень фінансово-економічної безпеки підприємства не може бути визначений лише наявністю власних та довгострокових джерел формування запасів, її оцінку здійснюють також на основі аналізу показників, які характеризують платоспроможність, фінансову стійкість, ефективність господарської діяльності і ділову активність підприємства тощо.

Тема 5 Організаційне забезпечення фінансово-економічної безпеки підприємства

План лекції

5.1 Організаційна структура управління безпекою установи

5.2 Процедура створення та ліквідації служби безпеки підприємства

5.3 Управління службою безпеки підприємства

5.4 Структура служби безпеки великих підприємств і корпорацій

5.1 Організаційна структура управління безпекою установи

Завдання гарантування безпеки підприємства є одним з основних, пріоритетних завдань, що стоять перед усіма структурними ланками і всіма працівниками підприємства, так само як і завдання збільшення прибутку, підвищення власного добробуту. Ефективний захист економічних інтересів фірми може бути забезпечений лише у разі об’єднання зусиль її персоналу: адміністрації, інженерно-технічних працівників, службовців, робітників.

Підприємство як система має певні структурні ланки: дирекцію – керівництво підприємства; бухгалтерію; відділи – функціональні ланки підприємства; допоміжні служби; службу безпеки.

Служба безпеки (СБ) фірми – це самостійний структурний підрозділ. Вона вирішує завдання безпосереднього забезпечення захисту життєво

важливих інтересів фірми в умовах комерційного і підприємницького ризику, конкурентної боротьби. На великих і середніх підприємствах (в організаціях) звичайно створюються автономні служби безпеки, а безпеку функціонування невеликих фірм можуть гарантувати територіальні (районні або міські) служби за договорами найму одного чи кількох охоронців. Такі служби охорони зазвичай створюються при місцевих органах внутрішніх справ або при державній службі безпеки.

Служба безпеки як відділ підприємства вирішує завдання: організації захисту економічних інтересів на підприємстві; гарантування безпеки спеціальними засобами і методами. Виконуючи організаційну функцію, служба безпеки працює у взаємодії з дирекцією і відділами (функціональними ланками) підприємства.

Служба безпеки *спільно з дирекцією* забезпечує: ухвалення правильних управлінських рішень (забезпечує керівництво інформацією, веде аналітичну роботу); управління системою безпеки (консультує керівництво з питань захисту економічних інтересів); створення режиму збереження комерційної таємниці (розробляє правила, що забезпечують його дотримання); надання допомоги і здійснення контролю за діяльністю всіх функціональних ланок підприємства.

Служба безпеки *спільно з відділами* забезпечує: здійснення комерційних операцій (бере участь у підготовці контрактів, перевіряє надійність партнерів, відстежує виконання взятих ними зобов’язань); підбір, перевірку і підготовку персоналу; навчання персоналу прийомів поведінки і правил спілкування, формування загальної і особистої зацікавленості, уваги та пильності.

Служба безпеки самостійно працює спеціальними засобами і методами: у середовищі працівників підприємства; у середовищі партнерів і конкурентів підприємства.

Організаційна структура підсистеми безпеки організації може бути різною залежно від виду підприємства (банк, фірма), його розмірів, власності тощо. Структура, чисельність і склад служби безпеки визначаються реальними

потребами фірми і ступенем конфіденційності її інформації. Залежно від розмірів і потужності організації її безпека і захист інформації можуть бути гарантовані по-різному: від абонементного обслуговування силами приватних охоронних і детективних структур до розгортання повномасштабної власної служби і системи безпеки з розвиненою структурою і штатною чисельністю.

У своїй діяльності *служба безпеки керується*: інструкцією з організації режиму і охорони; інструкцією щодо захисту комерційної таємниці; переліком відомостей, що становлять комерційну таємницю; інструкцією щодо роботи з конфіденційною інформацією для керівників, фахівців і технічного персоналу; інструкцією щодо організації зберігання справ, що містять конфіденційну інформацію, в архіві; інструкцією щодо інженерно-технічного захисту інформації; інструкцією про порядок роботи з іноземними представниками і представництвами та ін.

Служба безпеки будь-якої фірми постійно виконує певний комплекс завдань. Головними з них для будь-якої фірми є такі: 1) гарантування безпеки виробничо-господарської діяльності та захисту відомостей, що вважаються комерційною таємницею фірми (підприємства, організації); 2) організація роботи з правового та інженерно-технічного захисту комерційної таємниці фірми; 3) запобігання необґрунтованому допуску й доступу до відомостей та робіт, які становлять комерційну таємницю; 4) організація спеціального діловодства, яке унеможливлює несанкціоноване одержання відомостей, віднесених до комерційної таємниці відповідної фірми; 5) виявлення і локалізація можливих каналів витоку конфіденційної інформації в процесі звичайної діяльності та в екстремальних ситуаціях; 6) забезпечення режиму безпеки за здійснення всіх видів діяльності, зокрема зустрічі, переговори й наради у рамках ділової співпраці фірми з іншими партнерами; 7) забезпечення охорони приміщень, устаткування, офісів, продукції і технічних засобів, необхідних для виробничої або іншої діяльності; 8) забезпечення особистої безпеки керівництва та провідних менеджерів і спеціалістів фірми; 9) оцінка маркетингових ситуацій та неправомірних дій конкурентів і зловмисників.

5.2 Процедура створення та ліквідації служби безпеки підприємства

Для створення служби безпеки керівництво і менеджери повинні насамперед розпочати створення її системи безпеки, визначити структурні варіанти іі перспективи її розвитку. Але передусім треба визначити можливості: використання служб охорони за контрактом; створення власної служби безпеки; залучення допомоги державних служб охорони; протидії загрозам з боку терористів; протидії загрозам вибухів, комп'ютерним злочинам; використання спецтехніки (відео- та інших оперативних систем охорони різних суб'єктів і об'єктів, спеціальних технічних засобів охорони периметра об'єкта, систем охоронного устаткування і центрального управління тощо.

Вирішивши створити власну службу безпеки, підприємець передусім повинен звернутися до експертів у галузі організації сучасної системи безпеки недержавного підприємства з проханням провести дослідження цієї проблеми і підготувати пакет документів, що визначають програму і функціонування системи безпеки підприємства. Краще це можуть зробити професійно підготовлені менеджери з безпеки.

У процесі організації комплексної системи безпеки господарюючого об'єкта особливу увагу слід звертати на таке: здатність розробити програму, адекватну специфічним потребам захисту об'єкта; ступінь надійності працівників підприємства; вартість програми захисту об'єкта; ступінь надійності захисту об'єкта; достатня ефективність витрат на програму діяльності; рівень загальної відповідальності адміністрації; здатність програм гарантування безпеки відповідати вимогам; страхові премії як результат виконання програми; здатність модернізувати систему безпеки відповідно до сучасних вимог; здатність прищепити працівниками підприємства відчуття корпоративності; надійність виробника спеціального обладнання, яке використовується для захисту об'єкта; засоби впливу на громадську думку на користь вирішення проблем безпеки об'єкта.

Не менше значення для керівників служби безпеки має кадрове

забезпечення її діяльності. Роботу цю умовно можна поділити на два етапи. *На першому етапі* відбирають кандидатів для роботи в службі безпеки, перевіряють їх, кандидати проходять спеціальну підготовку і стажування на посаді. При їх відборі особливу увагу приділяють освіті (крім юристів, доцільно запрошувати на роботу також економістів, фінансистів). Крім перевірки органами внутрішніх справ, не зашкодить з'ясувати біографічні та інші дані про кандидата.

Для ефективного функціонування служби безпеки потрібно попередньо опрацювати багато питань. Серед них особливе значення має проектування оргструктури служби безпеки та її ресурсного забезпечення, оскільки без вирішення цих питань її діяльність взагалі неможлива.

Будь-яка оргструктура, навіть найоптимальніша, не зможе дати очікуваних результатів, якщо її не доповнити внутрішніми нормативними актами, що регулюють діяльність усіх підрозділів і співробітників служби безпеки. Причому ці нормативні акти умовно можна поділити на дві групи: 1) ті, що безпосередньо стосуються діяльності самої служби безпеки; 2) ті, що регулюють діяльність інших служб (підрозділів, працівників) підприємства. До першої групи належать: статут служби безпеки, положення про відділи і штаб служби безпеки, положення про групи і сектори служби безпеки, посадові інструкції працівників служби безпеки.

Структура посадової інструкції має такі розділи: загальні положення; функції; посадові обов'язки; відповідальність; взаємини і зв'язки за посадою. Розробляють ці нормативні акти послідовно, починаючи із статуту до посадової інструкції, що дає змогу охопити весь комплекс цілей, завдань і функцій, що вирішуються службою безпеки.

До другої групи внутрішніх нормативних актів, що забезпечують діяльність інших працівників і служб підрозділів підприємства-засновника, належать: договір підприємства з партнером про забезпечення ним заходів безпеки комерційної інформації; інструкція щодо виконавців робіт і документів, що містять комерційну таємницю; зобов'язання про

нерозголошення комерційної таємниці; перелік відомостей, що становлять комерційну таємницю підприємства і основні вимоги до працівників з її захисту; перелік відомостей, які не повинні розголошуватися стороннім особам з метою особистої безпеки працівників підприємства; перелік посадових осіб, уповноважених відносити інформацію до комерційної таємниці; правила віднесення інформації до комерційної таємниці і зняття з її носіїв грифу конфіденційності; правила ведення таємного діловодства; пам'ятка працівникові (службовцеві) про збереження комерційної таємниці підприємства; правила приймання відвідувачів на підприємстві; правила внутрішнього трудового розпорядку і т.ін.

Проте оптимальна оргструктура і повне правове забезпечення служби безпеки самі по собі не забезпечать ефективного функціонування, якщо вона не матиме відповідних ресурсів. Серед них першочергове значення мають фінансові ресурси.

Повне і якісне забезпечення служби безпеки матеріально-технічними ресурсами – не тільки засіб, а й умова підвищення ефективності роботи її працівників. Ці ресурси умовно поділяють на такі групи: зброя і боєприпаси; спеціальні засоби; службові приміщення різного характеру (кабінети, караульні приміщення, збройові кімнати, стрілецькі тири, кімнати огляду); допоміжна техніка (автотранспорт, відео-, кіно-, фототехніка, засоби оперативного радіо- і телефонного зв'язку, комп'ютери тощо); засоби запобігання й захисту (охоронно-пожежна сигналізація, сторожові собаки, охоронне освітлення, телебачення та ін.); засоби забезпечення нормальної діяльності працівників (спецформа, меблі, канцелярське приладдя, медикаменти, бланки документів, юридична і спеціальна література тощо).

Також важливо забезпечити діяльність служби безпеки інформаційними ресурсами. Насамперед слід визначити потребу і обсяги мінімуму інформації, без якої функціонування служби безпеки взагалі неможливе. Таку інформацію можна умовно поділити на три блоки: *до першого блоку «середовище функціонування підприємства»* зазвичай належать відомості про підприємства-

конкуренти, правоохоронні й контрольно-наглядові органи, ринкову кон'юнктуру, криміногенну ситуацію в регіоні, місце розташування підприємства, нормативні акти, що регулюють діяльність підприємства-засновника; *другий блок «стан безпеки в межах підприємства»* містить відомості про: стан злочинності серед персоналу; наявність або відсутність комерційної таємниці; джерела (канали) і суми матеріального збитку, завданого підприємству; аналіз насильницьких злочинів, здійснених проти персоналу; ефективність роботи юрисконсульта (юридичної служби); співробітників підприємства, що мають доступ до конфіденційної інформації і пов'язані зі збереженням товарно-матеріальних цінностей; про місцезнаходження документації, що містить комерційну таємницю, і правила роботи з нею; місце розташування і зберігання виробів (описи процесів), що становлять таємницю підприємства; *в третьому блоці «внутрішньо-організаційна діяльність служби безпеки»* мають бути відомості про склад і структуру служби безпеки, переміщення її працівників, дисциплінарну практику, результати перевірок, стан законності.

До документів, які складають у службі безпеки і прийнятих вищими державними органами управління, належать: організаційні (статут, положення, посадові інструкції, штатний розклад, правила внутрішнього трудового розпорядку); правові (закони, підзаконні акти, методичні рекомендації щодо проблем безпеки і т.ін.); розпорядчі (накази, інструкції, вказівки, графіки роботи персоналу тощо); інформаційно-довідкові (наприклад, протоколи, акти, довідки, листи, доповідні й пояснювальні записки, телефонограми, телеграми, досьє); договори, трудові угоди; документи про особовий склад (накази щодо особового складу, трудові книжки, матеріали перевірок скарг, графіки відпусток і т. ін.).

Ліквідація служби безпеки можлива у разі добровільної відмови її персоналу від виконання своїх обов'язків, за ініціативою підприємства-засновника, при ліквідації підприємства-засновника і при анулюванні органом внутрішніх справ ліцензій усіх охоронців і детективів.

5.3 Управління службою безпеки підприємства

Очолює службу безпеки начальник служби на посаді заступника керівника фірми з безпеки. Органами управління безпекою великого підприємства є: дирекція фірми – вищий орган управління; правління служби безпеки – виконавчий орган. До складу правління зазвичай входять начальник служби безпеки, заступник начальника служби безпеки, секретар-інспектор.

Начальник служби безпеки є безпосереднім керівником персоналу служби безпеки. Він підпорядковується директорові підприємства або одному із його заступників відповідно до штатного розпису. Начальник служби безпеки здійснює керівництво діяльністю служби безпеки, вирішує всі організаційні питання, пов'язані з діяльністю служби безпеки, крім тих, що стосуються виключної компетенції дирекції підприємства.

Начальника служби безпеки призначає дирекція підприємства з осіб, що мають вищу освіту.

Начальник служби безпеки без додаткового доручення діє від імені служби безпеки у всій своїй діяльності, має право підпису всіх правових і бухгалтерських документів служби безпеки, визначає посадові оклади її працівників, вирішує питання щодо надання чи позбавлення премій, інших видів заохочення та мотивування, укладає трудові договори із працівниками служби безпеки тощо. На час відпустки чи відрядження начальник служби безпеки делегує свої права заступникові.

Начальник служби безпеки відповідає за: надання охоронних і пошукових послуг з метою безпеки фірми і суворого дотримання чинного законодавства України; забезпечення збереженості спеціальних засобів, зброї, боєприпасів, що придбані підприємством; якість професійної підготовки осіб зі складу служби безпеки. Начальнику служби безпеки не дозволяється суміщати охоронну діяльність із державною службою чи виборною оплачуваною посадою в громадських об'єднаннях, а також надавати послуги особисто чи через своїх підлеглих, що пов'язані із забезпеченням безпеки інших підприємств.

Обираючи начальника служби безпеки, ставлять насамперед два питання, що стосуються його професіоналізму і лояльності. Відповідно до виконуваних ним функцій він має знати не просто дані про підприємство, а про всі проблемні аспекти його роботи, про особисте життя керівництва фірми, тощо.

При підборі кандидата на посаду начальника служби безпеки слід чітко визначити пріоритети його роботи. Такими пріоритетами можуть бути загрози з боку конкурентів, боротьба з шахрайством персоналу, протидія кримінальним угрупованням чи нейтралізація дії силових структур. Якщо головна проблема – силові структури, кращим буде працівник з керівної посади в цих структурах з відповідними налагодженими зв'язками. Якщо кримінал, то працівник має досвід роботи з ним і досвід створення відповідних систем безпеки. Якщо конкуренти, важливим є досвід збору інформації та аналізу економічної діяльності підприємства. У найзагальнішому вигляді цей процес складається з трьох стадій, кожна з яких охоплює послідовно здійснювані етапи або операції: 1 стадія: збирання, оброблення, узагальнення та аналіз інформації; 2 стадія: вироблення і ухвалення управлінського рішення; 3 стадія: організація виконання управлінського рішення.

Відповідно до специфіки діяльності служби безпеки та її зовнішнього оточення слід (у межах зазначеної структури) виробляти свій підхід до процесу управління.

Приклад структури процесу управління:

I. Оцінка обстановки (преамбула; формулювання обмежень і критеріїв ухвалення рішення, формування набору альтернативних вирішень проблеми; оцінка альтернатив).

II. Оцінка конкуруючих сил на ринку послуг (виробництві) – злочинних елементів (груп) у регіоні (зоні) дислокації фірми.

III. Оцінка своїх сил (технічне забезпечення захисту фірми; фізичне забезпечення захисту; якісна характеристика працівників служби безпеки);

IV. Оцінка фірм, що співпрацюють і взаємодіють на ринку послуг.

V. Організація взаємодії постів і порядок їх посилення за різних режимів

діяльності.

VI. Організація зв'язку між постами для забезпечення взаємодії.

VII. Організація взаємодії з органами МВС.

VIII. Дія сил і засобів служби безпеки при порушенні режимів захисту.

IX. Забезпечення охорони провідних фахівців фірми, їх сімей і власності.

Таким чином, раціональне впровадження в практику основних елементів системи, механізму і процесу управління дає змогу керівництву служби безпеки значно підвищити ефективність управлінської дії на результати її діяльності.

5.4 Структура служби безпеки великих підприємств і корпорацій

Організаційно служба безпеки великого підприємства складається з таких структурних одиниць: відділу режиму і охорони; спеціального відділу у складі сектора оброблення таємних документів і сектора оброблення документів з грифом «комерційна таємниця»; інженерно-технічної групи; групи інформаційно-аналітичної діяльності; розвідувального підрозділу; контррозвідувального підрозділу; штабного підрозділу (у випадку, якщо вищезазначені підрозділи є великими і складними оргструктур ними формуваннями).

Для продуктивного ведення господарської діяльності керівництво підприємства має ухвалювати різнорівневі рішення, інформаційну підтримку яких забезпечує система економічної розвідки.

Під терміном *«система економічної розвідки»* розуміють організаційну структуру, що займається питаннями збирання, перевірки (верифікації), оброблення та аналізу даних з різних аспектів зовнішньоекономічної діяльності підприємства з подальшим використанням отриманої інформації для вирішення конкретних завдань його господарської діяльності.

В умовах ринкової економіки підприємство не може ефективно працювати без глибокого розуміння її рушійних сил і не маючи у своєму розпорядженні новітньої інформації про те, що ж відбувається у займаному ним

сегменті ринку. При цьому обов'язково треба враховувати, що можливості підприємства, зумовлені навколишнім середовищем і балансом інтересів різних співтовариств, угруповань і окремих осіб, часто витікають не з логіки подій, а з емоцій, особистих симпатій і антипатій.

Підрозділ економічної розвідки підприємства – структурний підрозділ, на який покладено завдання єдиного (в межах господарюючого суб'єкта) інформаційного центру, із завданнями оброблення та аналізу інформації, що забезпечує ухвалення вищим керівництвом обґрунтованих рішень із найважливіших питань для інтересів підприємства.

Будь-яка діяльність має ґрунтуватися на певних принципах, не є винятком і розвідувальна діяльність. Першим і найважливішим принципом організації будь-якої розвідувальної діяльності, зокрема економічної), є *неупередженість у відборі, систематизації, обробленні й передачі здобутої інформації. Принцип системності інформації*, здобутої економічною розвідкою, забезпечує достовірність даних, а отже, ефективність розвідки. *Принцип конфіденційності.* Отримання будь-якої інформації з напівлегальних або нелегальних джерел має бути закритим. Іншими важливими принципами планування розвідувальної діяльності в економіці є: визначення мети проведення розвідувальної діяльності; визначення потреби суб'єкта економічної діяльності в інформації для досягнення цих цілей, визначення джерел отримання необхідної інформації.

Управління будь-якою організацією має як мінімум два рівні: управління поточною діяльністю підприємства і управління його стратегічним розвитком. Результати ухвалених рішень з цих питань виявляються по-різному: поточні – найближчим часом, стратегічні – в майбутньому.

Слід зазначити, що характер інформації для кожного рівня ухвалених рішень різний. У зв'язку з цим у роботі підрозділу економічної розвідки підприємства доцільно виокремити дві складові:

Стратегічну (макроекономічну) – збирання і аналіз стратегічної інформації про глобальні процеси в економіці, політиці, технології тощо, які

можуть впливати (позитивно чи негативно) на розвиток підприємства. *Мета стратегічного рівня ухвалення рішення* (відкриття нового виробництва, впровадження на ринок нового товару або послуги та ін.) полягає у визначенні напряму подальшого розвитку підприємства. Ці рішення визначають потребу зорієнтуватися на ринку та проаналізувати перспективи його розвитку, тобто розгледіти ще не заповнені конкурентами ринкові ніші. *Оперативно-тактична (мікроекономічна) складова економічної розвідки* – збирання та аналіз оперативно-тактичної інформації для ухвалення керівництвом обґрунтованих рішень з поточних проблем підприємства. Мета оперативно-тактичного рівня ухвалення рішення (будівництво або придбання будівлі під новий цех, навчання персоналу для випуску нової продукції або надання нової послуги), відповідно до напряму подальшого розвитку, – вибрати оптимальний шлях його досягнення і мінімізувати витрати розвитку цим шляхом.

Основне призначення системи економічної розвідки полягає у: забезпеченні керівництва фірми достовірною, об'єктивною і повною інформацією про наміри партнерів, суміжників, клієнтів і контрагентів, про сильні і слабкі сторони конкурентів; зборі даних, що дають змогу впливати на позицію опонентів у ділових переговорах; сповіщенні про можливе виникнення кризових ситуацій; моніторингу і контролі реалізації укладених договорів і досягнутих раніше домовленостей.

Розвідку на досліджуваному «об'єкті» можуть зацікавити:

особовий склад підприємства: загальна кількість працівників, їх національний і соціальний склад; розподіл їх за службовими категоріями, відділами, службами; списки і характеристики працівників, інші дані; облік особового складу (картотеки, особисті справи); посадові оклади і матеріальна забезпеченість різних категорій працівників; використання службового положення в особистих цілях; участь працівників у суспільно-політичних рухах і партіях, членство в організаціях, союзах, товариствах, клубах;

облаштування і режим: розміщення виробничих цехів, відділів і служб у приміщеннях підприємства; розміщення і обладнання сховищ і складів для

матеріалів і продукції; порядок обліку, розмноження, правила звернення і пересилання документів; перевірка працівників і відвідувачів на вході і виході; організація внутрішнього зв'язку та зв'язку з іншими установами і підприємствами; заходи захисту від витоку інформації; технічні засоби гарантування безпеки; структура і склад служби безпеки; положення про службу безпеки і розподіл посадових обов'язків;

умови наймання: укомплектованість основних підрозділів і служб, потреба у фахівцях певних професій; умови приймання на роботу; процедура допуску до роботи, терміни перевірки, випробувальний термін; практика хабарів, підкупу посадовців під час приймання на роботу;

виробництво: структура виробництва; характер виробництва об'єкта; оцінка якості й ефективності; номенклатура виробів; умови виробництва; організація праці; відомості про виробничі можливості підприємства (виробничі потужності й відсоток їх використання, можливості розширення); рівень запасів (технологічне устаткування, верстати), дані про їх тип і розміщення; рівень витрат; дані про резерви сировини на підприємстві; відомості про забезпеченість допоміжними матеріалами, комплектуючими; дані про фонди окремих товарів, що виділяються для постачання;

управління: відомості про перспективні методи управління; організація управлінського апарату та його діяльності, реалізація управлінських функцій керівництвом підприємства;

плани: стратегічні плани розвитку підприємства; плани інвестицій; комерційні задуми щодо розширенню виробництва; план виробництва і перспективний план; план закупівель і продажів; проекти річних і перспективних експортно-імпортних планів; інвестиційні програми і плани інвестицій; планово-аналітичні матеріали на поточний період і за минулий рік; оперативні дані про виконання експортно-імпортного плану з розширення виробництва; плани передбачуваного створення за кордоном самостійних фірм, офшорних компаній;

фінанси: відомості, що розкривають планові й фактичні показники

фінансового плану; майнове положення; вартість товарних запасів (для конкурентів, для визначення кредитоспроможності і надійності як партнерів); обороти; банківські операції; фінансові операції, особливо пов'язані з порушенням законодавства; банківські зв'язки; специфіка міжнародних розрахунків з інофірмами (наявність банківських рахунків за кордоном); планові і звітні дані про валютні операції; стан банківських рахунків підприємств і здійснюваних операцій; розмір виручки і доходів; боргові зобов'язання (перевірка партнерів); стан кредиту (пасиви й активи); розміри і умови банківських кредитів; звіт про розміри запланованого кредитування; генеральна лінія і тактика з валютних і кредитних питань; звіт про кредитні і валютні відносини з іноземними державами і фірмами;

ринок: оригінальні рішення щодо вивчення ринку збуту; стан ринків збуту; огляди ринку; відомості, що містять висновки й рекомендації фахівців із стратегії і тактики діяльності підприємства; частка на ринку і тенденції її зміни; використання кон'юнктури товарних ринків; ринкова стратегія; комерційно-політичні цілі й комерційні задуми фірми; звіт про час виходу на ринок при закупівлях (продажах) товарів і вибір фірм для ведення комерційних переговорів; політика зовнішньоекономічної діяльності в цілому і по регіонах; оригінальні методи продажів; відомості про конкретні напрями торгової політики; конкурентоспроможність продукції, товарів і послуг;

партнери: коло клієнтів, зокрема в торгівлі, рекламі; список представників або посередників; постачальники і споживачі; негласні компаньйони; комерційні зв'язки; відносини із споживачами і репутація; іноземні партнери; характеристика показників діяльності партнерів (їх виробничі фонди, товарообіг, прибуток, кредити, боргові зобов'язання, керівництво), їх ступінь надійності; лобі – «свої люди» в адміністративних і державних органах та органах законодавчої влади;

переговори: порядок опрацьовування пропозицій партнерів, відомості про отримувані й опрацьовувані замовлення та пропозиції; про факти підготовки і проведення переговорів; терміни підготовки і проведення переговорів;

директиви керівництва щодо проведення переговорів: тактика, межі повноважень щодо цін, знижок тощо; перебіг і результати; відомості про ділові прийоми; предмет і результати службових нарад та засідань органів управління;

контракти: умови по операціях і угодах; умови контрактів, включаючи ціни; особливі умови (знижки, приплати, розстрочка платежів, форми платежів); умови фрахтування морського, річкового, авіаційного і автомобільного транспорту; зведення про перебіг виконання контрактів; відомості про номенклатуру і кількість товарів за взаємними зобов'язаннями;

ціни: розрахунок цін, структура цін; ринкові ціни, знижки, торги й аукціони, відомості про передбачуваний конкурс або торги до їх публікації (склад учасників, ідеї, плани);

наука і техніка: характер і цілі науково-дослідної роботи; результати наукових досліджень і проектних розробок; винаходи, нові ідеї, наукові, технічні, конструкційні, технологічні рішення; проекти, моделі, документація з калькуляцією про нові вироби, не захищені патентами; пристрої, конструкції, креслення, формули, схеми, технічні рішення; промислові зразки; зведення про стан програмного і комп'ютерного забезпечення;

технологія: відомості технологічного характеру; технологічні досягнення, що забезпечують перевагу в конкурентній боротьбі; перспективні технології, технологічні процеси, прийоми і устаткування; модифікація раніше використовуваного устаткування з метою вдосконалення технологій.

Таким чином, мета розвідувальної діяльності полягає у виконанні двох умов: запобігання появі несприятливих чинників для діяльності компанії; забезпечення ефективного розвитку бізнесу в усіх сферах, регіонах і напрямах, в яких представлені інтереси організації.

Оргструктура розвідки має два види підрозділів (відділень, груп, секторів, співробітників): *добувні та інформаційні*.

Основне призначення *добувних підрозділів* полягає в добуванні всіма доступними і такими, що не суперечать законодавству, засобами і методами відомостей, документів, предметів та інших матеріалів, які становлять або

можуть становити розвідувальний інтерес. У складі цих підрозділів мають бути такі відділення (групи, сектори, окремі співробітники): роботи з інформаторами; з виявлення і збирання відкритих і закритих публікацій; прихованого спостереження; технічного забезпечення операцій, що проводяться; проведення розслідувань і документування поведінки об'єкта, що вивчається.

Основне завдання *інформаційних підрозділів* розвідки полягає в оцінці, класифікації, аналізі й наданні керівництву підприємства обробленої розвідувальної інформації. До складу цих підрозділів входять: аналітичне відділення (група, сектор), відділення стратегічного планування, довідково-інформаційний фонд (ДІФ), група експертів і консультантів. Між усіма підрозділами розвідки має бути чітке розмежування за такими параметрами, як завдання і форма подання результатів роботи.

Вимоги до особи розвідника: вища освіта (юридична і/або економічна), кмітливість, чесність, об'єктивна самооцінка, аналітичні здібності, пунктуальність, гнучкість, здатність чітко формулювати й висловлювати (в усній і письмовій формі) свої думки, винахідливість, товариськість, самодисципліна.

Поряд з розвідувальною діяльністю важливо організувати *контррозвідувальну діяльність.* Робота підрозділу економічної контррозвідки служби безпеки господарюючого суб'єкта пов'язана: з виявленням, попередженням, припиненням спроб інфільтрації і вербуванням агентури конкурентами, партнерами та кримінальними структурами; запобіганням просочуванню конфіденційної інформації про діяльність підприємства з боку його працівників, партнерів і клієнтів; профілактичною перевіркою лояльності його співробітників, службовим розслідуванням фактів фальсифікації і розкрадань; оперативним прикриттям персоналу, будівель і об'єктів підприємства.

ЗМ 2 Організація та управління фінансово-економічною безпекою банків та фінансових установ

Тема 1 Основи управління фінансово-економічною безпекою в банку

План лекції

1.1 Суть і зміст безпеки банківської діяльності, її мета та завдання

1.2 Види безпеки банківської діяльності та форми її організації

1.3 Організація управління фінансово-економічною безпекою в банку

1.1 Суть і зміст безпеки банківської діяльності, її мета та завдання

Безпека банківської діяльності є складовою частиною національної безпеки країни, і їй належить відповідна роль у формуванні економічної та соціальної політики.

Безпека банківської діяльності України – це такий стан чинних правових норм і відповідних їм інститутів безпеки, який відображає рівень захищеності державою кредитно-фінансових відносин між суб'єктами банківської діяльності та гарантує стійке функціонування всієї банківської системи України; забезпечує можливість повної реалізації та захист життєво важливих фінансових та економічних інтересів держави, суспільства й особи; виключає або максимально обмежує деструктивні наслідки від зовнішніх та внутрішніх загроз, недосконалості зовнішньоекономічної, внутрішньогосподарської та бізнесової діяльності.

Поняття «безпека банківської діяльності» також можна розглядати: *як стан* стійкої життєдіяльності, за якого забезпечується реалізація основних інтересів і пріоритетних цілей банку, захист від внутрішніх і зовнішніх дестабілізуючих факторів незалежно від умов функціонування; *як властивість* банку своєчасно та адекватно реагувати на всі негативні прояви внутрішнього й зовнішнього його оточення; *як здатність* протистояти різним посяганням на

власність, діяльність або імідж банку, а також здатність створювати ефективний захист від внутрішніх і зовнішніх загроз.

Метою безпеки банківської діяльності є виключення можливості заподіяння банку збитків або упущення вигоди, а також забезпечення ефективної діяльності банку і якісної реалізації ним всіх операцій та угод.

Мета безпеки банківської діяльності забезпечується виконанням таких *завдань*: захист законних інтересів банку і його працівників; профілактика та попередження правопорушень і злочинних зазіхань на власність і персонал банку; своєчасне виявлення реальних і потенційних загроз банку, проведення заходів щодо їх нейтралізації; виявлення внутрішніх і зовнішніх причин та умов, які можуть сприяти заподіянню банку, його працівникам, клієнтам і акціонерам матеріальної, моральної та іншої шкоди, перешкоджати їх нормальній діяльності; оперативне реагування елементів структури банку на виникаючі загрози й негативні тенденції розвитку зовнішньої та внутрішньої обстановки; виявлення та формування причин і умов, сприятливих для реалізації банком своїх основних інтересів; виховання та навчання персоналу банку з питань безпеки; послаблення шкідливих наслідків від акцій конкурентів або злочинців, спрямованих на підрив безпеки банку; збереження й ефективне використання фінансових, матеріальних та інформаційних ресурсів банку.

Головним критерієм ефективності і якості безпеки банківської діяльності є стабільність його фінансового й економічного розвитку відповідно до планів і завдань незалежно від зміни ситуації.

Надійність та ефективність функціонування системи безпеки банківської діяльності оцінюється за *наступними критеріями*: відсутність (своєчасне виявлення) спроб несанкціонованого проникнення в банк з метою скоєння злочину; відсутність (недопущення) фактів витоку інформації, розголошення відомостей обмеженого доступу; відсутність (попереджання) протиправних та негативних дій з боку персоналу банку; збереження фінансових і матеріальних цінностей банку, а також своїх працівників; попереджання надзвичайних подій.

Під управлінням безпекою банківської установи розуміється організовані

дії, які забезпечують погодженість функціонування всіх служб, підрозділів, відділів та співробітників з метою усунення різних загроз діяльності банку. Тобто це системне діяння через використання економічних, організаційних, правових та інших методів, в ході яких: *на мікрорівні* (окремій кредитній організації) здійснюється цілеспрямована побудова та використання системи забезпечення безпеки банківського бізнесу з максимальним результатом при мінімумі витрат за критерієм, який відповідає її індивідуальним особливостям та прийнятій стратегії; *на макрорівні* – у відповідності з економічною політикою держави, з врахуванням інтересів великої групи або всієї кількості банків, формуються умови забезпечення безпеки, а також умови цивілізованого банківського бізнесу в масштабі країни, регіону, сфери банківської діяльності; створюється цілісна система управління безпекою в масштабі країни; забезпечується її стійкість та цілеспрямований розвиток.

За своєю сутністю управління безпекою є безперервним процесом підтримання необхідного або заданого ступеня захищеності. *За змістом* управління безпекою є своєчасне та чітке виконання планових заходів, які розроблені на випадок виникнення тих або інших критичних ситуацій. Необхідність планування діяльності стосовно забезпечення банківської безпеки не викликає жодних сумнівів.

Система безпеки банку являє собою динамічну організацію вповноважених структур, що реалізує власними силами та засобами міри правового (нормативного), організаційного, технічного, розшукного, криміналістичного, кримінологічного характеру, з метою захисту майна, інфраструктури й порядку функціонування кредитної організації від протиправних посягань. Така система створюється з урахуванням необхідності захисту банку від всіх відомих різновидів негативних впливів та їх наслідків. Головними вимогами до системи безпеки є її надійність і ефективність.

Головною умовою організації системи безпеки банківської діяльності в Україні є наявність матеріальних та інтелектуальних засобів. Слід зауважити, що на сьогоднішній день не кожний банк може дозволити собі високоякісну,

найсучаснішу систему безпеки та постійно її оновлювати, оскільки комп'ютерні та ІТ-технології розвиваються постійно.

Для ефективного функціонування системи безпеки банку необхідно дотримуватись наступних *вимог:* безперервність; плановість; конкретність; активність; комплексність.

Ці вимоги забезпечуються з урахуванням дотримання в процесі її організації та функціонування наступних *основних принципів*:

законність: заходи, які виконуються в межах, необхідних для забезпечення безпеки банку, ґрунтуються на чинних законах України, Постановах Кабінету Міністрів, Указах Президента України, нормативних актах Національного банку України, вимогах та документів місцевих органів влади та уставу банку;

самостійність та відповідальність: підрозділи безпеки банку повинні мати у своєму розпорядженні всі необхідні засоби для ефективного рішення поставлених перед ними завдань; повноваження осіб та діяльність підрозділів банківської безпеки суворо регламентуються нормативними актами і внутрішніми розпорядженнями банків;

економічна доцільність: заходи безпеки не повинні приводити до погіршення умов діяльності та загального стану банку, перешкоджати реалізації його інтересів. Витрати на проведення заходів безпеки повинні бути адекватними ефективності останніх;

компетентність: виконання заходів безпеки повинно здійснюватися грамотно, на високому професійному рівні, ґрунтуватися на об'єктивних даних, не обмежувати права співробітників;

цілеспрямованість: заходи безпеки здійснюються в суворій відповідності із завданнями, які вирішує банк згідно з затвердженою керівництвом комплексною програмою безпеки діяльності;

координація та взаємодія: служба безпеки банку координує зусилля всіх його установ, підрозділів та відділів щодо виконання заходів безпеки. З цією метою служба безпеки встановлює необхідні зв'язки з підрозділами банку та

зовнішніми організаціями;

конфіденційність: заходи безпеки проводяться на конфіденційній основі тобто без їх розголошення; про результати виконання заходів безпеки інформується керівництво банку і у відповідності до його рішення, інші особи, робота яких пов'язана з необхідністю володіння цією інформацією;

комплексності: при побудові системи безпеки банківської діяльності необхідно враховувати всі загрози, які здатні завдати шкоди, а обрані заходи, сили, технології та засоби безпеки повинні функціонувати узгоджено, як єдиний механізм захисту, взаємно доповнюючи один одного у функціональному та технічному змістах;

ешелонування: полягає в створенні декількох послідовних рубежів захисту таким чином, щоб найбільш важлива зона безпеки банка перебувала усередині інших зон;

рівнозначності: всі рубежі, що захищають зону безпеки, повинні бути однаково міцними та рівнозначними з погляду ймовірності реалізації загрози. Якщо в рубежах є слабкі, погано захищені місця, то ніякі ефективні заходи захисту інших рубежів не захистять цю зону безпеки;

безперервності: у процесі функціонування системи захисту не повинно бути перерв у роботі, викликаних ремонтом, зміною паролів і т.п., якими може скористатися зловмисник;

своєчасність: характеризує попереджуючий характер заходів забезпечення безпеки.

Основними елементами системи безпеки банку є: заходи безпеки, технології безпеки, сили безпеки та засоби безпеки.

У свою чергу, *заходи безпеки* підрозділяються на заходи загального характеру та спеціальні. До заходів *загального* характеру відносять: здійснення організаційно-правового впливу на діяльність персоналу і клієнтів банку з питань безпеки; підбір, перевірка і контроль роботи персоналу, розроблення ефективної кадрової політики і програм стимулювання праці; охорона банку; організація спеціального діловодства; захист інформаційних ресурсів банку;

удосконалення технологій банківського виробництва, введення в них елементів захисту; формування позитивного іміджу банку; планування і забезпечення дій банку в кризових ситуаціях; забезпечення безпеки споруд і будівель установ банку, їх комунікаційних систем; створення системи сповіщення персоналу банку; розроблення заходів відповідальності за порушення установлених правил безпеки банківської діяльності. *Спеціальними* заходами банківської безпеки є: організація і ведення комерційної розвідки, формування інформаційних ресурсів банку; інформаційно-аналітичні дослідження клієнтів, партнерів і конкурентів банку; взаємодія із правоохоронними органами з питань забезпечення безпеки діяльності банку; втілення заходів щодо виявлення, попереджання, локалізації, протидії актів недобросовісної конкуренції і промислового шпигунства; проведення службових розслідувань у банку; вжиття заходів щодо дезінформації конкурентів; вжиття заходів щодо недобросовісних клієнтів, боржників і зловмисників з метою відшкодування ними збитків, яких банк зазнав з їх вини.

Організація банківської безпеки – трудомісткий, багатогранний процес, який охоплює практично всі сторони діяльності банку. Ефективність заходів безпеки досягається лише тоді, коли вони провадяться в комплексі із маркетинговою діяльністю, відповідними кадровою політикою та методами управління. Рекомендації з безпеки повинні враховуватись під час розроблення банківських технологій та методик проведення операцій. Виконання заходів безпеки забезпечується за допомогою сил безпеки та використання різноманітних засобів.

Силами та засобами безпеки банку є: підрозділи безпеки банку; спеціалізовані підприємства, фірми й організації, які здійснюють виконання заходів безпеки банківської діяльності на договірній основі; персонал банку; технічні засоби охорони банку; програмні і технічні засоби захисту банківської інформації; спеціальні засоби і техніка; інженерно-технічні засоби обмеження доступу; технічні засоби зв’язку, обробки і передавання інформації; інші засоби і техніка, які використовуються для забезпечення ефективної реалізації мір

безпеки банку.

Об'єкти безпеки банку, відносно яких здійснюються злочинні посягання, можна розділити на наступні групи: *фінансові ресурси* (національна і іноземна валюти, банківські (комерційні) операції і угоди банку, дорогоцінні метали, фінансові документи), *персонал банку* (керівництво і вищий менеджмент банку, а також особи, які мають доступ до банківських таємниць, інші працівники банку); *матеріальні засоби* (будівлі, споруди, сховища, обладнання, транспорт, кошти і системи комунікації та інформатизації); *інформаційні ресурси банку з обмеженим доступом.*

Необхідною умовою забезпечення безпеки є наявність інформації про цілі злочинних посягань на об'єкти безпеки банку. Ці цілі можна об'єднати в дві основні групи: заволодіння майном банку (правом на майно) з метою обертання його в свою власність; обмеження діяльності банку-конкурента або його усунення з ринку фінансових послуг.

Суб'єктами правовідносин при вирішенні проблеми безпеки є:

держава як власник ресурсів, що створюються, придбаваються і нагромаджуються за рахунок коштів державного бюджету, а також інформаційних ресурсів, віднесених до категорії державної таємниці. В процесі забезпечення безпеки банку держава виступає як гарант захисту його виняткового права на здійснення банківської діяльності (аналогічна діяльність інших суб'єктів визнається незаконною), а також його майна і інфраструктури. Вона здійснює свою функцію за допомогою державних органів законодавчої, виконавчої і судової влади шляхом: встановлення кримінальної і іншої відповідальності за протиправні посягання на інтереси банку; виявлення, запобігання, припинення, розслідування злочинів і інших правопорушень, покарання винних і відшкодування збитку; здійснення державного контролю і нагляду за виконанням банком встановлених законодавством вимог безпеки;

Національний банк України – бере участь в забезпеченні безпеки кредитних організацій шляхом вживання методів регулювання і нагляду за їх діяльністю. Він здійснює дозвільні, наглядові, контрольні і адміністративні

функції відносно банківських установ для підтримки стабільності банківської системи, захисту інтересів вкладників і кредиторів;

правоохоронні органи (зокрема, поліція). Форми їх участі в забезпеченні безпеки банківської діяльності визначаються їх належністю до державних органів виконавчої влади, основною функцією яких є охорона законності і правопорядку. Вказану функцію вони реалізують шляхом запобігання, виявлення, припинення і розслідування злочинів і адміністративних правопорушень, що посягають на безпеку банку;

*органи прокуратури***.** Прокуратура як суб'єкт забезпечення безпеки у сфері банківської діяльності реалізує свої функції шляхом нагляду за дотриманням законності, а також кримінального переслідування осіб, що скоюють злочини в банківській сфері. Для виконання цих функцій прокуратура проводить прокурорські перевірки виконання законів, здійснює попереднє розслідування злочинних посягань на інтереси банку. У разі потреби прокурор має право порушити справу про адміністративне правопорушення і провести адміністративне розслідування;

органи судової влади – здійснюють правосуддя по кримінальних справах і справах про адміністративні правопорушення, пов'язані з посяганнями на безпеку банківської установи. Їх рішення у сфері захисту інтересів банку спрямовані на покарання винних і відшкодування збитку, заподіяного майну та інфраструктурі кредитної організації;

Банк як юридична особа, який є власником фінансових, а також інформаційних ресурсів, що складають службову, комерційну і банківську таємницю. Банківська установа виконує законодавчо встановлені обов'язки забезпечення власної безпеки шляхом захисту майна і інфраструктури. Для виконання цих функцій банк застосовує засоби і методи правового, організаційного, технічного, розшукового і криміналістичного характеру;

окремі структурні підрозділи банку (служба внутрішнього контролю, служба безпеки). Служба безпеки банку є обов'язковим структурним підрозділом кредитної організації, без створення якого банк не може отримати

державну реєстрацію. Вона бере участь в забезпеченні безпеки банківської установи шляхом розробки заходів попереджання і виявлення дій і рішень персоналу, що містять потенційний ризик (загрозу) нанесення шкоди майну і порядку функціонування банку. Служба внутрішнього контролю банку є заснованою за ініціативою і на кошти банку охоронно-розшуковим підприємством. На відміну від служби безпеки її створення не обумовлене обов'язковими нормативними розпорядженнями. Основним завданням служби внутрішнього контролю є захист власності і інфраструктури банку від протиправних посягань. Для виконання своїх функцій служба застосовує засоби і методи правового, організаційного, технічного, розшукового, охоронного і криміналістичного характеру;

інші юридичні і фізичні особи, у тому числі партнери і клієнти, які ступають з банком в договірні стосунки, беруть участь в захисті майна і інфраструктури банку в межах зобов'язань, перейнятих на себе по відповідних договорах.

1.2 Способи, структура заходів і методи організації забезпечення безпеки діяльності банку

Заходи безпеки банку реалізуються за допомогою: *матеріально-технічного забезпечення:* технічні засоби охорони; технічні засоби захисту інформації; зброя, засоби індивідуального захисту; формений одяг сил охорони банку; засоби обробки, передавання інформації та зв'язку; транспортні засоби; програмне забезпечення; *фінансового забезпечення:* оплата праці працівників підрозділу безпеки; заохочення працівників за ефективне виконання заходів безпеки; витрати, пов'язані з виконання спеціальних заходів; *кадрового забезпечення:* підбір кваліфікованих фахівців і прийняття їх на роботу; фахова підготовка, перепідготовка й удосконалення підготовки фахівців; *інформаційного забезпечення*: отримання інформації від установ і підрозділів банку; отримання інформації на договірних засадах від установ і підприємств;

отримання інформації від ЗМІ; *наукового забезпечення:* проведення наукових досліджень проблем безпеки банківської діяльності; наукові обґрунтування вирішення проблем банківської діяльності; узагальнення та аналіз досвіду роботи.

Методи забезпечення безпеки банку варіюються залежно від специфіки завдань, що підлягають вирішенню, і від компетенції суб'єктів, які беруть участь в процесі забезпечення безпеки. У свою чергу вибір засобів забезпечення безпеки банку, тобто прийомів або спеціальних знарядь, зумовлений методами, в рамках яких їх планується використовувати. Всі методи можуть бути зведені в дві основні групи: *до першої групи* входять методи законодавчого і нормативного правового регулювання; *другу групу* складають методи реалізації законодавчих і інших нормативних правових розпоряджень. Серед них виділяють методи: організаційні; технологічні; захисту конфіденційної інформації; адміністративного і фінансового контролю; пошукової та охоронної діяльності; криміналістики.

Організаційні методи забезпечення безпеки. Містять спеціальні методи здійснення виробничої, управлінської, фінансової, комерційної, кадрової і іншої функціональної діяльності банку, що мають за мету попередити спричинення збитку як в результаті навмисних дій, так і внаслідок помилки. В рамках організаційних методів формуються спеціальні підрозділи захисту інтересів банку; проводиться вдосконалення структури керівних і контролюючих органів; ухвалюються рішення про обмеження і розмежування повноважень посадових осіб відносно обсягів і складу банківських операцій, в розпорядженні грошовими коштами і іншим майном банку; розмежовуються повноваження операціоністів і касирів при здійсненні розрахунково-касових операцій; встановлюється індивідуальна відповідальність конкретних осіб відносно забезпечення процедур виконання окремих операцій і порядку зберігання цінностей; організується система звітності банку і система роботи із персоналом. Суб'єктом застосування вказаної групи методів є банк в особі керівних органів, наділених правом прийняття відповідних рішень. Засобами

реалізації зазначених методів є організаційні рішення, закріплені у формі розпорядних документів банку.

Технологічні методи забезпечення банківської безпеки. В рамках цих методів розробляються безпечні технології банківських операцій, що не дозволяють злочинцям використовувати відомі на практиці способи скоєння злочинів До їх числа входять технології відкриття рахунків, укладання договорів, касового обслуговування клієнтів банку, роботи пунктів обміну валюти, оформлення, видачі та оплати цінних паперів тощо. Технологічні методи забезпечення безпеки банку ґрунтуються на відповідних рекомендаціях Національного Банку України, розробках власних підрозділів, на наукових і практичних рекомендаціях фахівців в області боротьби із злочинами у фінансовій сфері (наприклад, у сфері вексельного обігу). *Суб'єктами реалізації* є керівні органи банку, а також його структурні підрозділи в рамках відповідних напрямів банківській діяльності. *Засобами реалізації* є технологічні рішення, закріплені розпорядними документами.

Методи захисту конфіденційної інформації – досить різноманітні і охоплюють широкий спектр дій організаційного, програмно-апаратного і контрольного (перевірочного) характеру. В цілому вони можуть бути зведені *в чотири основні групи,* кожна з яких має за мету вирішення відносно самостійних завдань, а саме: закриття вільного доступу до відомостей конфіденційного характеру; виявлення, попередження та припинення спроб неправомірного заволодіння відомостями і документами конфіденційного характеру; організацію захисту конфіденційної інформації, оброблюваної засобами обчислювальної техніки, від несанкціонованого доступу; організацію захисту конфіденційної інформації від витоку по технічних каналах. Кожна з названих груп містить у собі ряд самостійних методів. *Суб'єктами застосування* методів і засобів захисту інформації є спеціальні підрозділи захисту інформації банку. *Засобами реалізації* методів захисту конфіденційної інформації служать нормативні правові документи рекомендаційного і заборонного характеру, а також спеціальні комп'ютерні програми і пристрої.

Методи адміністративного та фінансового контролю. Метою методів адміністративного контролю у сфері забезпечення безпеки банку є: перевірка наявності і правильного функціонування системи підбору і розміщення кадрів; перевірка змісту укладених з працівниками трудових угод (контрактів); перевірка наявності інструкцій, що регламентують посадові обов'язки співробітників. Крім того, за допомогою адміністративних методів забезпечується проведення операцій лише уповноваженими на те особами в строгій відповідності з визначеними банком повноваженнями і процедурами прийняття рішень щодо проведення операцій.

Методи фінансового контролю покликані забезпечити проведення операцій в строгій відповідності з прийнятою і закріпленою документально політикою банку стосовно різних видів фінансових послуг та їх адекватного віддзеркалення в обліку і звітності. Фінансовий контроль повинен з достатнім ступенем надійності забезпечити фіксацію операцій відповідно до встановлених вимог, реальне віддзеркалення стану активів і пасивів банку і забезпечення складання передбачених форм звітності; ведення фінансових документів з достатньою повнотою, їх відповідність фактичним обставинам і здійснення перевірок із встановленою періодичністю.

*Контроль з*а проведенням методів фінансового контролю здійснює Державний департамент фінансового моніторингу (згідно з Положенням Кабінету Міністрів України «Про Державний департамент фінансового моніторингу»).

Суб'єктами реалізації методів адміністративного і фінансового контролю є Служба безпеки банку та Служба внутрішнього контролю банку. *Засобами* адміністративного і фінансового контролю є: фактична перевірка; підтвердження; обстеження; опитування; аналітичні тести; логічна і арифметична перевірки.

Методи пошукової та охоронної діяльності. Методи пошуку застосовуються з метою: збору відомостей по цивільних справах; вивчення ринку, збору інформації про ділові переговори, виявлення

некредитоспроможних або ненадійних ділових партнерів; встановлення обставин недобросовісної конкуренції, а також розголошення відомостей, що становлять комерційну таємницю; з'ясування біографічних і інших даних, що характеризують особу, про окремих громадян (з їх письмової згоди) при укладанні ними трудових і інших контрактів; пошуку втраченого майна; збору відомостей по кримінальних справах.

Суб'єктами застосування методів і засобів пошукової і охоронної діяльності є Служба безпеки банку. *Реалізація методів* охорони здійснюється з метою захисту життя і здоров'я співробітників банку; охорона майна; проектування, монтажу і експлуатаційного обслуговування засобів охоронної і пожежної сигналізації. Методами пошукової діяльності є: усне опитування громадян і посадових осіб (з їх згоди); наведення довідок; вивчення предметів і документів (з письмової згоди їх власників); зовнішній огляд будов, приміщень і інших об'єктів; спостереження для одержання необхідної інформації. Допускається застосування в рамках вказаних методів відео- і аудіозаписів, кіно- і фотозйомки, технічних і інших засобів, що не заподіюють шкоди життю і здоров'ю громадян, навколишньому середовищу, а також засобів оперативного радіио- і телефонного зв'язку. У випадках небезпеки для життя і здоров'я особам, що здійснюють розшук і охорону, дозволяється використання спеціальних засобів і вогнепальної зброї.

Методи криміналістики. Суб'єктами реалізації методів і засобів криміналістки в комерційному банку є в основному Служба безпеки банку. Проте названі методи і засоби можуть використовувати при необхідності Служба внутрішнього контролю і Служба захисту інформації банку. За службовою роллю для забезпечення банківської безпеки криміналістичні методи і засоби поділяться на: методи і засоби встановлення причин і умов, що сприяли здійсненню або прихованню злочинів; методи і засоби отримання інформації про злочини, що готуються; методи і засоби захисту майна банку від злочинних посягань і створення сприятливих умов для виникнення доказової інформації. За джерелом походження, застосовні в зазначених випадках методи

і засоби, розмежуються на три основні групи: криміналістична техніка; криміналістична тактика; криміналістична методика.

Ефективність системи комплексного захисту банку може бути забезпечена шляхом раціонального поєднання всіх засобів і методів. Вони повинні об'єднуватися в єдиний, цілісний механізм захисту, створення якого краще всього вести паралельно із проектуванням і будівництвом банківського об'єкту.

Види безпеки банку:

особиста безпека – забезпечення спокійної роботи, вільного переміщення і відпочинку кожного працівника; здатність кожного працівника банку протистояти загрозам його здоров'ю, життю й професійній діяльності на основі оволодіння нормами й правилами безпечного поводження. Забезпечується за допомогою дотримання всіма працівниками засобів застереження, передбачених умовами роботи та нормами особистої поведінки; проведення відносно працівників банку спеціальних охоронних заходів; вивчення кожним працівником правил поведінки в складних умовах та екстремальних ситуаціях;

колективна безпека – здатність підрозділів банку забезпечувати ефективний режим роботи в умовах діяльності різноманітних дестабілізуючих факторів. Забезпечується за допомогою: створення доброзичливої, спокійної обстановки в колективах; дотримання принципу справедливості; грамотного стимулювання роботи; постійного вивчення психологічної обстановки в колективах; своєчасного виявлення підвищеної напруженості взаємовідносин працівників; попередження та швидкого розв'язання конфліктних ситуацій;

економічна безпека - забезпечення захисту і раціонального використання фінансових ресурсів банку, надійного збереження і транспортування готівки і цінностей, грамотної експлуатації технічних засобів і обладнання банку, забезпечення умов для ефективного проведення банком операцій і укладання угод; стан юридичних, виробничих відносин та організаційних зв'язків, матеріальних та інтелектуальних ресурсів, при яких забезпечується стабільність функціонування, фінансово-комерційний успіх, прогресивний науково-

технічний, економічний та соціальний розвиток банку; здатність адекватно та без особливих втрат реагувати на зміни внутрішньої та зовнішньої ситуацій. Забезпечується за допомогою створення ефективного комплексу заходів: захист електронної системи платежів банку та попередження витоку коштів через фальсифікацію фінансових документів; наявність відповідних місць зберігання готівки, цінностей, технічних коштів, транспорту й устаткування банку, кваліфікованою їх експлуатацією; грамотна організація охорони та режимних заходів банку; покарання за крадіжки матеріальних коштів та їх псування; ефективне планування заходів та дотриманням правил пожежної безпеки;

інформаційна безпека – стан інформаційних ресурсів банку, при яких забезпечується необхідний рівень інформованості керівництва, персоналу банку, а також зовнішнього середовища, ефективний захист всіх видів інформації від зовнішніх і внутрішніх загроз. Інформаційна безпека досягається за допомогою: організації збору інформації про внутрішнє та зовнішнє середовище банку; проведення інформаційно-аналітичного дослідження клієнтів, партнерів і конкурентів; інформаційного аудиту та моніторингу в банку, а також за допомогою аналітичної обробки інформації; організації системи інформаційного забезпечення рішень керівництва банку; визначення категорій банківської інформації та проведення відповідних заходів щодо її захисту; дотримання відповідних режимів діяльності банку; виконання всіма працівниками банку норм і правил роботи з інформацією.

1.3 Організація управління фінансово-економічною безпекою в банку

Економічна безпека банківської системи – стан банківської системи, за якого її фінансова стабільність або репутація не може бути підірвана цілеспрямованими діями певної групи осіб і організацій або фінансовою ситуацією, що складається, всередині і поза банківською системою.

Економічна безпека банку – стан, за якого забезпечується економічний розвиток і стабільність діяльності банку, гарантований захист його фінансових і

матеріальних ресурсів, здатність адекватно і без суттєвих втрат реагувати на зміни внутрішньої і зовнішньої ситуації.

Фактори, які обумовлюють особливу роль економічної безпеки в системі заходів безпеки діяльності банку: різноманітність інтересів суб'єктів ринку банківських послуг; прагнення суб'єктів ринку до збільшення прибутку, гостра конкурентна боротьба; обмеженість фінансових ресурсів банків та джерел їх формування; нестабільна економічна ситуація, несподівані і різкі її зміни; зростання економічної злочинності в кредитно-фінансовій сфері; підвищений ризик проведення банківських операцій у сучасних умовах; рівень концентрації активів банку у фінансових установах інших держав; рівень концентрації активів банку за галузями економіки або фінансово-промисловими групами; структура власності на банківські установи.

До показників економічної безпеки банку відносять: темпи зростання прибутковості та посилення економічної стабільності; рівень матеріального і соціального забезпечення працівників банку; розмір боргових зобов'язань банку; структура дебіторської заборгованості банку; обсяги використання тіньового капіталу.

Критеріями економічної безпеки банку є: ресурсний потенціал банку і можливості його розвитку; рівень ефективності використання ресурсів; рівень можливостей банку протистояти загрозам його економічної безпеки та самостійно ліквідувати їх; конкурентоспроможність банку; цілісність та масштаби структури банку; ефективність кадрової політики банку.

В сучасних умовах економічна безпека банку зазнає *таких загроз:* низька якість капіталів банків; проведення банками ризикованої кредитної політики; недостатня ефективність банківського нагляду; недостатнє покриття депозитів системою страхування внесків; низька ліквідність банківських активів.

Комплексна система економічної безпеки банку – це комплекс взаємопов'язаних заходів організаційно-правового характеру, що здійснюються спеціальними органами, службами, підрозділами банку, спрямованих на захист життєво важливих інтересів банківської установи від протиправних дій з боку

реальних або потенційних фізичних чи юридичних осіб, що можуть призвести до істотних економічних втрат та забезпечення сталого росту банку у майбутньому.

Існує два принципових *підходи до створення служби безпеки банку* : за допомогою укладення договорів із державними органами охорони, приватними охоронними і детективними фірмами (на повне або часткове здійснення заходів безпеки); створенням власної служби безпеки. Незалежно від вибору варіанта створення служби безпеки, керівник повинен мати спеціаліста на правах заступника, який відповідав би винятково за питання безпеки.

Служба безпеки організується органами управління банку, уповноваженими установчими документами кредитної організації. Її створення починається з внесення відповідного розділу до статуту банку та розробки і ухвалення внутрішнього нормативного акту – статуту (положення) про службу безпеки банку, яким регламентуються цілі і завдання служби, організація її діяльності, вимоги до керівника і співробітників, їх права і обов'язки. Положення про службу безпеки банку затверджується радою директорів банку. Керівник служби безпеки призначається і звільняється з посади органом управління банку. Структура, чисельність і склад служби безпеки банку визначається реальними фінансовими можливостями, масштабом комерційної діяльності, ступенем конфіденційності інформації. Штатний склад служби безпеки комплектується на основі укладання трудових договорів з особами, здатними завдяки своїх особистих і ділових якостей, освіті, професійним навичкам і стану здоров'я виконувати покладені на них обов'язки. Кваліфікаційні вимоги до керівника підрозділу і його співробітників розробляються і приймаються самим банком.

Основними *напрямками діяльності* служби безпеки є: виявлення фактів порушення законів з боку державних структур, випадків перевищення ними встановлених компетенцій в ході здійснення банком фінансової діяльності, недотримання з боку партнерів і клієнтів умов контрактів і договорів, інформування керівництва банку про ці порушення; забезпечення безпеки

банківських операцій; забезпечення охорони майна (включаючи гроші і прирівняні до них цінності), будинків, приміщень, обладнання, технічних засобів забезпечення банківської діяльності; захист інформації (банківської, комерційної, податкової таємниці, інших відомостей конфіденційного характеру, комп'ютерної інформації) і інформаційної інфраструктури; захист системи кадрового забезпечення банку; забезпечення особистої безпеки керівництва банку; організація взаємодії з правоохоронними органами у сфері забезпечення банківської безпеки; розробка і реалізація заходів профілактики протиправних посягань на інтереси банку.

У своїй діяльності служба безпеки банку керується: інструкцією з організації режиму і охорони; інструкцією із захисту комерційної таємниці; переліком відомостей, що складають комерційну таємницю інструкцією з роботи із конфіденційною інформацією для керівників, фахівців і технічного персоналу; інструкцією з організації зберігання справ, що містять конфіденційну інформацію, в архіві; інструкцією з інженерно-технічного захисту інформації; інструкцією про порядок роботи з іноземними представниками і представництвами.

Основні функціональні обов'язки служби безпеки: здійснення розшукової діяльності; здійснення охоронної діяльності; забезпечення особистої охорони керівництва банку; здійснення діяльності із захисту інформації банку; здійснення діяльності нормативного характеру; розробка і реалізація заходів попередження протиправних посягань на інтереси банку.

Функції служби безпеки банку є наступними: *адміністративно-розпорядча* – реалізується за допомогою розробки, встановлення і підтримки в банку різних режимів безпеки, визначення повноважень, прав, обов'язків і відповідальності працівників банку з питань забезпечення безпеки; *обліково-контрольна* – забезпечується організацією своєчасного виявлення реальних і потенційних загроз діяльності банку, несприятливими для банку ситуаціями і факторами; виявлення критичних напрямків фінансово-комерційної діяльності банку; накопичення інформації відносно проблем забезпечення безпеки банку;

соціально-кадрова – реалізується за допомогою участі служби безпеки в підборі, перевірці і розміщені кадрів; виявленні негативних тенденцій в колективах підрозділів банку, можливих причин і умов виникнення соціальної напруги; попередженні і локалізації можливих конфліктів; формування у працівників банку почуття відповідальності за забезпечення безпеки банку; *організаційно-управлінська* – реалізується за допомогою організаційного, матеріально-технічного і технологічного забезпечення режимів безпеки в банку; *методична* – реалізується за допомогою виявлення, накопичення і впровадження в діяльність банку позитивного досвіду уникнення проблем банківської безпеки; організації навчання працівників банку питанням безпеки; розробка методик роботи персоналу банку відносно забезпечення безпеки проведення банківських операцій; *інформаційно-аналітична* – забезпечується шляхом цілеспрямованого збору, накопичення, обробки і розподілу інформації; створення для цього необхідних технічних програмних засобів.

Тема 2 Загрози діяльності банківських установ

План лекції

2.1 Характерні особливості понять «ризик» і «загроза» банківської діяльності

2.2 Сутність недобросовісної конкуренції та промислового шпигунства, їх прояв у банках

2.3 Заходи щодо забезпечення безпеки в роботі з персоналом банку

2.1 Характерні особливості понять «ризик» і «загроза» банківської діяльності

Для характеристики рівня захищеності банку і його конкретних операцій від потенційної небезпеки в економічній науці і банківській практиці використовується поняття «ризик», що є складовим елементом поняття

«небезпека».

Ризик являє собою вірогідність зазнати збитків або упустити вигоду. Поняття «ризик» як міра допустимо (недопустимо) небезпечних умов діяльності (або дій) використовується в комерційній, фінансовій і в інших видах діяльності, як правило, пов'язаних з джерелами підвищеної небезпеки. У цій якості поняття «ризик» застосовується також в і Кримінальному кодексі України (ст. 42 «Дії пов'язані з ризиком»). Проте у всіх інших випадках Кримінальний кодекс України використовує як міру небезпеки поняття «загроза».

Загрози безпеці банку – потенційно можливі або реальні дії зловмисників чи конкурентів, здатні завдати банку матеріальної шкоди. Вони виявляються як сукупність факторів і умов, що утворюють небезпеку для нормального функціонування банку відповідно до його завдань та інтересів.

Об'єктами загроз у банку є: персонал (моральні та фізичні страждання); фінанси (крадіжки коштів та цінностей шахрайство з фінансовими ресурсами, фальсифікація валюти, фінансових документів та цінних паперів); матеріальні засоби (пошкодження будівель, приміщень та іншого нерухомого майна, виведення з ладу засобів зв'язку і систем комунального обслуговування, псування, пошкодження, крадіжки обладнання, техніки і транспортних засобів); інформація (несанкціоноване ознайомлення з відомостями, які охороняються, модифікація, знищення або розголошення).

Фактори, які посилюють активізацію загроз банківської безпеки можна звести до наступного: значна ступінь монополізації ринку, що частково збереглася від колишньої адміністративно-командної системи, частково – виникла в сучасних умовах. Водночас зростає рівень конкурентної боротьби за вітчизняні ринки з боку як вітчизняних, так і зарубіжних банків; встановлення контролю кримінальних структур над деякими секторами економіки (у т.ч. банківському) і суб'єктами господарювання; збереження значного тиску на банківські установи з боку державних органів (наприклад, в сферах ліцензування, оподаткування); зростання криміналізації українського бізнесу

взагалі і частішання використання кримінальними структурами операцій з метою відмивання «брудних» грошей, вивозу їх за кордон тощо; наявність низки соціальних проблем (низький рівень доходів населення, безробіття, текучість кадрів, що знижує ступінь відповідальності і збільшує імовірність схильності працівника до продажу відомостей, що складають банківську таємницю і інших незаконних дій); недосконалість законодавства, що регулює діяльність банківських установ (наприклад, орієнтація правових норм на боротьбу з наслідками правопорушень, а не з причинами); відносна «молодість» вітчизняного ринку банківських послуг і відсутність відпрацьованих засобів і методів забезпечення власної безпеки, відсутність досвідчених фахівців.

Загрози можна класифікувати наступним чином: *стосовно об'єкта посягань*: загрози майну банка (майно банку включає готівкові і безготівкові гроші (національна валюта), валютні цінності і цінні папери, майнові права на об'єкти банківської діяльності (предмети застави тощо), а також будівлі, устаткування, інвентар); загрози інфраструктурі банку; загрози банківській інформації; *стосовно видів діяльності банку*: загрози операційній діяльності (посягання на порядок здійснення банківських операцій та їх інформаційного, правового, організаційного, технічного і технологічного забезпечення); загрози позаопераційній діяльності (посягання на порядок діяльності банку, що виконується поза банківських операцій, а також на майно і прирівняні до нього об'єкти цивільного права); *стосовно осіб, причетних до їх реалізації:* загрози з боку персоналу банку (керівництво банку; особи, що беруть участь у виконанні банківських операцій; особи, що беруть участь в технологічному забезпеченні банківських операцій); загрози з боку осіб, що не входять до числа працівників банку і не пов'язані з банком будь-якими відносинами (юридичні особи (недобросовісні конкуренти, організації, що збирають конфіденційну інформацію та здійснюють інші дії, що суперечать інтересам банку); фізичні особи (кримінальні елементи) і неформальні групи (організовані злочинні групи)); *по відношенню суб'єкта до власних дій,* що створюють загрозу

інтересам банку: злочинний намір, необережність (легковажність або недбалість), невинність; *за заподіяним збитком:* матеріальний; моральний; *за імовірністю виникнення:* досить вірогідні: вірогідні; маловірогідні; *за ступенем тяжкості наслідків:* поправний (незначний) збиток (втрата майна і елементів інфраструктури, які банк може заповнити за рахунок власних засобів без загрози своєму існуванню і без переведення в позаштатний режим роботи); умовно поправний (граничний) збиток (втрата майна і елементів інфраструктури, що створюють загрозу існуванню банку, яку він не може усунути без залучення зовнішніх засобів; непоправний (катастрофічний, значний) збиток (втрата майна і інфраструктури банку, відшкодувати яких не виявляється можливим, його спричинення тягне ліквідацію або реорганізацію банку; за *природою виникнення:* природні або об'єктивні (загрози, викликані стихійними природними явищами, не залежними від людини (землетруси, повені, урагани тощо)); штучні або суб'єктивні (загрози, викликані діяльністю людини); *за причинами появи*: стихійні; навмисні; *за характером дії:* активні; пасивні.

В цілому всі загрози незалежно від їх класифікаційних ознак можна поділити на внутрішні та зовнішні. *Способи реалізації внутрішніх і зовнішніх загроз* безпеці банку: посягання, здійснені із застосуванням насильства і погроз (протиправні діяння насильницького характеру); посягання, здійснені таємно або із застосуванням обману (протиправні діяння ненасильницького характеру).

Захист банку від внутрішніх і зовнішніх загроз повинен мати попереджувальний характер і ґрунтуватися на трьох групах заходів: кадрових, організаційно-технологічних і інтелектуальних. *Заходи кадрового характеру* передбачають: підбір, вивчення, перевірка і відбір працівників банку; мотивацію роботи; контроль роботи; попередження і вирішення конфліктних ситуацій в колективах; робота з працівниками, які звільняються; розроблення системи заходів відповідальності за допущені порушення і зловживання; соціальний контроль окремих категорій працівників банку. *Організаційно-технічні заходи* переважно передбачають: розроблення технологій, які

виключають або ускладнюють шахрайські дії; дотримання принципу «чотирьох очей»; періодичні перевірки і ревізії, щорічний контроль і облік; інформаційно-аналітичні дослідження клієнтів, партнерів, конкурентів, ринку; категоріювання доступу до грошей, матеріальних засобів, цінностей, інформації, документів банку; нагляд за функціонуванням заходів захисту діяльності банку; моніторинг виконання обов'язків клієнтами і партнерами банку; розроблення службових субординацій, описів робочих місць і робочих процесів, розподіл функцій, регулювання розпорядчих і дозвільних повноважень. *Інтелектуальні заходи,* направлені на: формування у працівників банківського патріотизму; розроблення і впровадження Кодексу банківського службовця; організація і проведення заходів виховного і профілактичного характеру, навчання працівників протидії шахрайським посяганням.

Однією з найпоширеніших загроз діяльності банку, яка по своєму походженню може бути як внутрішньою, так і зовнішньою, є *банківське шахрайство.* Згідно Кримінального Кодексу України (ст. 222 «Шахрайство з фінансовими ресурсами») шахрайство визначається як зловживання довірою, обман власника матеріальних цінностей або засобів з метою заволодіння його власністю, розкрадання або придбання права на чуже майно обманним шляхом.

Головною особливістю шахрайства є те, що в основу заволодіння чужим майном або правом на майно зловмисник покладає обман і зловживання довірою, внаслідок чого власник добровільно передає належне йому майно або переуступає право на нього.

Основними видами шахрайського обману, до яких вдаються клієнти банку є: повідомлення неправдивих відомостей про себе і свою діяльність; укриття обставин і фактів, які за відповідних умов взаємодії з банком є істотним й обов'язковим; надання в банк підроблених, фіктивних документів; фальсифікація товарів і послуг.

Основні види зловживань довірою: через цивільно-правові (договірні) відносини; через передання власності (права власності) без застережень та відповідного оформлення.

До особистих мотивів банківського шахрайства можна віднести: скрутний фінансовий стан (непередбачені витрати через хворобу, нещасний випадок, сімейні проблеми); прагнення продемонструвати життєвий рівень, який не відповідає реальним можливостям, спроба не відставати від інших за рівнем життя; алкоголізм, наркотики; прагнення уникнути фінансових труднощів і/чи неприємностей у сімейних стосунках; пристрасть до спекуляції, азартних ігор; жадібність, марнославство, потреба в самоствердженні; збитки у власному бізнесі; необхідність знайти кошти, щоб погасити необмірковано отриманий кредит (віддати борг); марнотратний спосіб життя; схильність до позерства, завищене уявлення про власний статус; незадоволеність роботою або посадою, почуття помсти; спокуса яка виникає після того як випадкові помилки залишились непоміченими; потяг до задоволень і розваг, дорогих захоплень, хобі; виявлення слабких місць в системі контролю і безпеки.

До мотивів банківського шахрайства, які виникають унаслідок дій третіх осіб можна віднести: спроба приховати чи компенсувати збиток, який виник у результаті обману, учиненого клієнтом; залежність від третіх осіб; шантаж банківських працівників; завищені вимоги з боку друзів, коханок/коханців, членів сім'ї. До умов, які сприяють шахрайським діям можна віднести: складні і багатоступінчасті фінансово-економічні зв'язки; некомпетентність і юридична необізнаність громадян; безпечність і надзвичайна довірливість громадян; безвідповідальність працівників і керівників; невдосконаленість законодавчої бази і недоліки в організації фінансово-економічної діяльності.

Найбільша кількість випадків банківського шахрайства припадає на *кредитні операції*.

Виходячи з банківської практики шахрайських дій стосовно кредитних операцій, можна зробити висновок, що ці дії, як правило, стосуються:

1. *У випадку використання застави:* відсутність предмета застави; предмет застави надано в заставу іншому кредитору; предмет застави не є власністю заставодавця; предмет застави має кількох власників, від яких немає

згоди на передавання його в заставу; предмет застави є складовою об'єкта і самостійно функціонувати не може; предмет застави не відповідає кількісно-якісним характеристикам, обумовленим в договорі застави; предмет застави не користується попитом; у договорі застави не обумовлюється порядок користування предметом застави; предмет застави належить державі і перебуває в тимчасовому розпорядженні заставодавця; предмет застави не страхується, і в договорі застави порядок страхування не обумовлений; предмет застави під час дії кредитної угоди реалізується без відома банку.

2. *У разі страхування:* неправильно вибирається предмет страхування (страхується сума кредиту, а не відповідальність за його неповернення); страхова компанія не має ліцензії на даний вид страхування; можливості страхової компанії нижчі, ніж страхова сума; у страховій компанії відсутні правила страхування; неоплачений або запізно оплачений страховий платіж; у страховому договорі не враховані інтереси банку.

3. *У разі поручительства, гарантії:* документи щодо надання гарантій, поручительств підписуються особами, які не мають на те повноважень; надання гарантій, поручительств на суми, які значно перевищують можливості гаранта, поручителя; гарантом, поручителем є родич, або близька позичальнику людина, в тому числі її начальник або засновник, або співзасновник; неповне надання гарантійних документів; змова гаранта, поручителя та позичальника і зникнення їх після отримання кредиту; неправомірне використання найменувань відомих компаній, фірм, їх бланків, печаток тощо під час гарантій, поручительств.

Для ухилення від відповідальності шахраї застосовують прийоми, які дозволяють маскувати їх особисту участь в здійсненні злочину. До основних напрямків такого маскування відносять: отримання кредитів за допомогою підставних осіб; використання чужих паспортів; отримання кредитів дійсними володарями паспорту з подальшою відмовою від факту отримання кредиту за приводом того, що документ був викрадений та використовувався для отримання кредиту іншою особою; використання юридичних осіб (фірм-

«одноденок») для організації розкрадання грошових засобів банку під видом організації споживчого кредитування тощо.

Шахрайство в банках відбувається не лише при проведенні кредитних операцій. Досить часті випадки шахрайських дій і в ході інших банківських операцій. В деяких випадках до шахрайських дій притягуються працівники банку або беруть в них безпосередню участь.

Значну загрозу для вітчизняних банків представляють іноземні схеми шахрайства. Крім цього, значну загрозу для вітчизняних банків представляють компанії, які зареєстровані в офшорних зонах.

Поруч із шахрайством значну загрозу діяльності банку можуть представляти зловживання службовим становищем працівників банку, які виявляються в двох формах протиправних дій: використання посадових повноважень з корисливою метою; перевищення посадових повноважень з корисливою метою.

Характерними ознаками зловживання службовим становищем і скоєння шахрайських дій працівниками банку є: намагається «відгородити» свою ділянку роботи; підкреслює свою потрібність і незамінність; намагається не допускати, щоб його будь-хто заміняв на роботі; відкидає всі пропозиції перейти на іншу ділянку роботи; не йде у відпустку або розбиває її на короткі частини; залюбки береться виконувати роботу на інших ділянках або допомагати своїм колегам; життєвий рівень не відповідає заробітку.

Під час перевірок виявляється: часте коригування проведень, наявність помилкових проведень; часті розбіжності при звірянні матеріальних засобів і коштів; наявність видуманих рахунків; ухилення від контролю, великі проміжки між звіряннями; наявність нестач або надлишків матеріальних засобів і коштів.

Заходи локалізації шахрайських дій і зловживань службовим становищем можна звести до наступного: відсторонення від виконання обов’язків; отримання письмових пояснень щодо вчинків, які трапилися; позбавлення права підпису; передача справ і документів; конфіскація ключів, печаток,

бланків, штампів; вилучення перепусток і службових посвідчень; виключення самостійних дій; оповіщення охорони; за необхідністю оповіщення клієнтів; оповіщення працівників виконуючих спільну роботу; обмеження функцій і повноважень; прийняття рішення про порушення кримінальної справи або подачу позову до суду; анулювання паролів доступу в інформаційні мережі.

2.2 Сутність недобросовісної конкуренції та промислового шпигунства, їх прояв у банках

Форми недобросовісної конкуренції, які використовуються проти банку можна звести до наступного: порушення ритму роботи банку шляхом численних перевірок і ревізій; публікації та передачі, які негативно впливають на імідж і репутацію банку, його керівництво та персонал; встановлення відповідних правил діяльності банків через різноманітні громадські організації банків і банкірів або таємний зговір між ними; переманювання клієнтів та перспективних працівників; зловживання домінуючим положенням на ринку; зміна умов діяльності банків через державні органи; фіктивні пропозиції роботи та неправдиві переговори з метою отримання закритої інформації; неправдива, порівняльна реклама про якість послуг та ефективність діяльності; шантаж керівництва і працівників банку з метою прийняття ними відповідних рішень або виконання окремих дій, які дають можливість конкуренту отримати необхідні переваги.

Однією з несприятливих умов діяльності банку *є промислове шпигунство* – це сукупність заходів, які проводяться з метою несанкціонованого отримання, зміни, знищення інформації банку з обмеженим доступом. Об’єктом промислових шпигунів є інформація з обмеженим доступом, до складу якої можна віднести: документи, дискети, диски, комп’ютерна техніка, аудіо-, відео матеріали, креслення, схеми, карти, а також працівників банку, які є носіями такої інформації.

Метою промислового шпигунства є: викрадення новітніх технологій,

документів, ідей і впровадження їх у власному банку; перехоплення клієнтів і контрагентів; дискредитація або усунення конкуруючих банків з ринку; перепродаж секретів банків-конкурентів; використання викраденої інформації для ведення недобросовісної конкуренції; проведення диверсій.

Сьогодні найбільш відомими і поширеними формами нелегального і напівлегального отримання інформації є: неправдиві переговори з банком; підслуховування розмов, вивідування інформації; підкуп службовців банку, засилання до банку агентів, установлення спеціальних технічних засобів у його приміщеннях для несанкціонованого отримання інформації; спостереження за діяльністю установ банку та його персоналом; опитування фахівців конкурента на виставках, конгресах, конференціях, семінарах; посягання на інтелектуальну власність банку; анкетування фахівців під виглядом запрошення їх на роботу; шантаж і різні форми тиску на джерела інформації банку; викрадення документів, програмних засобів, які використовуються в банку; збирання інформації через закордонні філії, партнерів, клієнтів, спільних постачальників, консультантів, радників, колишніх працівників банку.

Дії промислових шпигунів щодо виявлення працівників банку, з якими може бути організовано співробітництво, зводяться до наступного : вивчення працівників, які працюють на ділянках і напрямах, що є об’єктами зацікавленості промислових шпигунів; виявлення серед працівників банку осіб, на яких є інформація про їх негативне ставлення до банку та його керівництва, невдоволених умовами роботи; виявлення серед працівників банку осіб, які мають негативні риси характеру (пияцтво, наркотична залежність, захоплення азартними іграми тощо), хвороби (як особисто працівника, так і його близьких), невідомі оточуючим; вивчення працівників, які працюють на ділянках і напрямах, що забезпечують діяльність об’єктів зацікавленості промислових шпигунів; виявлення серед працівників банку осіб, щодо яких є інформація про їх протиправну (злочинну) діяльність; використання отриманої негативної інформації для залучення працівників банку до роботи на промислових шпигунів або банків-конкурентів; штучне створення ситуацій, які мають

негативні наслідки для відібраних працівників банку з метою подальшого їх залучання до роботи на промислових шпигунів або банків-конкурентів.

Характерні вади, риси характеру, особливості поведінки працівників банку, на які звертають увагу промислові шпигуні, передусім: пристрасть до азартних ігор, безконтрольність поведінки в стані азарту; егоїзм, самозакоханість, нездоровий кар'єризм; нечесність, недисциплінованість, необов'язковість; заздрість, постійна незадоволеність, потяг до помсти, нездатність до взаєморозуміння, співпереживання; нестриманість, дратівливість, необдуманість вчинків, агресивність; підвищений романтизм, потяг до пригод; підвищене почуття батьківської, подружньої любові; наявність вад і ознак, характерних для поведінки шахраїв, бюрократів; замкнутість, відсутність почуття колективізму, товариськості; схильність до частої зміни обстановки, роботи, свого оточення.

До способів утримання залучених до роботи на промислових шпигунів працівників банку відносять: значна винагорода; взаємодопомога; підтримання страху.

Основними заходами протидії актам недобросовісної конкуренції можуть бути: доскональне вивчення ринків та їх суб'єктів, складання характеристик впливу; визначення найбільш вірогідних конкурентів і складання прогнозів розвитку взаємовідносин з ними; вибір методів поведінки із суб'єктами ринку, використання ділових зв'язків і партнерів для вироблення компромісних рішень із конкурентами; створення нормативної бази банків, яка регламентувала б порядок взаємовідносин персоналу з зовнішнім середовищем; включення до технологій операцій і угод елементів їх захисту; ведення комерційної розвідки в середовищі конкурентів; періодичне оприлюднення результатів своєї діяльності; створення союзів, асоціацій і вироблення відповідних правил поведінки на ринку, які вкладаються в межі добросовісної конкуренції.

2.3 Заходи щодо забезпечення безпеки в роботі з персоналом банку

Банківські фахівці повинні бути не тільки професіоналами, здатними нетрадиційно і творчо вирішувати складні завдання діяльності банку, а й патріотами свого банку, всіляко захищати його інтереси, не допускати правопорушень і злочинних дій. Реалізувати такий підхід можна тільки тоді, коли визначальною фігурою у діяльності банку буде його працівник.

Уся система управління персоналом має бути спрямована на пробудження у працівників різноманітних здібностей, які б максимально використовувались у процесі банківської діяльності, а самі працівники прагнули б до розквіту свого банку. Тобто умови для стабільної діяльності банку створюють високопрофесійні і віддані йому співробітники, боротьба за залучення та виховання яких має бути в центрі уваги кадрової політики банку.

Завданнями управління персоналом банку є: оптимізація системи набору персоналу; організація ефективної роботи персоналу; формування й удосконалення навичок роботи, розвиток виробничої культури й банківського патріотизму; управління діяльністю працівників: розвиток лідерських функцій, ділове планування, постановлення мети, розроблення заходів і оцінка результатів, стимулювання праці і мотивація до розвитку кар'єри; задоволення потреб та інтересів працівників і колективів.

Методами перевірки кандидатів на роботу до банку є: перевірка минулої поведінки; самооцінка; оцінка професійних навичок; психологічне тестування; анкетування; спостереження.

Основні особисті риси працівника банку, яким надається перевага чесність, принциповість, добросовісність, ретельність і пунктуальність у виконанні своїх обов'язків, дисциплінованість, емоційна стійкість, прагнення до успіху і порядку в роботі, самоконтроль вчинків і дій, правильне оцінювання особистих можливостей і здібностей, помірна схильність до ризику, обережність, уміння зберігати таємниці, хороша пам'ять і тренована увага.

Відбір і розстановка кандидатів здійснюється за критерієм найбільшої

відповідності вимогам робочих місць. Крім цього, враховуються перспективи подальшого використання прийнятих на роботу працівників, можливості оволодіння ними новими технологіями банківського виробництва та генерування таких технологій ними самими, відсутність фактів серйозних порушень банківської безпеки та непорозумінь із законом у минулому.

Одне із завдань безпеки – запобігти можливій економічній шкоді, якої може завдати розголошення банківської та комерційної таємниці. Через це, одним із напрямів роботи з кадрами є виховна і профілактична діяльність, яка охоплює сукупність методів впливу на свідомість, почуття, волю, характер працівників банку з метою формування у них уміння зберігати комерційну та банківську таємницю і суворо додержуватись установлених правил роботи в банку. Головними напрямками цієї діяльності можуть бути: формування навичок умілого застосування заходів безпеки для додержання таємниць банку у ході виконання працівниками їх службових обов'язків; створення дійової системи відповідальності за розголошення таємниць банку; формування у працівників банку і його колективів моральних основ банківського патріотизму, які забезпечують протидію посяганням на таємниці банку.

Однією найпоширенішою причиною звільнення працівника як за власним бажанням, так і з ініціативи адміністрації є конфліктні ситуації в колективі. Конфлікти в банку можуть бути внутрішніми (між окремими працівниками, групами працівників одного колективу) і зовнішніми – між колективами підрозділів одного банку та колективами банків.

Сприятливому психологічному стану в колективі значною мірою сприяють *зовнішні фактори*: раціоналізація режиму, інтенсивності, складності, чергування завдань професійної діяльності; забезпечення ефективними сучасними засобами роботи; високий соціальний захист; нормалізація режиму харчування, вітамінотерапія; ефективна кадрова політика, орієнтована на людину.

До *внутрішніх факторів*, спрямованих на попередження конфліктів, слід віднести: повну довіру до співробітників, надання їм максимальної

самостійності; у центрі управління мають бути не плани і робота, а людина та її ініціатива, бо саме вона виконує і плани, і роботу; максимальне делегування функцій управління співробітникам; постійний розвиток мотивації працівників; результат діяльності колективу визначається ступенем його згуртованості.

Тема 3 Організація охорони банківських установ та дії в екстремальних умовах

План лекції

3.1 Обладнання та технічна оснащеність банку

3.2 Режими охорони установ банку

3.3 Дії банківської установи в екстремальних ситуаціях

3.1 Обладнання та технічна оснащеність банку

Охорона банку являє собою комплекс організаційних та спеціальних заходів, спрямованих на обмеження доступу до установ банку, захист його території, приміщень, об’єктів та персоналу від протиправних посягань.

Основною метою організації режиму та охорони є: виключити можливість несанкціонованого проникнення до установи банку та викрадення його матеріальних цінностей або заподіяння шкоди персоналу; створення умов і можливостей для припинення і локалізації протиправних посягань на матеріальні цінності банку та його персонал; попереджання проникнення в службові приміщення, зони, які охороняються, а також на територію банку сторонніх осіб; забезпечення порядку внесення (винесення), ввозу (вивозу) матеріальних цінностей, а також входу (виходу) працівників та клієнтів банку.

Охорона банків має комплексний характер та забезпечується не тільки спеціальними заходами, але і відповідним обладнанням банківських установ. У зв’язку з цим важливою умовою ефективної охорони банків є відповідність установ, приміщень та будівель вимогам та нормам інженерного та охоронного

обладнання, їх технічної укріпленості.

При будівництві, реконструкції або ремонті банківських установ та приміщень необхідно враховувати: досвід забезпечення безпеки діяльності банків; стан криміногенної ситуації в районі, регіоні та в країні в цілому; вимоги нормативних документів Національного банку України, Міністерства внутрішніх справ України; вимоги будівельних норм відносно технічної оснащеності установ та приміщень банку.

Враховуючи специфіку діяльності банківських установ, основною та головною вимогою з точки зору безпеки є регулювання доступу в приміщення банку. Для цього виділяються три зони доступності: територія банку, установа банку та приміщення банку, кожна з яких повинна бути обладнана належним чином. *Територія банку* – це обладнана ділянка місцевості, на якій розташовано безпосередньо установа, сховище та інші приміщення, які необхідні для забезпечення ефективної діяльності банку. Територія банку повинна бути забезпечена: периметральним загородженням, яке не дозволить злочинцю беззаборонно проникнути в банк; периметральною сигналізацією, яка в реальному масштабі часу дозволить охоронцю прийняти необхідні дії; охоронним освітленням, яке буває штатним та тривожним (штатне освітлення використовується для постійного використання в неробочий час, увечері та вночі, навколо та в середині банку. Тривожне освітлення включається у випадку сигналу тривоги від засобів охоронної сигналізації); охоронно-пожежною сигналізацією, яка попереджає про вогненебезпечний стан; системою відеоспостереження, яка документує події в банку; обладнанням системи контролю доступу, яка дозволяє документувати рух персоналу на території банку; обладнанням входів та виходів, вікон, дверей, вентиляційних люків інженерними засобами захисту. Розміщення на території подвір’я будівель, приміщень інших установ, підприємств, а також прокладка транзитних комунікаційних тунелів та прохідних каналів заборонено.

Структура банківських приміщень та їх склад визначається специфікою роботи установи банку та обирається за рішенням керівника банку.

Приміщення установ банку, в яких здійснюються операції з грошовою готівкою та іншими цінностями, конфіденційною інформацією, а також відомостями які складають банківську та комерційну таємницю, доцільно обладнати спеціальними засобами захисту, які попереджають або виключають їх прослуховування, можливість спостерігати сторонніми особами за діяльністю персоналу в цих приміщеннях.

Вимоги щодо обладнання установ банку: кількість входів і виходів у будівлях банку має бути мінімальною і відповідати протипожежним нормам; сховище цінностей та його двері або сейф, що використовуються як сховище цінностей, повинні мати сертифікат відповідності Держстандарту України; внутрішні приміщення касового вузла мають бути ізольованими від інших приміщень банку і недоступними для сторонніх осіб; наявність штучних бар'єрів у будівлях установ банків та особлива конструкція їх периметрів, проходів, приміщень, сховищ; прилади серверних міжбанківських електронних розрахунків та електронної пошти обладнуються резервним електроживленням; приміщення установ банків розташовуються з урахуванням забезпечення оптимальних маршрутів клієнтів і створення максимуму зручностей під час їх обслуговування; апаратура охоронної, охоронно-пожежної і тривожної сигналізації обладнується аварійним електроживленням; віконні прорізи перших, цокольних, підвальних поверхів, приміщень касового вузла, виготовлення й обробка ламінованих карток, архіві, служби безпеки, підрозділів захисту інформації та тих, що прилягають до пожежних драбин, покрівель прибудов, а також вентиляційні канали, люки, шлюзи та інші комунікаційні прорізи захищаються від несанкціонованого доступу; наявність охоронного (чергового та тривожного) освітлення.

Для охорони приміщень банку застосовують багаторубіжну систему захисту: *перший рубіж* охорони захищає будівельні конструкцій, периметри приміщень, віконні та двірні прорізи, люки, вентиляційні канали, теплові вводи, тонкостінні перегородки та інші елементи приміщень, які доступні для проникання зовні; *другий рубіж* охорони контролює простір в середні

приміщення. Сигнал тривоги поступає у випадку несанкціонованого проникання сторонньої особи; *третій рубіж* охорони являє собою засоби для блокування підходів до окремих предметів, елементів, обладнань приміщення, робочих місць.

Одним із охоронних заходів є використання засобів фізичного захисту, до яких належать *природні та штучні бар'єри*, особливі конструкції периметрів, проходів, приміщень, зони безпеки. Природні та штучні бар'єри служать для протидії несанкціонованого проникання на територію банку. До природних бар'єрів відносять особливе розташування установ банку. Основними штучними бар'єрами є огородження території, де розташований банк.

Найважливіший засіб фізичного захисту банку – розподіл його установ та приміщень стосовно зон безпеки, які враховують важливість різних елементів установ банку з точки зору нанесення йому шкоди або збитків від різних видів загроз. Оптимальне розташування зон безпеки та розміщення в них ефективних технічних засобів охорони представляє основу інженерно-технічного захисту банку. Зони безпеки повинні розташовуватися послідовно від загородження навколо території банку до сховищ.

3.2 Режими охорони установ банку

Охорона банків організовується згідно з вимогами законодавчих і нормативних актів, які регламентують порядок, організацію охорони та устаткування банківських установ. Основними нормативними документами з організації охорони установ банку є: Закон України «Про банки і банківську діяльність»; Інструкція з організації охорони установ банків України (Затверджена Постановою Національного банку України від 25 грудня 1998 р. № 548 та наказом МВС України від 25 грудня 1998 р. № 963); Інструкція про вимоги з організації охорони установ банків України (Затверджена Постановою Національного банку України від 29 березня 2001 р.№ 134); Наказ МВС України від 14 квітня 1998 р. № 257 «Про організацію контролю за охоронною

діяльністю підприємств»; Наказ МВС України від 30 грудня 1992 р. № 571 «Про порядок придбання, зберігання, видачі і застосування газової зброї»; Постанова Верховної Ради України від 24 січня 1995 р. №19/95-ВР «Про право власності на спеціальні засоби охорони»; Постанова Кабінету Міністрів України від 07 вересня 1993 р. № 706 «Про порядок продажу і придбання спеціальних засобів самооборони»; Наказ Державного комітету України по нагляду за охороною праці від 5 листопада 1999 р. № 123 «Про визнання охоронної діяльності роботою з підвищеною небезпекою»; Наказ Міністерства охорони здоров'я України від 31 березня 1994 р. № 45 «Про попереднє і періодичне медичне обстеження працівників охорони».

Ефективний режим охорони покликаний забезпечити збереження будівель і приміщень в банку, збереження і контроль за переміщенням матеріальних цінностей, працівників та клієнтів, попередити витік інформації про діяльність банку, підтримувати протипожежну безпеку. Вирішальне значення для режиму охорони грають кваліфікований підбір, підготовка і розставляння сил і засобів охорони, збір і аналіз інформації про стан режиму охорони, а також контроль за функціонуванням служби безпеки банку.

Вибір форм, методів і засобів охорони банку залежить від таких факторів: можливі способи злочинних посягань на банк; характеристика технічної укріпленості банку; наявність і характеристики технічних засобів охорони; наявність уразливих місць у технічній укріпленості банку; вибраний режим охорони установи банку; кількісні й якісні характеристики сил та засобів охорони; режим і характер роботи банку, склад матеріальних і фінансових цінностей; умови розташування банку і його конструкційні особливості.

Режим охорони поділяється за таким ознаками: за терміном перебування об'єктів банку під охороною: цілодобовий, частковий, вибірковий; залежно від сил і засобів, що використовуються для охорони: простий, підсилений; залежно від завдань охорони: пропускний, внутрішньооб'єктовий.

Основні принципи охорони: активність і запобіжний характер охорони (полягає в своєчасному виявленні ознак підготовки злочинних посягань на банк

і виконання заходів щодо їх попередження або протидії); доцільність і обґрунтованість організації режиму охорони банку, своєчасність його посилення, раціональне використання сил і засобів охорони; доцільне поєднання власних можливостей із можливостями державних правоохоронних органів; здійснення охорони за єдиним планом; прихованість і демонстративність охорони залежно від ситуації, яка складається навколо банку; максимальна інформованість сил охорони про всі події, які відбуваються в банку, зміни умов його діяльності; законність, тобто всі дії стосовно охорони банку повинні виконуватись згідно із законодавчими актами та вимогами.

Установи банків організовують охорону власною службою охорони або залучають до охорони на договірних засадах спеціальні підрозділи МВС України (державна служба охорони) або юридичних осіб, яким надано право здійснювати охоронну діяльність (надавати охоронні послуги) згідно з чинним законодавством України. Вибір сил охорони покладається на керівника установи банку.

За використанням сил і засобів охорона ділиться на фізичну і технічну. У свою чергу, фізична охорона здійснюється силами фізичних осіб за допомогою встановлення стаціонарних постів, виділення груп для супроводу вантажів і цінностей, патрульних груп, груп охорони посадових осіб банку.

За рішенням керівника банку і начальника служби безпеки можуть використовуватися такі *види фізичної охорони*:

Цілодобова фізична охорона з використанням відповідних технічних засобів охорони для спостереження сил охорони: у робочий час (фізична охорона з підключенням відповідних технічних засобів для спостереження сил охорони); у неробочий час (охорона за допомогою відповідних технічних засобів із залучанням для спостереження сил охорони);

Технічна охорона забезпечується встановленням в певних місцях технічних засобів охорони. Технічними засобами охорони є: засоби затримання; засоби нагляду за приміщеннями і територією; засоби охоронної сигналізації; засоби, які контролюють правильність виконання своїх обов’язків

черговими охоронниками; засоби тривожної сигналізації; пристрої-пастки; пристрої, які реєструють пронесення заборонених матеріалів і виробів; засоби обліку і накопичення даних з питань безпеки.

Працівники охорони повинні відповідати таким вимогам (згідно Наказу МВС України від 28 лютого 1994 р. № 112): *керівник підрозділів охорони* повинен мати вищу юридичну освіту або стаж роботи не менше трьох років в охоронних, оперативних, слідчих підрозділах органів МВС, СБУ, або стаж служби не менше п'яти років на командних посадах стройових частин і навчальних підрозділів збройних сил, або стаж роботи не менше п'яти років за останні 10 років у структурах, які надають охоронні послуги; *працівники підрозділів охорони* повинні мати вік не менше 18 років, позитивний висновок медичної комісії про відсутність протипоказань виконувати функції, пов'язані з охоронною діяльністю, початкову підготовку до виконання своїх обов'язків з охорони об'єктів і громадян, відсутність інформації про систематичне порушення громадського порядку, зловживання алкогольними напоями або захоплення наркотиками, відсутність пред'явленого обвинувачення в скоєні злочину, притягнення до суду, непогашеної судимості за умисні злочини, а також відсутність вироку суду про позбавлення права займатись охоронною діяльністю, наявність постійного місяця проживання.

Керівник банку або уповноважена ним особа *під час організації охорони:* забезпечує організацію пропускного і внутрішньооб'єктного режиму в установі банку; визначає місця встановлення технічних засобів охорони та їх кількість; визначає кількість технічних засобів охорони для забезпечення відповідного реагування на їх сигнали сил охорони; встановлює конкретні (мінімально можливі) терміни оперативного реагування сил охорони на сигнали технічних засобів; визначає дії працівників банку і сил охорони у разі спрацювання технічних засобів охорони, а також їх дії в непередбачених ситуаціях; забезпечує взаємодію між різними суб'єктами охорони, якщо до виконання завдань охорони залучаються різні суб'єкти; вживає інші заходи, які необхідні для забезпечення надійного збереження цінностей і належного рівня охорони

установи банку.

На випадок розбійного нападу, пожежі, стихійного лиха, інших надзвичайних обставин розробляються плани дій персоналу банку і сил охорони. Згідно таким планам один раз в квартал можуть проводитися відповідні інструктажі або тренування працівників банку.

На випадок пожежі наряд охорони або працівники банку повідомляють про це пожежну охорону, чергового органу внутрішніх справ і управління (відділ) охорони, керівника банку і приймають заходи щодо порятунку цінностей і майна.

Пропускний режим – це встановлений в банку порядок, при якому унеможливлюється безконтрольний прохід (проїзд), внесення (винесення) матеріальних цінностей. Прохід (проїзд), а також вихід (виїзд) співробітників, службовців і інших осіб на територію банку, внесення і винесення матеріальних цінностей проводиться по пропусках через контрольно-прохідні та проїзні переходи. Пропускний режим передбачає: встановлення певного порядку допуску на територію банку працівників та відвідувачів; встановлення певного порядку вивозу (винесення), ввезення (внесення) продукції і матеріальних цінностей; устрій огорожі, освітлення, обладнання контрольно-прохідних і проїзних пунктів (постів) і бюро пропусків засобами сигналізації, зв'язку тощо, необхідною технікою, що забезпечує здійснення пропускного режиму, а також забезпечення їх документацією і інвентарем; визначення кола посадових осіб, що мають право видачі і підпису всіх видів пропусків; обладнання камер схову особистих речей і майданчиків для особистого автотранспорту; порядок документування порушень пропускного режиму.

Обов'язковим на перепустках та посвідченнях є: прізвище, ім'я, по батькові; знак зони доступності; термін дії; право пронесення ручної поклажі; номер перепуски, посвідчення; у посвідченнях – посада. Період перебування співробітників на території банку в робочий і неробочий час визначається керівництвом із проставленим цифровим знаком на посвідченні або перепустці.

Затверджені зразки посвідчень особи, перепусток, відтисків цифрових

знаків, печатки (штампів), що проставляється на посвідченнях і перепустках, списки із зразками підписів керівників або уповноважених осіб, що мають право підписувати посвідчення та перепустку передаються начальникові відділу режиму і охорони під розписку.

Внутрішньооб'єктовий режим охорони банку – створення відповідної системи заходів і правил, спрямованих на забезпечення схоронності матеріальних цінностей, його інформаційних ресурсів, особистої безпеки працівників банку та його клієнтів, аварійної та пожежної безпеки. Він включає: розроблення та введення в дію внутрішнього розпорядку роботи; порядок видачі і зберігання ключів від робочих приміщень, металевих печаток для опечатування дверей приміщень; порядок допуску працівників банку до режимних приміщень; порядок відкривання, закривання і здавання під охорону робочих приміщень; порядок використання індивідуальних карток, призначених для проходу в банк через автоматичні системи доступу; порядок дій сил охорони і персоналу банку у позаштатних ситуаціях; порядок дій працівників банку та сил охорони у разі виявлення пошкоджень, відбитків печаток, відмови роботи індивідуальних карток, втрати ключів, карток, перепусток або металевих печаток; порядок доступу в банк у вихідні і святкові дні.

Обов'язки персоналу банку щодо дотримання режиму охорони полягають у такому: знати та неухильно дотримуватися вимог режиму охорони; своєчасно повідомляти керівника відділу і начальника служби безпеки про необхідність виходу на роботу в неробочий час; постійно мати при собі пропускні документи, пред'являти їх на першу вимогу працівників охорони і забезпечувати надійну схоронність; не передавати нікому, в тому числі і працівникам банку, своїх пропускних документів; дозволяти доступ відвідувачів тільки в межах своєї компетенції, організовувати їх супроводження під час переміщення по банку; виконувати вимоги встановленого в банку внутрішнього розпорядку роботи.

Працівники банку несуть дисциплінарну відповідальність за порушення

встановленого в банку режиму охорони.

3.3 Дії банківської установи в екстремальних ситуаціях

В окремих випадках виникають ситуації, за яких підприємства, банки, установи та їхні працівники піддаються серйозному впливу досить напружених, майже критичних обставин, які характеризуються високим рівнем загрози їхньому здоров'ю, життю та діяльності. Такі ситуації слід визначати як *екстремальні.*

За своїм походженням екстремальні ситуації бувають: психологічного (ідеологічного) характеру; фізичного характеру; стихійного характеру; техногенного характеру.

Класифікуючи екстремальні ситуації *відповідно до характеру їх впливу на банк та його працівників*, можна виділити такі: ситуації, що виникають навколо банку і стосуються тільки його; ситуації, що виникають навколо працівників банку і мають суттєвий вплив на банк; ситуації, що виникають у колективах банку або навколо них і створюють напружені умови їх роботи; ситуації, в які банк або його працівників потрапляють випадково.

Дії екстремальних ситуацій, як правило, спрямовані на завдання банку матеріальної або моральної шкоди та шкоди його працівникам.

Так, *матеріальна шкода банку* може виникати внаслідок фінансових збитків, яких він може зазнавати через вимушеність окремих працівників банку приймати неефективні рішення; втрату майна, обладнання, техніки банку внаслідок їх пошкодження та знищення від терористичних актів, пожеж, стихійного лиха або техногенних аварій і катастроф; упущення вигоди або збитки від несанкціонованої втрати інформації банку з обмеженим доступом; витрат банку, пов'язаних з ліквідацію наслідків дії екстремальних ситуацій.

У свою чергу, *моральна шкода банку* може виражатись у зниженні його іміджу та позицій на ринку. Моральна шкода, завдана працівникам банку, може виявлятись через різні стреси, психологічний розлад у роботі і поведінці,

пониженні психологічної стійкості до різних загроз (страх, невпевненість у собі тощо), порушенні загальноприйнятих принципів моралі.

Крім того, працівники банку можуть зазнавати *фізичної шкоди* від дій екстремальних ситуацій. Насамперед це може бути пов'язано з послабленням їхнього здоров'я, хворобами, каліцтвом, загибеллю тощо.

Основними причинами та джерелами виникнення екстремальних ситуацій можуть бути: недобросовісні дії конкурентів; протиправна діяльність злочинців; різкі зміни правових умов; невиконання зобов'язань партнерами; сили природи; техногенні процеси виробничої діяльності підприємств; безпечна поведінка окремих осіб.

Дії екстремальних ситуацій, як правило, бувають раптовими, внаслідок чого банк та його працівники не мають можливості заздалегідь підготуватись до них і не завжди можуть правильно реагувати на перші ознаки та прояви таких ситуацій. Тому банки повинні прогнозувати можливість створення навколо їхніх установ різних видів екстремальних ситуацій і розробляти відповідні кризові плани. Зокрема *план містить:* заходи щодо захисту персоналу банку, його цінностей, грошей, майна, обладнання, техніки, споруд; заходи, спрямовані на обмеження доступу у банк сторонніх осіб; заходи щодо попередження скоєння будь-яких протизаконних дій, якими може бути створено загрозу наступу екстремальної ситуації; порядок дій при загрозі терористичного акту або у разі його скоєння: схема сповіщення про наявність загрози; заходи щодо евакуації персоналу, грошей, цінностей; схема зв'язку; місце для пункту управління діями банку в період екстремальної ситуації; заходи щодо взаємодії з правоохоронними органами, пожежною службою, службою медичної допомоги; перелік невідкладних заходів, вжиття яких необхідне у зв'язку з ситуацією, що склалася; склад групи управління діями банку в екстремальній ситуації; склад евакуаційних команд та команд рятівників, місце їх розташування та порядок дій стосовно ситуації, що склалася; інструкція персоналу банку про поведінку у разі загрози терористичного акту; список документів цінностей для особливої охорони та

евакуації; графік проведення тренувань щодо дій в екстремальних ситуаціях.

Першочергові заходи щодо забезпечення діяльності банку в умовах дії екстремальної ситуації: сповіщення заінтересованих осіб про: перенесення ділових зустрічей і термінів підписання договорів; тимчасове призупинення фінансових розрахунків; зміни графіків і термінів виконання зобов'язань і проведення операцій; зміну адреси, номерів телефонів, головного офісу (у разі, коли прийнято рішення про перенесення управління діяльністю банку до однієї з його філій); підготовка матеріалів для можливого вирішення в суді питання про визнання екстремальної ситуації форс-мажорними обставинами, які перешкоджають нормальній діяльності банку і виконанню ним договірних зобов'язань.

До складу *групи управління діяльністю банку в екстремальних ситуаціях,* як правило, входять керівник банку, керівники підрозділів безпеки, кадрів, юридичного, фінансового, господарського, інформаційного, по зв'язках з громадськістю.

У межах кризових планів зі складу працівників банку створюються *евакуаційні та рятівні команди.* Особи, які є членами таких команд, проходять відповідну підготовку та інструктажі щодо їхніх дій у період виникнення загрози наступу екстремальних ситуацій та у разі настання таких ситуацій. Зокрема, *евакуаційні команди* вивчають: правила та процедуру евакуації, можливі небезпеки, які можуть виникати у ході екстремальних ситуацій, способи протидії та виходу з них, основні та запасні маршрути евакуації, правила попередження паніки, місця збору персоналу і зосередження матеріальних цінностей, яким загрожує небезпека після евакуації. *Команди рятівників* вивчають найбільш вірогідні місця, у яких можуть переховуватись окремі працівники банку під час настання екстремальної ситуації, правила поведінки з людьми, які перебувають у стресовому стані, стані найвищого емоційного напруження або психологічного розладу, правила надання першої медичної допомоги і транспортування поранених, травмованих, уражених осіб та правила гасіння пожеж і поведінки в приміщеннях, які горять.

Одними із найбільш поширених ситуацій, які виникають у банках, можуть бути ситуації, пов'язані з ідеологічними диверсіями проти них. Під *екстремальною ситуацією, створеною в результаті ідеологічної диверсії,* розуміють нагнітання моральної і психологічної обстановки навколо банку або в його колективах з метою створення високої емоційної напруги в роботі і поведінці персоналу, зниження довіри клієнтів і партнерів до банку, провокування його керівництва до непродуманих рішень і дій. Серед *дій, які спрямовані на проведення ідеологічних диверсій,* можуть бути: тиск на банк шляхом оприлюднення інформації, яка ганьбить банк чи його керівництво; тиск на банк шляхом безпідставного проведення численних перевірок і ревізій, вимог надання різноманітних довідок та звітів; поширення негативних чуток навколо банку; провокація агресивної поведінки щодо банку, його клієнтів, партнерів, акціонерів та персоналу; поширення інформації, яка сприяє виникненню конфліктних ситуацій у колективах банку.

Попереджувальні заходи протидії ідеологічним диверсіям умовно можна розділити на *заходи організаційного та спеціального характеру.*

До першої групи відносять: періодичні публікації, виступи представників банку про його стан і діяльність у засобах масової інформації.

Заходи спеціального характеру, у свою чергу, поділяються на заходи активного характеру – протидії і заходи пасивного характеру – захисту. *Активними заходами* є: установлення авторства і замовників негативних та неправдивих публікацій, виступів (надання інформації), організація та проведення кампанії антидиверсій щодо них; збір фактів недобросовісної поведінки щодо банку з боку джерел ідеологічних загроз (диверсій) тощо.

У свою чергу, *до пасивних заходів* відносять: викриття вигаданого і неправдивого характеру негативної інформації про банк або окремих його працівників, яка з'явилась в його інформаційному просторі; звернення до суду щодо дій окремих осіб та організацій, установ, які поширюють негативну, наклепницьку інформацію про банк; вжиття заходів щодо обмеження каналів подання негативної інформації, впливу її на персонал та клієнтів банку,

недопущення доступу такої інформації в банк; вжиття заходів щодо зміни об'єкта ідеологічних диверсій, модифікації інформації, яка створює негативну ситуацію навколо банку тощо.

Терористичний акт – застосування або загроза застосування насильства за допомогою використання фізичної сили, зброї, вибухових пристроїв щодо окремих осіб, організацій, установ з метою примушення об'єкта дії приймати або відмовитись від прийняття будь-яких рішень чи дій, порушення роботи, виведення з ладу, знищення промислових об'єктів, залякування різних категорій громадян, фізичного усунення небажаних терористам осіб. *Види терористичних актів:* загрози підриву або підрив вибухового пристрою; захоплення заручників; диверсії на об'єктах; розбійні напади; убивства, каліцтво окремих осіб.

Дії адміністрації банку в разі загрози терористичного акту: посилити пости охорони; створити резерв автотранспорту на випадок евакуації; сповістити команди рятівників та евакуаційні команди; установити оперативний зв'язок з правоохоронними органами; застосувати додаткові заходи захисту сімей керівництва банку і вищого менеджменту; уточнити заходи кризового плану щодо дій на випадок терористичного акту; попередити керівників підрозділів банку про готовність до роботи в умовах екстремальної ситуації; забезпечити готовність до негайної роботи групи управління діями банку в екстремальній ситуації.

Дії в разі виявлення загрози нападу на банк: оцінити ситуацію і самостійно або спільно з правоохоронними органами прийняти рішення про протидію наступу загрози; зменшити обсяг цінностей і суму грошових коштів, які одночасно перебувають у банку; посилити охорону банку і його керівництва; перевірити роботу технічних засобів охорони; у разі прийняття рішення про спільні дій з правоохоронними органами, організувати взаємодію з ними; посилити чергові зміни охоронців додатковими засобами захисту; уточнити плани дій банку та його підрозділів у кризових ситуаціях, за необхідності провести тренування; зменшити інтенсивність переміщення транспортних

засобів банку та його керівництва.

Дії підрозділу безпеки в разі здійснення нападу на банк: сповістити персонал банку і вжити заходів до його евакуації або переміщення в безпечне місце; по можливості уточнити час і місце нападу, якщо нападники перебувають у банку, вжити заходів до встановлення їх місцезнаходження; посилити режим охорони банку, сформувати мобільні групи, які будуть контролювати територію банку; змінити місцезнаходження і маршрути переміщення керівництва банку, легендувати його діяльність; блокувати місце перебування і маршрути переміщення зловмисників штучними огорожами і бар'єрами; реєструвати всіх сторонніх осіб, які перебувають у момент нападу в банку, опитати очевидців нападу, направити їх для бесіди із співробітниками правоохоронних орган; вжити заходів, спрямованих на ліквідацію наслідків нападу на банк; у разі затримання нападника (нападників) провести його огляд, вилучити зброю і підозрілі предмети; кожного із затриманих помістити в окреме приміщення і виставити охорону, по прибутті працівників правоохоронних органів передати їм затриманих.

Основні заходи протидії загрозі наступу екстремальної ситуації : запобігання ситуації (створення обстановки, яка б виключала різного роду конфлікти і конфронтацію суб'єктів підприємництва, провокувала злочинні дії кримінальних структур); зниження ефективності впливу ситуації (вжиття заходів безпеки, які забезпечують захист об'єкта); розкриття ситуації (розголошення спроб компрометації, фактів загрози насильницького і морального впливу; звернення уваги до фактів недобросовісної конкуренції, створення суспільної думки навколо можливостей ситуації, звернення в суд чи правоохоронні органи); переведення ситуації на інші об'єкти (страхування об'єктів, ризиків, здоров'я; залучення до протидії загрозі компаньйонів і партнерів); ігнорування ситуації (загроза незначна, а становище об'єкта достатньо стійке і спирається на серйозні сили).

Тема 4 Інформаційна безпека банківських установ

План лекції

4.1 Банківська інформація

4.2 Особливості інформаційної безпеки банку

4.3 Інформаційно-аналітичне забезпечення діяльності банківських установ

4.1 Банківська інформація

Згідно Закону України «Про інформацію» під *інформацією* (у тому числі під відкритою банківською інформацією) розуміється документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Доступ до відкритої інформації забезпечується шляхом: систематичної публікації її в офіційних друкованих виданнях (бюлетенях, збірниках); поширення її засобами масової комунікації; безпосереднього її надання заінтересованим громадянам, державним органам та юридичним особам.

Порядок і умови надання громадянам, державним органам, юридичним особам і представникам громадськості відомостей за запитами встановлюються Законом України «Про інформацію» або договорами (угодами), якщо надання інформації здійснюється на договірній основі. Обмеження права на одержання відкритої інформації забороняється законом. Переважним правом на одержання інформації користуються громадяни, яким ця інформація необхідна для виконання своїх професійних обов’язків.

Інформація з обмеженим доступом – це будь-яка інформація, що знаходиться у розпорядженні банку, не є загальнодоступною та для якій встановлено спеціальний режим збору, зберігання, обробки, поширення та використання. Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є

предметом суспільного інтересу і якщо право громадськості знати цю інформацію переважує право на її захист.

Відповідальність персоналу банку за порушення правил роботи з інформацією з обмеженим доступом: дисциплінарна (згідно Кодексу законів про працю в Україні); матеріальна (згідно Кодексу законів про працю в Україні); кримінальна (згідно Кримінального Кодексу України); цивільна (згідно Цивільного Кодексу України); адміністративна (згідно Кодексу України про адміністративні правопорушення).

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну. *Конфіденційна інформація* – відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб, поширюється за бажанням власників відповідно до передбачених ними умов. Відповідно до ч. 3 ст. 30 Закону України «Про інформацію», власникам конфіденційної інформації надано право самостійно включати її до категорії конфіденційна, визначати режим доступу до неї і встановлювати систему (способи) її захисту. Виключення становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлений Верховною Радою України за клопотанням Кабінету Міністрів України (з питань статистики, екології, банківської діяльності, податків тощо), а так само інформація, укриття якої являє собою загрозу життю й здоров'ю людей. До *таємної інформації* належить інформація, що містить відомості, які становлять державну й іншу передбачену вітчизняним законодавством таємницю, розголошення якої несе загрозу особам, суспільству, державі. Так, до *банківської таємниці* належить інформація про діяльність і фінансовий стан клієнта, яка стала відома банку в процесі його обслуговування і взаємовідносин з ним або третіми особами при час надання послуг банком, розголошення якої може завдати матеріального або морального збитку клієнту. Також, до банківської таємниці відносять: відомості про стан рахунків клієнтів, у тому числі й кореспондентських рахунків банків; операції, проведені на користь або за дорученням клієнта, виконані ним угоди; фінансово-

економічний стан клієнта; система охорони банку і клієнта; коди, які використовуються банками для захисту інформації; інформація про організаційно-правову структуру юридичної особи-клієнта, його керівників, напрямки діяльності; відомості про комерційну діяльність клієнта, його комерційну таємницю, будь-який із проектів, винаходів, зразків продукції та інша комерційна інформація; звітність окремого конкретного банку, за винятком тієї, яка підлягає опублікуванню; інформація про банки і клієнтів, що збирається під час проведення банківського нагляду.

Заходи, які проводяться банками з метою збереження банківської таємниці: обмеження кола осіб, які мають доступ до інформації, що становлять банківську таємницю; організація спеціального діловодства з документами які містять банківську таємницю; застосування технічних засобів для запобігання несанкціонованого доступу до електронних та інших носіїв інформації; застосування заходів попередження по збереження банківської таємниці і відповідальності за її розголошення в договорах і угодах між банком і клієнтами.

Згідно Закону України «Про підприємства в Україні» під *комерційною таємницею* розуміються відомості, пов'язані з виробництвом, технологічною інформацією, управлінням фінансами та іншою діяльністю підприємства, розголошення яких може завдати шкоди інтересам підприємства. Критерії визначення відомостей, які становлять комерційну таємницю: новизна інформації та термін її «життя»; економічна ефективність використання; наявність аналогової інформації; вартість заходів захисту інформації, джерело отримання інформації; конкурентоспроможність інформації.

Нормативні документи банку з питань захисту інформації:

закріплення права банку на комерційну таємницю та організацію її захисту у його Статуті;

Положення про порядок підготовки, надсилання, обробки та зберігання електронних документів під час використання електронної пошти;

Положення про режимні приміщення банку;

Концепція безпеки банку;

Пам’ятки, зобов’язання щодо збереження в таємниці працівниками банку відомостей, що становлять комерційну, банківську таємницю та конфіденційну інформацію;

Інструкція щодо дій у випадку компрометації криптографічних ключів в установах банку;

Положення про забезпечення безпеки при наданні послуг з міжнародними банківськими платіжними засобами;

Положення про комерційну таємницю банку і його конфіденційну інформацію, тощо.

До профілактики та попереджання посягань на інформацію банку з обмеженим доступом відносять: підбір і перевірка персоналу банку; розроблення відповідної нормативної бази з питань інформаційної безпеки; контроль дотримання працівниками банку правил інформаційної безпеки; визначення ступеня таємності інформації, облік відомостей, що мають обмежений доступ; розмежування доступу до відомостей, що становлять банківську, комерційну таємницю та конфіденційну інформацію; проведення ефективної політики мотивації та стимулювання праці; періодичне проведення аналізу та тестування стійкості системи захисту інформації в електронних системах і мережах банку; аналіз способів посягання на інформацію з обмеженим доступом, своєчасне вироблення заходів протидії ним; обладнання місць зберігання носіїв комерційної таємниці засобами захисту; правове та спеціальне (щодо заходів захисту інформації) навчання персоналу банку; організація спеціального діловодства у банку; упровадження в систему захисту інформації спеціальних технічних засобів діагностики випадків несанкціонованого доступу до інформаційної мережі банку; проведення заходів дезінформації щодо місць зберігання, носіїв та важливості інформації.

4.2 Особливості інформаційної безпеки банку

Інформаційна безпека – це стан захищеності життєво-важливих інтересів особи, суспільства і держави в інформаційній сфері від внутрішніх і зовнішніх загроз. Забезпечення інформаційної безпеки в загальній постановці проблеми може бути досягнуте лише при взаємопов'язаному вирішенні трьох проблем, а саме: перша – захист інформації, що знаходиться в системі, від дестабілізуючої дії зовнішніх і внутрішніх загроз інформації; друга – захист елементів системи від дестабілізуючої дії зовнішніх і внутрішніх інформаційних загроз; третя – захист зовнішнього середовища від інформаційних загроз з боку даної системи.

Інформаційна інфраструктура банку включає: інформаційні ресурси; технічні інформаційні системи і засоби (ТІСЗ); інженерні системи, їх життєзабезпечення; приміщення, в яких функціонують інформаційні системи і обробляється банківська інформація. З інформаційною інфраструктурою нерозривно пов'язані персонал і клієнти.

Інформаційні ресурси банку складаються з вихідної банківської інформації, баз даних, системного, мережного, операційного і інструментального програмного забезпечення, процесорного обладнання і устроїв довготривалої і оперативної пам'яті, в яких безпосередньо розміщується (обробляється і зберігається) інформація, представлена як в документальній формі, так і в іншій, зручною для електронної обробки.

Банківська інформація формується банківським персоналом і безпосередньо обробляється в Автоматизованій Системі Обробки Інформації (АСОІ) з використанням інтегрованих пакетів прикладних програм, що складає Автоматизовану Банківську Систему (АБС).

Під *безпекою інформаційної інфраструктури* банку розуміється її властивість захищеності, виражена в здатності протистояти або протидіяти випадковим або навмисним деструктивним діям природного або штучного характеру на нормальний процес функціонування банківських електронних технологій, здатним завдати збитку власникам і користувачам інформації.

Неправомірне отримання інформації здійснюється через: мимовільний її витік (мимовільне поширення інформації за рахунок технічних або експлуатаційних особливостей певного обладнання, втрати, пошкодження, знищення документальних та програмних носіїв інформації у результаті дії стихійного лиха, поширення інформації через потрапляння в інформаційні мережі комп'ютерних вірусів, інші випадки, які не мають навмисного характеру); розголошення (умисне або необережне повідомлення інформації, опублікування, передавання, надання для ознайомлення, пересилання, втрат її особами, яким вона була відома у зв'язку з їх професійною діяльністю і коли у цьому не було службової необхідності); несанкціонований доступ (доступ до інформації, що здійснюється з порушенням установлених правил розмежування доступу).

Усі зазначені вище шляхи отримання інформації можуть використовуватись конкурентами, спецслужбами, промисловими шпигунами за допомогою створення так званих каналів витоку та передавання інформації.

Каналами витоку інформації можуть бути: оптичні, радіоелектронні, акустичні, акусто-реформуючі, матеріально-речові. У свою чергу, ці канали передбачають створення відповідних умов для переходу інформації від її носія до споживача.

До факторів, які сприяють створенню умов для витоку (передаванню) інформації відносять: безконтрольне використання інформаційних систем і мереж; наявність передумов для виникнення в колективах та серед працівників підприємств, фірм, банків конфліктних ситуацій тощо.

Захистити об'єкти від витоку інформації можна за допомогою:

а) пошукових досліджень на об'єкті: виявлення вмонтованих пристроїв та їх комунікацій, в інтер'єрі приміщень; обстеження комунікацій з погляду можливого їх використання для організації каналів витоку інформації; обстеження діючої апаратури зв'язку, комп'ютерної, розмножувальної техніки з погляду можливої їх обробки з метою створення каналу витоку інформації; вивчення можливості активного впливу на електронне обладнання і базу даних

комп'ютерних мереж;

б) організаційно-режимних заходів: інформування осіб зайнятих у роботі з інформацією та охоронно-режимних заходах, про можливі канали витоку інформації, заходи захисту і виявлення ознак посягань на інформаційні ресурси банку; упровадження режиму спеціального діловодства і створення системи збереження документів і носіїв інформації; формування переліку відомостей, які становлять комерційну таємницю, і визначення правил поводження цими відомостями, тощо.

Захистити інформацію, що міститься у системах і мережах передавання та обробки даних банку, можна за допомогою наступних заходів: *апаратних:* перешкоджання візуальному спостереженню і дистанційному підслуховуванню; нейтралізація паразитних електромагнітних випромінювань і наводок; виявлення несанкціоновано встановлених технічних засобів підслуховування і технічного запису; захист інформації, що передається засобами зв'язку і міститься в системах автоматизованої обробки даних; *програмних:* захист інформації від несанкціонованого копіювання або руйнування; захист інформації від несанкціонованого доступу до неї; *криптографічних:* виконання відповідних дій з перетворення сигналу, який передається, в такий, що є абсолютно незрозумілим для сторонніх осіб; створення умов дешифрування інформації тільки протягом часу, необхідного для втрати її цінності.

Загроза безпеці інформації – виникнення такого явища або події, наслідком якої можуть бути негативні дії на інформацію: порушення фізичної цілісності, логічної структури, несанкціонована модифікація, несанкціоноване отримання, несанкціоноване розмноження.

Основоположними параметрами, визначаючим цільову спрямованість захисту інформації є вид загроз та джерело загроз.

4.3 Інформаційно-аналітичне забезпечення діяльності банківських установ

В основі формування інформаційних ресурсів лежать методи збору інформації, характерні для розвідувальної діяльності. Тому заходи інформаційно-аналітичного забезпечення діяльності банку перш за все повинні ґрунтуватися на засадах комерційної розвідки. Разом з тим під комерційною розвідкою розуміють сукупність заходів щодо збору і обробки інформації про стан і можливі перспективи діяльності суб'єктів відповідного ринку, які виконуються за допомогою спеціальних методів силами комерційних підприємств, фірм, банків або спеціалізованих організацій (установ).

Структуру комерційної розвідки складають організація розвідувальних кіл, збирання необхідних відомостей і інформаційно-аналітична робота. Ця структура є сукупністю взаємопов'язаних елементів розвідувальної системи, вилучення будь-якого з них веде до припинення функціонування всієї системи.

Мета комерційної розвідки завжди направлена на недопущення неочікуваної появи несприятливих факторів для діяльності банка; забезпечення об'єктивною інформацією для прийняття відповідних рішень керівництвом.

Об'єктами комерційної розвідки є перш за все конкуруючі структури, підприємства, організації, які надають подібні послуги, виробляють аналогічні товари або в тій чи інший спосіб впливають або можуть впливати на діяльність даного підприємства, банка, та в яких зосереджена або проводиться необхідна даному підприємству, банку інформація. Об'єктами комерційної розвідки також можуть бути технології виробництва товарів або послуг, комерційні операції.

Об'єктами інформації для діяльності сил комерційної розвідки банку можуть бути: банки; підприємства, організації, які надають фінансові послуги; підприємства, організації, банки контрагентів, клієнтів, партнерів; інформаційні агентства; установи засобів масової інформації; громадські та політичні організації; семінари, конференції, збори, зустрічі (офіційні і неофіційні), інші заходи колективного обговорення питань, які цікавлять банк; окремі установи

та організації.

Безпосереднє отримання інформації може здійснюватися через відповідні носії (джерела) такої інформації. Джерелами необхідної для комерційної розвідки інформації можуть бути: персонал об'єкта інформації; звільнені працівники об'єкта інформації; персонал банку, працівники ЗМІ, інших установ і організацій; члени громадських і політичних організацій; приватні детективи; інші категорії громадян, які за тих або інших причин мають доступ до відповідної інформації; документи; карти, схеми, креслення; фотокопії, фотографії; законодавчі та нормативні акти; матеріали засобів масової інформації; аудіо- і відеозаписи; чернетки, відходи виробництва і діловодства; наукові видання, результати наукових досліджень; рекламні продукти; електронні носії інформації: комп'ютери, дискети, диски та ін.

Зважаючи на специфіку діяльності банків і структуру їх інформаційного простору, сфера інформаційної уваги може включати: *сфера інтересів банку* – інформація про об'єкти, регіони, галузі економіки, до яких прагне проникнути банк в майбутньому; про події й об'єкти, які можуть формувати умови майбутньої діяльності банку; *сфера впливу* – характеризується інформацією про події й об'єкти, які можуть впливати на поточну діяльність банку, а також дії банку, що здійснюються в межах попередньої сфери; *сфера безпосередньої діяльності банку* – вся інформація про події й об'єкти, які перебувають у прямому зв'язку з діяльністю банку, та які характеризують або впливають на проведення тієї або іншої банківської операції.

Як правило, банки забезпечують роботу сил безпеки у всіх сферах інформаційної уваги і використовують інформацію: сфери інтересів – *стратегічну* для прийняття рішень відносно довгострокових угод, договорів, планування перспектив розвитку банку; сфери впливу – *тактичну* для прийняття рішень відносно співпраці з партнерами, інвестування (вкладення) засобів в нові проекти, протидії недоброговісній конкуренції, визначення поведінки на ринку в той або інший проміжок часу; сфери безпосередньої інформаційної діяльності – *оперативну* для прийняття рішень відносно

безпосереднього здійснення конкретної операції, укладення конкретного договору.

Отримання інформації в сферах інформаційної уваги здійснюється через відповідні канали: *інформаційний канал «текст»* – загальні публікації, спеціальні публікації, бази даних. Характеристика каналу: наявність великих обсягів «свіжої» інформації, хоча і не зовсім об'єктивної. Місткість каналу – 40– 60% інформації; *інформаційний канал «банк, фірма»* – персонал, клієнти, партнери. Характеристика каналу: технологічна, ділова інформація, інформація про окремих суб'єктів і окремі події, приблизно точна і об'єктивна. Місткість каналу – 30-40% інформації; *інформаційний канал «консультант»* – нормативні документи, експерти, радники, консультанти, органи управління, політичні і громадські організації. Характеристика каналу: достовірна інформація. Місткість каналу: 10-15% інформації; *інформаційний канал «бесіда»* – усі види ділового спілкування: конференції, семінари, переговори, зустрічі, презентації, виставки, наради. Характеристика каналу: достовірна інформація на перспективу. Місткість каналу – 5% інформації; *інформаційний канал «джокер» (випадок)* – випадкова інформація. Місткість каналу: 0-100% інформації.

Основними заходами інформаційно-аналітичної роботи банків є інформаційний аудит і інформаційний моніторинг.

Під *інформаційним аудитом* розуміють проведення інформаційних досліджень підрозділів і установ банку з метою вивчення і оцінки наявної інформації. В ході інформаційного аудиту здійснюється і визначається: склад інформації підрозділів і установ; джерела, форми і регламент отримання інформації; можливості щодо використання отриманої інформації в інших підрозділах банку; можливості інформації щодо трансформації в різні її види (ділову, фінансову, стратегічну, тактичну, оперативну, конфіденційну, відкриту тощо); вибір і формування інформації для використання в інтегрованих базах даних; ступінь захисту інформації.

Під час *інформаційного моніторингу* проводиться контроль надходження

інформації з метою визначення її важливості, цінності і можливості використання в інтегрованих базах даних. В ході моніторингу визначається і здійснюються: оцінка інформації та її розподіл за інформаційними базами даних; виявлення неправдивої або шкідливої інформації і визначення джерел надходження такої інформації; формування інформаційних потоків залежно від завдань, які вирішує банк; своєчасна реакція на зміни інформаційних каналів, пошук додаткових джерел інформації.

Структура інформаційно-аналітичної роботи має всі ознаки структури комерційної розвідки і передбачає організацію роботи, збір інформації та її обробку.

Обробка інформації забезпечується через: накопичення, оцінку й аналіз інформації; класифікацію інформації, її зіставлення і формування гіпотез; інтерпретації інформації; створення інтегрованих баз даних; розподіл інформації, розробка інформаційних документів. Інформаційно-аналітична робота в загальному вигляді направлена на створення моделі відповідного об'єкту (людина, фірма, виробництво), діяльності (банківські операції, взаємовідносини суб'єктів на ринку банківських послуг), стан (рівень розвитку, основні показники) тощо на основі отримання і аналізу інформації. Створення таких моделей є продуктом інтелектуальної діяльності конкретної людини, фахівця служби безпеки.

Під час побудови моделі використовується *низка специфічних прийомів:* порівняння; аналіз; узагальнення; абстрагування – розгляд предмету, явища, елементу інформації відірвано від будь-якої реальності; трансформація.

Основними завданнями інформаційно-аналітичного підрозділу є: участь у формуванні інформаційних ресурсів банку; створення інтегрованих інформаційних баз даних; інформаційно-аналітичне дослідження об'єктів інформаційної уваги банків; організація і проведення інформаційного аудиту підрозділів банку і інформаційного моніторингу; розроблення інформаційних документів для забезпечення управлінських рішень керівництва банку; прогнозування розвитку ринку банківських послуг, ролі та місця банку на

ньому; інформаційно-аналітичне дослідження клієнтів, партнерів, конкурентів та інформаційне забезпечення операцій і угод банку.

В свою чергу, *завдання підрозділів економістів-аналітиків* установ банку полягає в такому: аналіз ефективності технологій банківських операцій і послуг, які використовуються підрозділом; проведення інформаційного аудиту; інформаційно-аналітичне дослідження ринку послуг підрозділу, їх реклама, просування послуг на ринок; участь в інформаційно-аналітичних дослідженнях клієнтів, партнерів і конкурентів, інших суб'єктів ринку банківських послуг; пропозиції щодо оптимізації і удосконалення форм і методів діяльності підрозділів.

МОДУЛЬ 2 ОРГАНІЗАЦІЙНІ ТА УПРАВЛІНСЬКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМСТВА

ЗМ 3 Організація та управління майновою й особистою безпекою підприємця

Тема 1 Теоретичні основи управління безпекою підприємця

План лекції

1.1 Поняття безпеки підприємця. Особиста безпека підприємця

1.2 Внутрішні та зовнішні загрози підприємця

1.1 Поняття безпеки підприємця. Особиста безпека підприємця

Кризовий стан економіки, активна діяльність структур економічної розвідки, організованої злочинності, корумпованих чиновників, повсякчасне застосування жорстких методів конкуренції, у тому числі і недобросовісної, відкриті посягання на майнові і особисті права підприємців створюють серйозну загрозу ефективній діяльності підприємств і економіці в цілому. За цих умов забезпечення безпеки своєї діяльності стає життєвою необхідністю, одним із базових принципів функціонування суб'єктів господарювання.

Особиста безпека підприємця – поточний стан захищеності її життєдіяльності від безпосередніх загроз її життю, здоров'ю, тілесній неушкодженості особистій свободі, а також діяльність суб'єктів безпеки і сил безпеки з організації та практичного здійснення заходів, спрямованих на забезпечення особистої безпеки індивідуально визначеної фізичної особи шляхом відвернення та/або недопущення негативного безпосереднього впливу

факторів кримінального, побутового або екологічного характеру на стан її життєдіяльності.

Головна мета особистої безпека підприємця підприємця полягає в тому, щоб виключити можливість заподіяння йому збитків або упущення вигоди та забезпечити ефективну його діяльність якісну реалізацію всіх планів та гарантувати його стабільне й максимально ефективне функціонування тепер та високий потенціал розвитку в майбутньому.

Виходячи з мети, *основними завданнями особистої безпеки підприємця* є: захист законних інтересів особистої безпека підприємця та його співробітників; профілактика та попередження правопорушень і злочинних посягань на власність і персонал підприємства; своєчасне виявлення реальних і потенційних загроз, вжиття заходів щодо їх нейтралізації; виявлення внутрішніх і зовнішніх причин і умов, які можуть сприяти заподіянню підприємцю, його працівникам матеріальної, моральної та іншої шкоди та перешкоджати їх нормальній діяльності; виховання та навчання персоналу з питань безпеки; послаблення шкідливих наслідків від акцій конкурентів та злочинців з підриву безпеки; збереження й ефективне використання фінансових, матеріальних та інформаційних ресурсів підприємця тощо.

Мета забезпечення особистої безпеки підприємця полягає у фізичному захисті підприємця від загроз його життю, здоров'ю та матеріальному благополуччю, а також законних прав і інтересів у сфері підприємницької діяльності.

Забезпечення особистої безпеки персоналу, зокрема головних посадових осіб фірми, передбачає: охорону з використанням охоронців; власну безпеку особи, що виявляється у фізичній готовності до відбиття злочинних дій, психологічній готовності до сприйняття критичних умов реагування на них; використання засобів власної безпеки, дозволених для використання в особистих інтересах відповідними законами, зокрема собак.

Особисту безпеку можуть гарантувати особисті охоронці, що поряд з високими моральними якостями уміють володіти собою в критичні ситуаціях, здатні швидко й рішуче діяти за будь-яких обставин.

Основними *принципами,* впровадження яких у систему безпеки підприємства підвищить її ефективність, є: 1) системність – створення такої системи безпеки, яка забезпечила б захищеність підприємства, його майна, персоналу, інформації, різних сфер діяльності від небезпек і загроз, форс-мажорних обставин. У забезпеченні безпеки підприємства повинні брати участь всі співробітники підприємства. Організаційною формою комплексного використовування сил і засобів повинна стати програма забезпечення безпеки підприємства; 2) своєчасність – виявлення різних деструктивних чинників, вживання заходів щодо запобігання їхній шкідливій дії і нанесення збитку підприємству; 3) безперервність – система безпеки повинна бути побудована так, щоб вона діяла постійно, захищаючи інтереси підприємства в умовах ризику; 4) плановість – організованість у функціонуванні системи безпеки.

Діяльність щодо забезпечення безпеки організовується на основі єдиного задуму, визначено в комплексній програмі та конкретних планах за окремими напрямами і підвидами безпеки. *До основних елементів системи безпеки* підприємства належать: захист комерційної таємниці і конфіденційної інформації; комп'ютерна безпека; внутрішня безпека; безпека будівель і споруд; фізична безпека; технічна безпека; безпека зв'язку; безпека перевезень вантажів і осіб; екологічна безпека; конкурентна розвідка тощо.

Методика побудови системи економічної безпеки підприємства охоплює такі *етапи:*

– вивчення специфіки бізнесу підприємства, сегмента, який воно займає на ринку, штатного розпису, а також знайомство з персоналом;

– аналіз зовнішніх і внутрішніх загроз економічній безпеці підприємства та вивчення інформації про кризові ситуації, їхні причини і шляхи врегулювання;

– аудит наявних засобів із забезпечення безпеки й аналіз їх відповідності виявленим загрозам;

– моделювання нової системи економічної безпеки підприємства: розроблення плану усунення виявлених під час аудиту недоліків; підготовка пропозицій щодо удосконалення системи економічної безпеки, розрахунок усіх видів необхідних ресурсів; планування щомісячних витрат на забезпечення функціонування системи економічної безпеки (бюджет);

– затвердження керівництвом моделі нової системи та бюджету на її утримання;

– формування нової системи економічної безпеки;

– оцінка ефективності сформованої системи, а також її удосконалення.

Основне значення системи економічної безпеки підприємства полягає в тому, що вона повинна мати *попереджувальний характер*, а основними критеріями оцінки її надійності та ефективності є: забезпечення стабільної роботи підприємства, збереження і примноження фінансів і матеріальних цінностей; попередження кризових ситуацій, у тому числі різних надзвичайних подій, пов'язаних з діяльністю зовнішніх або внутрішніх супротивників.

У кризові періоди розвитку найбільшу небезпеку для підприємства становить руйнування його потенціалу (виробничого, технологічного, науково-технічного і кадрового) як головного чинника життєдіяльності підприємства, його можливостей. У такому випадку необхідно розроблення *стратегії економічної безпеки,* яка повинна містити: характеристику зовнішніх і внутрішніх загроз економічній безпеці підприємства; визначення і моніторинг чинників, що зміцнюють або руйнують стійкість його соціально-економічного положення на короткострокову і середньострокову перспективу; розроблення економічної політики, що охоплює механізми обліку, які впливають на стан економічної безпеки чинників; напрями діяльності підприємства щодо реалізації стратегії.

Організаційними заходами, що забезпечують реалізацію стратегії економічної безпеки, є: створення координаційного центру на чолі з керівником

організації, оперативним органом якого є служба безпеки; розроблення і затвердження наказом по підприємству нормативно-методичного забезпечення стратегії; ресурсне забезпечення і цільове використання ресурсів.

Комплексна система економічної безпеки підприємства має включати в себе комплекс взаємозв'язаних заходів організаційно-правового характеру, що здійснюються спеціальними органами, службами, підрозділами суб'єкта господарювання, спрямованих на захист життєво важливих інтересів особистості, підприємства і держави від протиправних дій з боку реальних або потенційних фізичних або юридичних осіб, що можуть призвести до істотних економічних втрат та забезпечення економічного зростання в майбутньому.

1.2 Внутрішні та зовнішні загрози підприємця

Підприємницька діяльність неможлива без захищеності життєво важливих інтересів підприємців від внутрішніх і зовнішніх загроз. Основними причинами виникнення економічних загроз можуть бути: недостатня адаптація підприємця до постійно змінних умов ринку; загальна неплатоспроможність суб'єктів господарювання; зростаюча злочинність; споживчий менталітет значної кількості громадян; низький рівень трудової дисципліни та відповідальності працівників підприємницьких структур; недостатнє правове регулювання підприємницької діяльності; низький професійний рівень частини керівного складу і працівників суб'єкта підприємницької діяльності.

Зовнішні загрози для безпеки суб'єкта підприємницької діяльності можуть утворюватись: вітчизняними й іноземними кримінальними елементами і структурами; конкурентами; засобами масової інформації; окремими представниками державних установ; приватними детективними фірмами; колишніми працівниками суб'єкта підприємницької діяльності; консультантами та радниками, які не є працівниками суб'єкта підприємницької діяльності; клієнтами та партнерами; контролюючими органами та аудиторськими організаціями; стихійними лихами.

Зовнішніми загрозами безпеці підприємницької діяльності є: криміналізація економіки і падіння виробництва; недосконалість законодавчої бази та державної економічної політики; нерозвиненість ринкової інфраструктури та відсутність найважливіших інститутів ринкової економіки; деформованість економіки, її монополізація і низька конкурентоспроможність; злочинні дії кримінальних угруповань тощо.

У свою чергу, *внутрішні загрози* в основному утворюються: працівниками суб'єкта підприємницької діяльності; недосконалими технологіями виробництва та неповним його врегулюванням нормативними актами суб'єкта підприємницької діяльності; через недосконалу систему захисту інформації. Внутрішні загрози, як правило, обумовлюються наявністю передумов для негативних, протиправних дій персоналу суб'єкта підприємницької діяльності, безконтрольним використанням засобів виробництва, порушенням режимів діяльності суб'єкта підприємницької діяльності. Ураховуючи, що значна частина внутрішніх загроз реалізуються з участю або за сприяння персоналу суб'єкта підприємницької діяльності, можна вважати, що основним джерелом таких загроз є власні працівники.

Внутрішні загрози суб'єкта підприємницької діяльності можуть утворюватися внаслідок: непрофесійних дій працівників суб'єкта підприємницької діяльності; низького стану виховної та профілактичної роботи; недосконалої системи заробітної плати та стимулювання праці персоналу; порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи; психічних та комунікаційних особливостей працівників; відсутності нормативної бази, яка б установлювала режими їх діяльності та правила поведінки персоналу; низького стану трудової і виробничої дисципліни, слабкої вимогливості керівного складу суб'єкта підприємницької діяльності.

Внутрішні загрози безпеки є постійними і не залежать від ролі, місця, значення суб'єкта підприємницької діяльності або наявності зовнішніх загроз.

Забезпечення безпеки підприємницької діяльності вимагає створення комплексної режимно-охоронної системи; системи роботи з кадрами, вдосконалення методик та процедур застосування оперативно-технічних засобів зв'язку; взаємодії комерційних служб безпеки з державними правоохоронними органами.

Однією з умов забезпечення безпеки є зниження ризиків підприємницької діяльності. До факторів, що визначають рівень ризику, можна віднести наступні. *Політичний фактор.* Безпека підприємницької діяльності багато в чому залежить від політичної стабільності в суспільстві. Знання політичної ситуації дуже важливо для компанії і окремого підприємця для маневрування і прийняття адекватних рішень. *Нормативно-правовий фактор.* Цей стан системи законів і нормативних актів, що визначають «правила гри» на ринку. *Економічний чинник.* Він визначається внутрішньою і міждержавною економічної ситуацією. Можна виділити наступні види ризику; фінансовий, ринковий, кредитний, інвестиційний, ризик управління, ризик складання неправильної звітності (або ризик бухгалтера) і ін. *Фінансовий ризик* – є невід'ємним атрибутом ділової активності економічних агентів і означає можливість фінансових втрат. *Ринковий ризик* - викликається залежністю прибутковості бізнесу від зміни цін на ринках. Він багато в чому визначається ступенем інформованості та часом реакції суб'єкта на відповідну інформацію. *Кредитний ризик* – ризик щодо контрагента, пов'язаний з можливістю невиконання контрагентом своїх зобов'язань. *Інвестиційний ризик* – ризик, пов'язаний з можливістю знецінення капітальних вкладень у виробництво або в цінні папери. *Ризик управління* – з'являється в результаті невірних дій підприємця в конкретній ситуації (наприклад, прийняття рішень на основі використання математичних моделей і прогнозів низької якості). Цей ризик також пов'язаний зі зневагою до проблем підбору кадрів, інформаційно-технічного забезпечення і організаційної структури підприємства. *Ризик неправильного складання звітності* – викликаний некомпетентністю

бухгалтера, який може нанести підприємству величезних збитків, навіть поставити його на межу банкрутства.

Розробка заходів щодо зниження різних видів ризику підприємців є найважливішим компонентом стратегії підприємства в сфері забезпечення безпеки підприємництва. Реалізація такої стратегії на внутрифірмовому рівні поряд з діяльністю держави по створенню системи захисту підприємництва, інформаційного забезпечення дозволить пом'якшити ситуацію в підприємництві, підвищити його безпеку.

Тема 2 Взаємодія структурних підрозділів у системі безпеки підприємства

План лекції

2.1 Структура та склад служби безпеки підприємства

2.2 Комплексна програма служби безпеки

2.1 Структура та склад служби безпеки підприємства

Створення служби безпеки підприємства (СБП) має бути стратегічним рішенням керівництва підприємства. Адже сама по собі наявність чи відсутність цього підрозділу не є вирішальною у забезпеченні безпеки підприємства як стану захищеності його головних інтересів (не тільки економічних). Головним є розуміння з боку керівництва необхідності розробки, прийняття та реалізації політики безпеки підприємства як складової частини стратегії розвитку підприємства. При створенні СБП повинні враховуватися розміри підприємства, наявність реальних чи потенційних загроз господарській діяльності, оцінка ризиків цієї діяльності, бажані результати від створення СБП.

Організаційно служба безпеки великого підприємства складається з таких структурних одиниць:відділу режиму і охорони; спеціального відділу у складі сектора оброблення таємних документів і сектора оброблення документів з грифом «Комерційна таємниця»; інженерно-технічної групи; групи

інформаційно-аналітичної діяльності; розвідувального підрозділу; контррозвідувального підрозділу; штабного підрозділу (у випадку, якщо вищезазначені підрозділи є великими і складними оргструктур ними формуваннями).

Види діяльності СБП повинні збігатися з напрямками реалізації політики безпеки підприємства, яка в свою чергу повинна відображати реальні інтереси підприємства. Ключовими видами можуть бути: аналіз зовнішнього середовища (партнери, клієнти, постачальники, конкуренти); робота з персоналом: проведення тестування з метою виявлення прихованих інтересів кандидата при прийнятті на роботу, постійне роз'яснення необхідності дотримуватися законодавства персоналом; аналіз потенційних загроз безпеці; охорона вищого керівництва підприємства та критичних ресурсів господарської діяльності; протидія промисловому шпигунству.

Відповідальність посадових осіб:

1. Служба безпеки (СБ) підприємства створюється наказом директора з метою захисту економічних інтересів підприємства і забезпечення максимальної безпеки його діяльності як суб'єкта ринкових відносин.

2. СБ є самостійним підрозділом і підпорядковується безпосередньо керівнику підприємства.

3. Керівництво службою здійснює начальник СБ, що призначається і звільняється від займаної посади керівником підприємства.

4. Структура і штати СБ за поданням її начальника затверджуються керівником підприємства.

5. Діяльність СБ фінансується за рахунок включення її витрат у собівартість робіт, виконуваних підприємством.

6. СБ у своїй діяльності керується законами України, указами Президента, постановами Кабінету Міністрів, відомчими наказами і вказівками, Статутом підприємства, наказами і вказівками керівника підприємства і внутрішнім Положенням про СБ.

Діяльність служби безпеки товариства регламентується такими документами: положення про службу безпеки; положення про структурні підрозділи служби безпеки; посадова інструкція працівника служби безпеки; інструкцію про порядок проведення службових розслідувань на підприємстві; внутрішні документи (доповідні записки, службові записки, розпорядження, накази, довіреності); документи з питань забезпечення охорони праці(інструкція з охорони праці, журнал інструктажу).

2.2 Комплексна програма служби безпеки

Комплексна програма безпеки відображена на встановленні заходів, технологій, сил і засобів безпеки, спрямованих на створення відповідного режиму захисту товариства від зовнішніх та внутрішніх посягань на його власність та імідж, а також на забезпечення ефективної реалізації його інтересів на ринку.

Система безпеки виконує дві функції: *упереджувально-профілактичну* та *оперативно-інформаційну.* Відповідно, система безпеки включає дві групи заходів:

1. *Заходи загального забезпечення безпеки діяльності підприємства.* Здійснення організаційно-правового впливу на діяльність персоналу підприємства, його клієнтів та партнерів з питань забезпечення безпеки у взаємовідносинах з товариством, що забезпечується: впровадженням на підприємстві режимів безпеки (пропускного, внутрішньо об’єктового, конфіденційності, фінансової безпеки, кризового та ін.), які створюють відповідні умови для діяльності підприємства і його взаємовідносин з зовнішнім середовищем; розробкою нормативної бази товариства з питань безпеки, яка регламентує порядок виконання заходів безпеки та підтримання відповідних її режимів.

Розробка ефективної кадрової політики, яка б передбачала якісне кадрове забезпечення, обґрунтовану мотивацію і стимулювання праці, розвиток

персоналу та формування у нього фірмового патріотизму, впровадження системи об'єктивної перевірки та контролю діяльності персоналу, виконання ним відповідних режимів безпеки, забезпечення соціально-психологічного супроводження заходів безпеки та роботи персоналу товариства.

Охорона підприємства: об'єктів, грошей, матеріальних цінностей, обладнання, вантажів, персоналу; протипожежна охорона. Атестація приміщень, спеціальне обладнання окремих з них, облік носіїв інформації обмеженого доступу, захист засобів зв'язку, створення системи службового і спеціального діловодства. Захист інформаційних ресурсів обмеженого доступу з використанням програмно-апаратних засобів та нормативно-правових документів; використання систем криптографічного захисту.

Удосконалення технологій виробництва, введення до структури комерційних операцій елементів захисту інтересів товариства. Рекламно-пропагандистське забезпечення, формування позитивного іміджу підприємства, широке проведення маркетингових досліджень ринків, сфер і регіонів реалізації його інтересів. Планування та забезпечення дій підприємства у кризові ситуаціях. Проведення заходів щодо забезпечення економічної безпеки товариства. Забезпечення безпеки експлуатації будівель і споруд товариства, їх комунікаційних систем. Створення систем сповіщення персоналу товариства. Розробка заходів щодо відповідальності за порушення встановлених режимів та правил техніки безпеки.

2. Спеціальні заходи. Проведення заходів з комерційної розвідки. Інформаційно-аналітичні дослідження клієнтів, партнерів та конкурентів товариства, інформаційно-аналітичне забезпечення рішень керівництва товариства. Взаємодія з правоохоронними органами з питань попередження та перетинання протиправних і злочинних посягань на власність та імідж товариства. Заходи щодо протидії актам недобросовісної конкуренції і промислового шпигунства щодо товариства, проведення службових розслідувань за фактами протиправних і злочинних дій працівників підприємства, порушення ними встановлених правил роботи.

Проведення спеціальних інформаційних операцій. Заходи впливу на недобросовісних клієнтів, зловмисників і боржників товариства щодо відшкодування завданих йому збитків.

Процес організації комплексної безпеки діяльності товариства. Організація безпеки діяльності товариства передбачає аналіз та оцінку загроз; визначення мети, завдань і складу сил безпеки; розробку нормативної бази товариства з питань безпеки його діяльності; визначення функцій підрозділів товариства з питань безпеки; планування заходів безпеки; забезпечення взаємодії з правоохоронними органами та підрозділами товариства; управління системою безпеки та забезпечення її функціонування; контроль за ефективністю виконання заходів безпеки.

Безпосереднє керівництво діяльністю сил безпеки здійснює служба безпеки, на яку покладається відповідальність за безпеку товариства. Вона віддає розпорядження з питань безпеки, ставить завдання підрозділам та установам товариства щодо посилення безпеки товариства відповідно до змін умов його діяльності, періодично якісний контроль за функціонуванням системи безпеки та ініціює заохочення працівників товариства за бездоганне виконання ними заходів безпеки.

Планування заходів безпеки здійснюється підрозділом безпеки відповідно до чинного законодавства. В основу планування заходів безпеки покладено: визначення пріоритетних напрямів і об’єктів, на яких зосереджуються зусилля безпеки, розподіл сил і засобів для вирішення задач безпеки, визначення строків їх виконання; розробка форм і методів діяльності сил безпеки і проведення організаційних заходів; розробка дій та організація управління роботою персоналу товариства у кризових ситуаціях. Крім того, розроблюються і періодично уточнюються плани дій на випадок стихійного лиха, соціальних та воєнних конфліктів. Контроль за станом безпеки діяльності забезпечується шляхом періодичного проведення перевірок виконання заходів безпеки в підрозділах і установах товариства, надання останніми відповідних звітів про ефективність впровадження заходів безпеки. Фінансове і

матеріально-технічне забезпечення фінансове забезпечення заходів безпеки регулюється відповідно до внутрішніх положень та регламентів підприємства і здійснюється на плановій основі у відповідності з кошторисом сил безпеки.

Матеріально-технічне забезпечення заходів безпеки здійснюється централізовано у відповідності з критерієм достатньої необхідності. Спеціальні засоби придбаваються підрозділами безпеки в межах коштів, визначених на фінансування сил безпеки.

Інформаційне забезпечення. Інформаційне забезпечення заходів безпеки здійснюється виходячи з необхідності ефективного забезпечення діяльності підприємства інформаційними ресурсами. Основними джерелами інформації є підрозділи та установи підприємства, які самостійно або за запитом надають інформацію підрозділу безпеки, правоохоронні органи, інші організації і установи, з якими підрозділ безпеки підтримує договірні взаємовідносини щодо обміну інформацією. Інформаційну роботу з усіма відомостями, що стосуються питань безпеки, здійснює підрозділ безпеки. З метою інформування керівництва та персоналу товариства підрозділом безпеки періодично готуються відповідні інформаційні документи. За певних умов може бути передбачено фінансування отримання інформації.

Наукове забезпечення. Наукове забезпечення заходів безпеки має бути спрямоване на удосконалення форм і методів діяльності сил безпеки. Для вирішення завдань наукового забезпечення заходів безпеки може використовуватись інтелектуальний потенціал всіх підрозділів і установ товариства, а також зовнішніх наукових організацій. Основними формами наукового забезпечення є: науково-дослідні роботи, дисертації, видання, статті з проблем і питань безпеки, інноваційні технології, винахідницькі та раціоналізаторські роботи в сфері безпеки діяльності товариства.

Тема 3 Майно підприємства та організація його охорони

План лекції

3.1 Майно підприємства; сутність, види, класифікація

3.2 Сутність майнової безпеки підприємства та системи управління нею

3.3 Фактори впливу на майнову безпеку суб'єкта господарювання

3.1 Майно підприємства; сутність, види, класифікація

Будь-яке підприємство не може існувати без майна. Підприємство розпочинає свою діяльність вирішуючи питання про можливість формування майна за рахунок різноманітних джерел, і закінчує своє існування на етапі переходу прав власності на майно або ліквідації майна. Майно підприємства збільшується в процесі операційної та інших видів основної діяльності. Воно може бути об'єктом угод, відчужуватися, закладатися тощо.

В умовах ринкових відносин з поширенням приватної форми власності на засоби виробництва кардинально змінилося як сприйняття майна, так й підприємницьких можливостей щодо його використання. Майно підприємства стає як важливішим ресурсом, так й об'єктом найнебезпечніших загроз, що мають природу походження як з середини так й з оточуючого зовнішнього середовища. Враховуючи означене стає очевидною проблема створення на підприємствах системи захисту майна, що може бути вирішена шляхом застосування методів, принципів та прийомів управління економічною безпекою у вигляді злагодженого механізму.

Для своєї діяльності підприємство має розраховувати певним набором економічних ресурсів – елементів, що використовуються для виробництва економічних благ. Діяльність будь-якого підприємства повинна забезпечуватися засобами, що необхідні для задоволення його потреб. Сукупність засобів підприємства називають *майном.*

Термін «майно» активно використовується у законодавчих та нормативних актах. Відповідно до Господарського Кодексу України (ГКУ) майном визнається сукупність речей та інших цінностей (включаючи нематеріальні активи), які мають вартісне визначення, виробляються чи використовуються у діяльності суб'єктів господарювання та відображаються в їх балансі. Суб'єктами господарювання визнаються учасники господарських відносин, які здійснюють господарську діяльність, реалізуючи господарську компетенцію (сукупність господарських прав та обов'язків), мають відокремлене майно і несуть відповідальність за своїми зобов'язаннями в межах цього майна, крім випадків, передбачених законодавством.

Згідно ЗУ Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні (2001р., стаття 3) *майном, яке може оцінюватися*, вважаються об'єкти в матеріальній формі, будівлі та споруди (включаючи їх невід'ємні частини), машини, обладнання, транспортні засоби тощо; паї, цінні папери; нематеріальні активи, в тому числі об'єкти права інтелектуальної власності; цілісні майнові комплекси всіх форм власності;

майновими правами, які можуть оцінюватися, визнаються будь-які права, пов'язані з майном, відмінні від права власності, у тому числі права, які є складовими частинами права власності (права володіння, розпорядження, користування), а також інші специфічні права (права на провадження діяльності, використання природних ресурсів тощо) та права вимоги.

Згідно до Цивільного кодексу «підприємством як об'єктом прав визнається майновий комплекс, використовуваний для реалізації підприємницької діяльності». До складу підприємства як майнового комплексу входять всі види майна, призначені щодо його діяльності, включаючи земельні ділянки, будинку, споруди, устаткування, інвентар, сировину, продукцію, права вимоги, борги, і навіть права на позначення, що ідентифікують підприємство, продукцію, роботи й послуги (фірмове найменування, товарні знаки, знаки обслуговування), та інші виняткові права, якщо інше не передбачено в законі.

Стаття 191 Цивільного кодексу визначає підприємство як єдиний майновий комплекс і встановлює, що підприємство може бути об'єктом купівлі і продажу, застави, оренди та інших дій. Право власності на майно виходить з ознак юридичної особи і має самостійну майнову відповідальність, характеризується наявністю *відособленого майна.*

Значення майна для підприємства, в основному, зводиться до такого: майно – важливий економічний ресурс, один з факторів виробництва (фактори виробництва: земля, праця, капітал, менеджмент); майно – об'єкт права власності; майно – фактор забезпечення ефективності господарської діяльності підприємства; майно – гарантія підприємства щодо виконання його зобов'язань**.** Підприємство відповідає за свої борги своїм майном, яким можуть поширюватися позови господарських партнерів, чи кредиторів у разі невиконання підприємством будь-яких зобов'язань. При визнання підприємства неспроможним (банкрутом) його майно відповідно до встановленими законами, процедурами можна використовувати у якості задоволення вимог кредиторів. Решта майна ліквідованого підприємства передається його засновникам (учасникам), що мають відповідні права.

Майно – основа формування ринкової вартості підприємства. Вартість майна має безпосередній вплив на оцінку ринкової вартості підприємства, максимізація якої – головна стратегічна мета підприємства.

Майно – головний стратегічний ресурс підприємства, запорука його «виживання» в ринкових умовах. Визначає його економічний потенціал та є запорукою стійкого безупинного розвитку.

Класифікація майна побудована за ознаками: за розміщенням засоби підприємств поділяються на засоби виробничої сфери, сфери обігу та невиробничої сфери. Таке групування дозволяє визначити, де використовується майно, яким володіє господарюючий суб'єкт; за функціональною роллю у процесі відтворення засоби підприємства поділяються на дві великі групи: необоротні засоби та оборотні засоби; за майновою приналежністю основні засоби поділяються на власні та орендовані за джерелами утворення –: власний

і залучений (позиковий), капітал тощо. Але більш популярним є поділ майна на матеріально-речові елементи та нематеріальні елементи.

Майно є не тільки найважливішим ресурсом, що формує переваги підприємства, але й об'єктом різних загроз, що визначає необхідність розгляду системи управління безпекою майна.

Класифікація майна організації як об'єкта загроз здійснюється за кількома ознаками: *за видом майна:* грошові кошти в готівковій і безготівковій формах; цінні папери, а також будь-які інші документи, що підтверджують майнові права; товарно-матеріальні цінності; *за ступенем ліквідності* абсолютно ліквідні активи – грошові кошти та цінні папери на пред'явника); високоліквідні матеріальні активи – товарно-матеріальні цінності, придатні для швидкої реалізації на відкритому ринку (наприклад, товари широкого вжитку, паливо і т.п.); середньо ліквідні матеріальні активи – товарно-матеріальні цінності, що користуються попитом, але не придатні для реалізації на відкритому ринку (наприклад, напівфабрикати, деякі види сировини або промислового обладнання); низько ліквідні матеріальні активи – товарно-матеріальні цінності, які не придатні для реалізації на відкритому ринку і, крім того, здатні зацікавити тільки обмежену групу потенційних покупців (наприклад, більшість видів промислового обладнання); *за правом власності:* власне майно організації; орендоване організацією майно; майно, що належить партнерам або клієнтам організації; *за вартістю:* особливо цінне майно (наприклад, грошові кошти, цінні папери, основне виробниче обладнання тощо); малоцінні елементи майна (наприклад, МШП); інше майно.

3.2 Сутність майнової безпеки підприємства та системи управління нею

Майнова безпека – діяльність суб'єктів безпеки і сил безпеки з організації та практичного здійснення заходів, спрямованих на забезпечення схоронності, цілісності визначених власником майна належних йому будівель, споруд, іншого рухомого та нерухомого майна з метою відвернення або недопущення

безпосередніх посягань на майно, припинення несанкціонованого доступу до нього для збереження його фізичного стану і забезпечення здійснення власником цього майна всіх належних йому повноважень щодо нього.

Майнову безпеку можна розглядати в широкому і вузькому розумінні: в широкому – під майновою безпекою розуміється стан захищеності майна від внутрішніх і зовнішніх загроз як протиправного, так і природного (стихійні лиха), техногенного, екологічного, космічного й іншого характеру, у вузькому – це стан захищеності майна від протиправних посягань правовими, організаційними, інженерно-технічними, попереджувальними й іншими заходами**.**

Головна мета майнової безпеки підприємства – полягає в тому, щоб виключити можливість заподіяння йому збитків або упущення вигоди та забезпечити ефективне використання майна, якісну реалізацію всіх планів та гарантувати його стабільне й максимально ефективне функціонування тепер та високий потенціал розвитку в майбутньому.

Завдання майнової безпеки підприємства: захист законних майнових інтересів суб'єкта господарської діяльності та його співробітників; виявлення та формування причин і умов, сприятливих реалізації підприємством власних майнових інтересів; своєчасне виявлення реальних і потенційних загроз майну суб'єкта підприємництва та вжиття заходів щодо їх нейтралізації; виявлення внутрішніх і зовнішніх причин і умов, які можуть сприяти заподіянню матеріальної та іншої шкоди, а також перешкоджати нормальній діяльності підприємства; оперативне реагування на загрози, що виникають та на негативні тенденції розвитку зовнішньої та внутрішньої ситуації; збереження та ефективне використання матеріальних, фінансових та інформаційних ресурсів; послаблення шкідливих наслідків від дій конкурентів та злочинців з підриву системи майнової безпеки підприємства; профілактика та попередження правопорушень і злочинних посягань на власність підприємства; виховання та навчання персоналу з питань майнової безпеки.

Система майнової безпеки – це сукупність взаємопов'язаних суб'єктів (система суб'єктів), покликаних забезпечити стан захищеності майна від протиправних посягань у межах своїх повноважень властивими кожному з них способами.

Рівні системи майнової безпеки підприємця: *адміністративний* – управлінські рішення, необхідні для забезпечення безперебійного функціонування об'єкта; *оперативний* – заходи забезпечення безпеки господарюючого суб'єкта специфічними засобами і методами; *технічний* – використання сучасних технологій у сфері забезпечення безпеки; *режимно-пропускний* – система фізичної безпеки, зокрема охорона фінансових і матеріально-технічних цінностей підприємства

Базовими елементами системи забезпечення майнової безпеки підприємства є: майнові інтереси суб'єкта господарювання, фактори, що перешкоджають реалізації означених інтересів та система захисту майнових інтересів.

Майнові інтереси підприємства – забезпечення недоторканості прав власності, схоронності і примноження майна і майнових прав, розвиток цілісних майнових комплексів. Інтереси підприємства в сфері майнової безпеки зводяться до: забезпечення основними та оборотними засобами в обсягах, достатніх для виробничо-господарської діяльності; формування оптимальних пропорцій між складовими елементами майна для забезпечення їх збалансованості; ефективне використання майна в процесі господарської діяльності з метою одержання найвищих показників від його використання; збереження та примноження майна впродовж існування підприємства та, відповідно, зростання ринкової вартості підприємства.

У своїй діяльності підприємство повинно паралельно здійснювати узгодження власних майнових інтересів з інтересами суб'єктів зовнішнього середовища.

3.3 Фактори впливу на майнову безпеку суб'єкта господарювання

Майновий ризик являє собою ймовірність втрати підприємством частини свого майна, його псування і недоотримання доходів в процесі здійснення виробничої і фінансової діяльності. До таких ризиків можна віднести: ризик втрати майна в результаті стихійних лих (пожеж, повеней, землетрусів, ураганів і т. п.); ризик втрати майна внаслідок дій зловмисників (розкрадання, диверсії); ризик втрати майна в результаті аварійних ситуацій на виробництві; ризик втрати або псування майна під час експлуатації, транспортування; ризик відчуження майна в силу дії місцевих органів влади або інших власників.

Типові форми загроз майнової безпеки: перехоплення прав власності на майно організації; розкрадання майна організації; пошкодження або знищення майна організації; нанесення організації збитку в формі реалізації невигідних або прямо збиткових для неї господарських операцій.

Суб'єкти ризиків (загроз) майнової безпеки організації:

конкуренти – зацікавлені в перехопленні прав власності на її майнові комплекси або намагаються послабити її позиції шляхом знищення його елементів;

кримінальні структури – зацікавлені або в мирному проникненні в бізнес організації, або у відчуженні частини її майна (перехоплення прав власності, розкрадання в насильницької або ненасильницької формі);

індивідуальні зловмисники (хакери, зломщики, фінансові аферисти) – зацікавлені в отриманні додаткового доходу шляхом протиправних дій відносно майна підприємства;

клієнти або партнери організації – зацікавлені в отриманні додаткового доходу шляхом різних форм шахрайства в процесі реалізації господарських відносин;

власні співробітники – намагаються поліпшити своє матеріальне становище за рахунок роботодавця, а також завдають шкоди його майну з злого наміру або внаслідок власної безвідповідальності.

Методи реалізації загроз майнової безпеки організації диференціюються залежно від**:** об'єкта загрози; суб'єкта загрози**.**

При використанні класифікації за першою ознакою можна відзначити, що основним об'єктом загроз є грошові кошти організації. Тут можуть бути реалізовані найрізноманітніші за характером і технології виконання форми загроз, зокрема: розкрадання в ненасильницької формі (крадіжки, в тому числі, зі зломом); розкрадання в насильницькій формі (пограбування); розкрадання шляхом фальсифікації фінансових документів; розкрадання з використанням інформаційних технологій.

Для реалізації загроз щодо майна в матеріальній формі суб'єкти використовують такі методи, як: розкрадання в ненасильницької формі; розкрадання в насильницькій формі; перехоплення прав власності; пошкодження; знищення.

Класифікація за другою ознакою дозволяє виділити наступні найбільш поширені методи. Найбільш широку їх номенклатуру потенційно можуть використовувати *власні співробітники організації*. Найчастіше ними застосовуються: дрібні розкрадання товарно-матеріальних цінностей організації, що здійснюються зазвичай в змові з колегами або сторонніми зловмисниками; розкрадання готівкових коштів; розкрадання готівкових та безготівкових грошових коштів шляхом фальсифікації фінансових документів; розкрадання грошових коштів з використанням інформаційних технологій; нанесення організації збитку в результаті корупції при укладанні господарських договорів і контрактів; умисне пошкодження або знищення майна організації (саботаж); ненавмисне пошкодження або знищення майна організації (злочинна недбалість).

Кримінальні структури для досягнення поставлених цілей можуть схиляти співробітників організації до співучасті в таких злочинних діях, як: крадіжки; пограбування; вилучення або фальсифікація документів, що підтверджують право власності; умисне знищення майна; шахрайські фінансові операції.

Індивідуальні зловмисники для досягнення поставлених цілей можуть схиляти співробітників організації до співучасті в таких злочинних діях, як: крадіжки грошових коштів і товарно-матеріальних цінностей; шахрайські фінансові операції; забезпечення можливості доступу до управління фінансовими операціями з використанням інформаційних технологій.

Конкуренти для досягнення поставлених цілей можуть схиляти співробітників організації до співучасті в таких злочинних діях, як: вилучення або фальсифікація документів, що підтверджують право власності; проведення свідомо збиткових операцій; знищення майнових комплексів (наприклад, підпал офісу або складу з продукцією).

Недобросовісні клієнти або партнери для досягнення поставлених цілей можуть схиляти співробітників організації до співучасті в таких злочинних діях, як: вилучення або фальсифікація документів, що підтверджують право власності організації на відвантажену продукцію або передане в оренду майно; визнання невигідною або прямо збитковою для організації угоди купівлі-продажу, оренди тощо, а також приховане лобіювання її.

ЗМ 4 Корпоративні конфлікти та методи їх подолання

Тема 1 Корпоративні конфлікти в системі корпоративних відносин

План лекції

1.1 Поняття корпоративного конфлікту

1.2 Основні причини виникнення корпоративних конфліктів

1.3 Класифікація корпоративних конфліктів

1.4 Організаційне забезпечення запобігання виникненню конфліктів

1.1 Поняття корпоративного конфлікту

За своєю суттю, *конфлікт* – зіткнення сторін, думок, сил, або відсутність згоди між двома або більшою кількістю сторін, що можуть бути конкретними особами або групами. У випадку виникнення конфліктів кожна із конфліктуючих сторін робить все, аби прийнятною була її точка зору або мета та заважає іншій стороні робити теж саме.

Корпоративний конфлікт – вузькогруповий, замкнутий межами корпорації, конфлікт. Корпоративні конфлікти впливають на стратегічний розвиток і безпеку компанії. Отже, *корпоративний конфлікт* – це зіткнення інтересів, цілей учасників корпоративних відносин на вищому рівні управління компанії, а також інвестора (при «дружньому» поглинанні) чи рейдера (при «недружньому поглинанні) з приводу права власності на акції компанії і прав, які дають ці цінні папери.

Під даним терміном, слід розуміти розбіжності і суперечки, що виникають між акціонерами товариства, акціонерами і менеджментом товариства, інвестором (потенційним акціонером) і суспільством, які призводять або можуть призвести до наступних наслідків: порушення норм чинного законодавства, статуту або внутрішніх документів товариства, прав

акціонера або групи акціонерів; позови до підприємства, його органів управління або по суті прийнятих ними рішень; дострокове припинення повноважень діючих органів управління; істотні зміни в складі акціонерів.

До суб'єктів корпоративного конфлікту можна віднести акціонерів, членів правління, топ-менеджерів, інвесторів або рейдерів.

Об'єктом корпоративного конфлікту є права власності на акції компанії і права, які дають ці цінні папери (участь в управлінні, участь у розподілі прибутку компанії тощо).

Суперечки, пов'язані з питаннями корпоративного управління, можуть стосуватися: конфліктів інтересів членів правління або провідних виконавчих посадових осіб компанії; обрання членів правління та їх призначення; розміру винагород/премій, що виплачуються членам правління; звільнення членів правління/провідних виконавчих посадових осіб компанії; оцінки вартості акцій (стосовно емісії нових акцій чи облігацій, або «витіснення міноритарних акціонерів»); умов запропонованого поглинання; а також придбання активів компанії або розпорядження ними тощо.

Суб'єктами корпоративного спору можуть виступати: юридична особа, орган управління юридичної особи, підприємницькі об'єднання юридичних осіб, акціонер, учасник (засновник).

В основу корпоративного спору покладено *конфлікт інтересів*. Передумови конфлікту інтересів – обмеженість єдиних для безлічі зацікавлених осіб грошових та інших майнових ресурсів, психологічно обумовлене проти річчя особистих інтересів та інтересів компанії.

Стадії корпоративного конфлікту: 1. Передконфліктна стадія. Період, коли конфліктуючі сторони оцінюють свої ресурси, перш, ніж зважитися на агресивні дії або відступити. До таких ресурсів відносяться: кількість голосуючих акцій, якими володіють сторони конфлікту, інформація (доступ до інформації), фінансові, адміністративні можливості та інтелектуальний потенціал сторін. 2. Безпосередній конфлікт. Ця стадія характеризується, перш за все, наявністю інциденту, тобто дій, спрямованих на зміну поведінки

суперників (наприклад, проведення альтернативних зборів акціонерів). Дуже характерним моментом на етапі безпосереднього конфлікту є наявність критичної точки, при досягненні якої конфліктні взаємини досягають максимальної сили і гостроти. 3. Заключна стадія – вирішення конфлікту.

Основними факторами ризику для підприємства, у системі якого виникає корпоративний конфлікт, слід визнати такі:

1) Ризик паралізації діяльності вищого управління підприємством (блокування роботи вищого органу – загальних зборів) виникає у випадку переростання конфлікту у корпоративний спір та проявляється у поширеному забезпечувальному заході суду щодо позовних вимог – забороні проведення загальних зборів та здійснення дій щодо їх скликання, або забороні участі у голосуванні «спірних» акцій (часток), що у випадку їх опосередкування великого пакету може не дозволити відбутися кворуму тощо. Внаслідок, зокрема, заборони проведення загальних зборів, з одного боку, порушуються права на участь в управлінні підприємством тих учасників, які не беруть участі у конфлікті, а з іншого, порушується інтерес підприємства щодо його функціональної спроможності, від якої залежить вирішення найважливіших питань з діяльності підприємства.

2) Ризик паралізації поточної діяльності або її окремих сфер (блокування діяльності органів управління) проявляється у таких забезпечувальних заходах суду: заборона органам управління виконувати певні рішення загальних зборів та інших органів (наприклад, заборона правлінню виконувати рішення наглядової ради); заборона здійснення певних дій органам підприємства, пов’язаних з відчуженням його майна, тощо.

3) Ризик декапіталізації діяльності («розмивання» активів) − відбувається вибуття активів, скорочення обсягів господарської діяльності (виробництва), зменшення доходів, втрата клієнтів, знецінення товарного знаку та ін.

4) Ризик припинення господарської діяльності підприємства − є можливістю настання найгіршого (зокрема, для підприємства) наслідку корпоративного конфлікту. Внаслідок цього можливе зупинення або

припинення виробничого процесу, настання неплатоспроможності підприємства як підстави порушення справи про банкрутство тощо.

1.2 Основні причини виникнення корпоративних конфліктів

Причини корпоративних конфліктів, як правило, безпосередньо пов'язані з питанням: хто буде керувати товариством і кому належить контрольний пакет акцій підприємства. Найважливішими особливостями організаційно-правової й економічної природи товариства, що породжують конфлікти є:

1. Наявність низки самостійних акціонерів-співвласників, економічні підходи та інтереси яких щодо акціонерного товариства не збігаються.

2. Різна кількість акцій, якими володіють акціонери і як наслідок, різний обсяг їх відповідних прав в акціонерному товаристві, контролю над ним і ризиків інвестування в товариство.

3. Поділ влади в акціонерному товаристві на «законодавчу» (загальні збори акціонерів, спостережна рада), «виконавчу» (правління) і «судову» (ревізійна комісія).

4. Відмежування «реальних» власників (акціонерів) від «реальної» власності (майна) за допомогою інститутів акції і юридичної особи.

5. Наявність власників-акціонерів і найманих робітників.

6. Взаємодія акціонерного товариства, його акціонерів й менеджерів із широким колом контрагентів, економічні підходи і інтереси яких щодо акціонерного товариства не збігаються з інтересами акціонерного товариства (господарюючі суб'єкти, влада, засоби масової інформації, політичні групи тощо).

Організаційні підстави виникнення корпоративного конфлікту пов'язані з побудованою в корпорації системою корпоративного управління, зокрема з формуванням системи виборних органів (наглядової ради, ревізійної комісії), створенням призначених органів (правління), напрямами стратегічного

розвитку корпорації,змінами статутного капіталу, прийнятими внутрішньокорпоративними положеннями тощо.

1.3 Класифікація корпоративних конфліктів

Класифікацію корпоративних конфліктів, використовуючи три групи критеріїв.

Перший критерій – оцінка корпоративних конфліктів за широтою охоплення ними корпоративних відносин, що формуються у зв'язку із бізнесом і стратегічним управлінням даною компанією – внутрішні і зовнішні корпоративні конфлікти. При цьому до внутрішніх корпоративних конфліктів зараховуються корпоративні конфлікти, в яких беруть участь співвласники компанії і її провідні менеджери. До зовнішніх – корпоративні конфлікти, учасниками яких є потенційні інвестори і здобувачі посади одноосібного виконавчого органу, а також різні інші зацікавлені особи – *стейкхолдери.*

Другий критерій диференціації типів корпоративних конфліктів – угруповання корпоративних конфліктів за їхніми конкретними учасникам. За другим критерієм корпоративні конфлікти ділять на дві групи, кожна з яких включає в себе кілька видів конфліктів. Так, *першу групу корпоративних* конфліктів, склали внутрішні корпоративні конфлікти, що диференціюються за такими підгрупами: 1) конфлікти між різними групами акціонерів; 2) конфлікти між акціонерами і дирекцією підприємства; 3) конфлікти між менеджментом-адміністрацією підприємства і згуртованим трудовим колективом; 4) конфлікти між арбітражним керуючим підприємства, що знаходиться на ранніх стадіях процедури банкрутства, і акціонерами компанії. *Другу групу* корпоративних конфліктів утворюють зовнішні корпоративні конфлікти, які поділяються на такі підгрупи: 1) конфлікти в форматі «контрольні і наглядові державні органи проти акціонерної компанії в цілому»; 2) різні версії недружніх поглинань; 3) конфлікти між державою в цілому як активним учасником ринку капіталу; 4) конфлікти між органами управління керуючої організації, що реалізує за

рішенням загальних зборів акціонерів повноваження генерального директора даного акціонерного товариства, і акціонерами останньої в ситуації неможливості оперативного прийняття рішення зборів про дострокове припинення повноважень спеціальної керуючої компанії; 5) конфлікти між мешканцями населеного пункту, в якому підприємство є роботодавцем та платником податків, і дирекцією компанії; 6) протиборство між громадськими об'єднаннями, які пропагують соціально значимі цілі, реалізації яких перешкоджає дана компанія (наприклад, екологічні організації), і компанією, яка актуальність цих цілей не визнає.

Третій критерій класифікації корпоративних конфліктів – за їх основним предметом. Під предметом корпоративних конфліктів маються на увазі ключові цілі, що реалізуються учасниками найбільш поширених акціонерних конфронтацій. За даним критерієм такі групи корпоративних конфліктів: 1) набуття контролю над підприємством з наміром зберегти його як бізнес. У цій групі виявляється значна частина схем недружнього поглинання.; 2) прагнення придбати права власності на ключові активи підприємства-мети, в числі яких земельні ділянки, виробничі будівлі та споруди, обладнання, корпоративні цінні папери дочірніх і залежних товариств компанії – об'єкта атаки; 3) завоювання місця на ринку товарів, послуг, технологій та ідей, займаного компанією-ціллю.; 4) зміна управлінських технологій участі значущих акціонерів, контрагентів компанії чи інших осіб в легальному розподілі доходів акціонерної компанії; 5) забезпечення або розширення участі в тіньовому розподілі доходу компанії; 6) обґрунтований захист прав учасників корпоративних відносин у випадках їх порушення будь-ким з інших агентів корпоративних зв'язків; 7) збільшення процентної участі в капіталі компанії, що забезпечує нарощування акціонерної влади; 8) відновлення або зміцнення особистого авторитету тієї чи іншої посадової особи апарату управління компанії.

1.4 Організаційне забезпечення запобігання виникненню конфліктів

Організаційне забезпечення запобігання виникненню конфліктів визначається: наявністю органів, які запобігають виникненню конфлікту; частотою розгляду питань, що стосуються контролю за діяльністю корпорації; підзвітністю органів контролю; прозорістю та публічністю процесу контролю та його результатів.

Існує багато методів вирішення конфліктів: ухилення; згладжування (потреба в солідарності); примушення (намагання заставити прийняти свою точку зору любою ціною); компроміс (прийняття точки зору іншої сторони, але лише до деякого ступеню); вирішення проблеми (віднайти курс дій, що сприйнятливий для всіх сторін).

Алгоритм вирішення конфлікту через вирішення проблеми складається з п'яти етапів і виглядає таким чином: визначити проблему в категоріях цілей, а не рішень; після того, як проблема визначена, визначити рішення, що сприйнятливе для конфліктуючих сторін; зосередити увагу на проблемі, а не на особистих якостях іншої сторони; створити атмосферу довіри, збільшуючи взаємний вплив та обмін інформації; під час спілкування створювати позитивне відношення один до одного, виявляючи симпатію та вислуховуючи думку іншої сторони, а також зводячи до мінімуму прояви погроз та гніву.

Найважливішим завданням керівництва є формування єдності мотивації членів колективу.

Психологічну атмосферу колективу визначає соціальна мета діяльності колективу, ціннісно-орієнтаційна єдність групи, почуття колективної й особистої відповідальності, взаємозалежності членів групи, що ведуть до поєднання особистих інтересів із суспільними.

Дуже багато залежить від керівника – стиля його керівництва, а також характеру та ступеню його лідерства в групі. Керівнику необхідно певну увагу приділяти завданням, які дозволять поліпшити психологічний клімат колективу: розробка місії та цінностей компанії; формування корпоративних

правил, корпоративної культури; повага до співробітників компанії, як обов'язкова складова успіху; проведення командотворчих тренінгів; проведення свят та неформальних зустрічей між співробітниками.

Тема 2 Теоретичні основи рейдерства та грінмейлу підприємств

План лекції

2.1. Сутність та історія виникнення рейдерства та грінмейлу

2.2. Способи захоплення підприємств і методи захисту їх від захоплення

2.1 Сутність та історія виникнення рейдерства та грінмейлу

Протягом останнього десятиліття рейдерство стає однією з найбільш гострих проблем вітчизняної економіки. Феномен рейдерства включає в себе не тільки корпоративне рейдерство, але також земельне рейдерство і майнове рейдерство.

Рейдер в перекладі з англійської – «загарбник». *Ціль рейдера – заволодіти цілою компанією.*

Історія рейдерства налічує сотні років, хоча сам термін з'явився на рубежі XIX і XX століть. Рейдерство з'явилося разом з акціями, які дали можливість поглинання компанії поза волею керівництва.

Рейдерська діяльність – це злагоджена командна робота висококласних фахівців (юристів, економістів, аналітиків, бухгалтерів, аудиторів, силовиків), спрямованих в потрібне русло організаторами, які мають певний адміністративний і фінансовий ресурс.

В сьогоднішніх умовах можна виділити види рейдерів – «білі рейдери», що працюють виключно в рамках закону, і «чорні рейдери», які використовують вельми кримінальні способи. Існують також грінмейлери.

Деякі великі торгово-промислові та фінансові групи були створені саме шляхом недружніх поглинань. Іноді рейдерська фірма є дочірньою або

афілійованою по відношенню до таких структур. Для боротьби з рейдерством при Українському комітеті Міжнародної Торгової Палати засновано спеціальний орган – *Бюро протидії комерційним злочинам та рейдерству*. Серед заявлених завдань організації – розробка ефективної нормативно-правової бази для захисту інвесторів, використання рекомендованих міжнародними організаціями методів протидії комерційним злочинам та рейдерству, проведення масштабних інформаційно-роз'яснювальних кампаній серед інвесторів.

Форми рейдерства: поглинання підприємства – зміна власника юридичної особи та / або його активів. З подібною ситуацією стикаються, коли акції / частки однієї компанії купуються інший, або продаються всі активи; *недружнє поглинання* – поглинання підприємства, що відбувається поза волею поточних власників та / або керуючих, в тому числі з примусу економічними, організаційними, правовими та іншими засобами.

Етапи рейдерського захоплення підприємства: підготовка; створення передумов для захоплення; захоплення та утримання підприємства; перепродаж підприємства замовнику.

Ознаки, за якими можна припустити, що відносно компанії (підприємства) готується захоплення: збір інформації про компанію; збільшення числа угод з дрібними пакетами акцій; надмірна активність міноритарних акціонерів; пропозиції з продажу акцій або часткою, що надійшли від інвестиційних компаній; судові процеси; перевірки контрольно-наглядових і правоохоронних органів; проблеми з контрагентами і партнерами; «чорний PR»; скупка боргів підприємства.

Протягом кількох останніх років в українську практику корпоративних конфліктів увійшов новий термін *«greentail» («грінмейл»)* або «greenmailing» («грінмейлінг»). *Грінмейл* – форма легального корпоративного шантажу, це процедура придбання значної кількості акцій компанії для того, щоб створити загрозу її ворожому поглинанню з метою подальшого перепродажу цих акцій за завищеною ціною тій самій компанії. Грінмейл, як правило, використовується

дрібним акціонером з метою продажу своїх акцій «мажоритарію» за спекулятивною ціною.

2.2 Способи захоплення підприємств і методи захисту від захоплення

Існують кілька *законних способів позбавити власника контрольного пакета* управління акціонерним товариством: (законний) власник контрольного пакета добровільно продає свої акції; (законні) збори акціонерів приймають рішення про додатковий випуск акцій, і загарбник скуповує їх; (законний) акціонер позбавляється своїх акцій за борги в силу судового рішення; підкуп генерального директора товариства з виведенням активів з компанії; підкуп генерального директора товариства з продажем їм контрольного пакета акцій; проведення акціонерних зборів без кворуму з рішеннями про призначення нового керівництва і додатковий випуск акцій, в результаті чого контрольний пакет акцій переходить до рейдеру; незаконне переведення акцій реєстроутримувачем; підробка угоди про продаж акцій з пред'явленням його реєстроутримувачу; підробка боргового зобов'язання з пред'явленням його в суді і отримання рішення про стягнення заборгованості; підкуп генерального директора з формуванням фіктивної заборгованості; підкуп генерального директора з доведенням компанії до банкрутства; шляхом оскарження приватизації: умови для такого рейдерства створюються в той момент, коли приватизація підприємства здійснена незаконним шляхом.

Найбільш оптимальним рішенням є проведення *превентивної діагностики* власного підприємства із залученням професіоналів, в результаті якої можна буде виявити слабкі місця в корпоративній структурі і вибудувати надійну систему корпоративного захисту.

Найбільш ефективні заходи щодо захисту від рейдерського захоплення:

1. *Перевірка на наявність історичних ризиків.* Вони можуть проявлятися в порушеннях корпоративного, податкового, договірного та іншого законодавства, які можуть успішно використовуватися рейдером для

досягнення своїх цілей. Щоб виявити і усунути історичні ризики, рекомендується проводити незалежний юридичний, податковий і фінансовий аналіз (due diligence) на етапі придбання бізнесу.

2. *Захист інформації.* Так, щоб уникнути витоку відомостей про організацію, що сприяють розробці схем захоплення, керівнику бізнесу слід вживати всіх можливих заходів для захисту інформації про його підприємство: із залученням професійних юристів провести правовий моніторинг ступеня захисту інформації, інструктаж співробітників, скористатися послугами фахівців із захисту інформації та ін.

3. *Захист інсайдерської інформації.* На початку будь-якого проекту недружнього поглинання рейдер вдається до збору і подальшого юридичного аналізу всілякої інформації про компанію, її акціонерів, менеджерів і контрагентів. При цьому інформацію, що цікавить рейдера з метою недружнього поглинання, можна розділити на *інформацію особистого характеру* щодо власників і членів виконавчого органу (компромат), *юридичну, фінансову та іншу* інформацію про компанію. Інформація особистого і ділового характеру, як правило, використовується з метою шантажу, юридична ж інформація ретельно вивчається з метою визначення вразливих з правової точки зору місць компанії з тим, щоб в подальшому завдати по ним удар. Слід затверджувати на підприємстві *Положення про комерційну таємницю*, що регулює порядок віднесення інформації до комерційної таємниці, доступ до неї і її захист, а також відповідальність за її розголошення (додатково до тієї, що передбачена законодавством). При цьому до комерційної таємниці може бути віднесена будь-яка інформація про підприємство (його діяльність), крім тієї, що передбачена постановою Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційну таємницю».

4. На підприємстві має бути на високому рівні організовано *діловодство,* всі документи підприємства повинні бути юридично бездоганними. Крім цього, необхідно вести постійну роз’яснювальну роботу з акціонерами (учасниками) і співробітниками компанії з приводу важливості

збереження конфіденційної інформації про компанію та можливі наслідки її розголошення.

5. *Підтримка довірчих відносин з акціонерами та персоналом.* Істотно сприяє посиленню антирейдерського захисту вибудовування доброзичливих відносин між керівництвом компанії і її акціонерами, а також між працівниками і керівником. Для цього в першу чергу керівництву необхідно дотримуватися всі права зазначених осіб, передбачені чинним законодавством, адже нерідко витік інформації з метою нашкодити підприємству може здійснюватися через співробітників, які перебувають в конфліктних відносинах з керівництвом.

6. *Профілактика за допомогою доопрацювання документації компанії.* Оскільки більшість недружніх поглинань починається з аналізу інформації про підприємство та його документації, і стратегія захоплення здебільшого визначається результатами цього аналізу, найкращим засобом захисту від атаки є її профілактика. Для цього керівництву організації бажано замовити правову діагностику, в ході якої професійні юристи проведуть аналіз історії придбання контролю над підприємством поточного власника, історії угод компанії за попередні роки, структури статутного капіталу, повноважень органів управління, стану кредиторської та дебіторської заборгованості, правового режиму нерухомості та інших активів підприємства, і так далі. Подібний захід дозволить визначити слабкі місця в захисті компанії і зробити все можливе для їх усунення або мінімізації.

7. *Захист активів (нерухомості).* Як правило, основною метою недружніх поглинань є активи підприємства, зокрема, нерухомість. Відповідно для того, щоб зробити захоплення бізнесу якомога менш привабливим для агресора, слід організувати якісну правову захист основних активів компанії. Дані заходи роблять захоплення або нерентабельним для рейдера, або істотно збільшують його вартість. Також підконтрольне обтяження основних активів підприємства створює перешкоди для їх несанкціонованого виведення.

8. *Реструктуризація.* Одним із способів захисту бізнесу є також реструктуризація компанії. Діяльність компанії веде не одна особа, а група

взаємопов'язаних юридичних осіб, з яких, наприклад, виділяються: *компанія-володар*: володіє активами підприємства, однак її діяльність зводиться до мінімуму, що знижує ризик виникнення кредиторської заборгованості та судових справ; *управлінська компанія:* в ній працюю професійні юристи, фінансисти, бухгалтера і керуючі менеджери, які керують діяльністю інших компаній; *виробнича компанія:* здійснює безпосереднє надання послуг або виробництво товарів, як правило, користується матеріальними активами на правах оренди; *торгова компанія:* займається продажем товарів і послуг. Подібна диференціація допомагає захистити основні активи бізнесу, а також істотно ускладнює потенційний захоплення.

9. *Облік і скасування довіреностей.* Щоб уникнути проблем від дій осіб, які є повноважними представниками організації в очах третіх осіб і органів державної влади, доцільно визначити локальними нормативними актами порядок видачі довіреностей, а також вести облік всіх довіреностей, які видаються від імені компанії, в спеціальному журналі.

10. *Контроль кредиторської заборгованості.* Консолідація кредиторської заборгованості (боргів) компанії є, поряд з консолідацією контрольного пакета акцій, одним з основних способів недружнього поглинання підприємства. При цьому він може використовуватися як основний спосіб захоплення (з метою доведення компанії до банкрутства), так і додатковий (з метою створити тиск на компанію і змусити її до вигідних для рейдерів дій).

11. *Перманентний моніторинг ситуації.* Постійний збір і аналіз інформації щодо діяльності компанії дозволяє завчасно судити про загрозу рейдерського захоплення. З цією метою слід здійснювати постійний моніторинг внутрішньої і зовнішньої ситуації. Об'єктом внутрішнього моніторингу є право власності на акції (частки) компанії і її основні активи, а також дотримання компанією вимог законодавства. Засобами такого моніторингу буде періодичне отримання витягів з відповідних державних реєстрів, моніторинг прав на акції шляхом періодичного отримання виписок з рахунків у цінних паперах у

зберігача, моніторинг судових рішень, пов'язаних з компанією, через інтернет-ресурс «Єдиний державний реєстр судових рішень України». Зовнішнім аспектом моніторингу є факти рейдерських захоплень подібних підприємств в тій же галузі або в тому ж регіоні. Недружнє поглинання одного підприємства може бути лише частиною кампанії рейдера з поглинання цілого комплексу підприємств. Також слід звертати увагу на характерні сигнали, що дозволяють з високою часткою ймовірності судити про загрозу ворожої атаки: раптова активність міноритарних акціонерів (учасників), раптовий інтерес з боку ЗМІ, безліч судових справ проти компанії і перевірок правоохоронних та контролюючих органів за короткий проміжок часу.

12. *Формування «тривожного пакету».* Так званий «тривожний пакет» – це пакет документів, що дозволяє підприємству в разі рейдерського захоплення зберегти головні корпоративні документи компанії, при цьому забезпечивши собі мінімальний набір документів, необхідний для звернення в правоохоронні органи. У «тривожний пакет» входять: завірені копії установчих та інших корпоративних, а також реєстраційних документів компанії (статут з усіма змінами, свідоцтво про державну реєстрацію компанії, протоколи зборів колегіальних органів управління, накази призначення керівника і головного бухгалтера); зразки почерків і підписів акціонерів і засновників, керівника та головного бухгалтера; зразки печатки організації; завірена копія реєстру акціонерів; завірені копії свідоцтв про право власності на об'єкти нерухомості, а також довідка про ринкову вартість об'єктів нерухомості; пояснення акціонерів (учасників) з приводу того, що після останніх загальних зборів акціонерів (учасників) вони не брали участі в інших спільних зборах, не видавали довіреності на участь від свого імені в загальних зборах, не були повідомлені про проведення таких зборів, ніяких документів по відчуженню акцій (частки) не підписували. «Тривожний пакет» повинен зберігатися в недоступному для рейдера місці (наприклад, у нотаріуса або адвоката), доступ до нього повинен бути максимально обмежений, документи потрібно постійно оновлювати в разі змін на підприємстві.

13. *Створення ефективної структури корпоративного управління.* Для створення такої структури, перш за все, рекомендується критично переглянути установчі та інші корпоративні документи компанії, в першу чергу статут і внутрішні положення про органи управління компанії. Корпоративні документи компанії, по-перше, не повинні суперечити імперативним нормам законодавства, а по-друге, повинні передбачати механізми, спрямовані на недопущення можливих рейдерських атак.

ЗМ 5 СУЧАСНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ПЕРСОНАЛУ

Тема 1 Теоретичні основи кадрової політики та кадрової безпеки організації

План лекції

1.1 Суть і завдання та елементи кадрової політики

1.2 Кадрова безпека: сутність та чинники впливу

1.1 Суть і завдання та елементи кадрової політики

Реалізація цілей і завдань управління персоналом здійснюється через кадрову політику. Кадрова політика визначає генеральну лінію і принципові настанови в роботі з персоналом на довготривалу перспективу.

Термін «кадрова політика» має широке та вузьке *значення. В широкому* – це система усвідомлених та певним чином сформульованих та закріплених правил, норм, які приводять людський ресурс у відповідність із довгостроковою стратегією фірми. Вона спрямована на вирішення виробничих, соціальних і особистих проблем людей на різних рівнях відповідальності. *У вузькому* – це набір конкретних правил, привітань та заборон, які реалізуються, як в процесі безпосередніх взаємодій між співробітниками, також і у взаємовідносинах між робітниками та організацією в цілому.

Кадрова політика формується державою, керівними партіями та керівництвом підприємств і знаходить конкретне вираження у вигляді адміністративних і моральних норм поведінки людей у суспільстві, організації. В ринковій економіці істотно змінюється суть і принципи кадрової політики. Вона є усвідомленою і цілеспрямованою на створення високопрофесійного трудового колективу, який би сприяв розвитку організації та особистості.

Формування кадрової політики здійснюється на основі загальної

Декларації прав людини, Конституції держави, Програм керуючої партії, Цивільного Кодексу та Кодексу законів про працю. Кадрова політика розробляється вищим керівництвом підприємства і кадровими службами.

Основним завданням кадрової політики є: своєчасне забезпечення організації персоналом певної якості і кількості відповідно до стратегії розвитку організації; створення умов реалізації, передбачених трудовим законодавством прав і обов'язків громадян; раціональне використання персоналу; формування і підтримка ефективної роботи підприємства.

Кадрова політика формується з врахуванням впливу зовнішніх та внутрішніх факторів, характерних для сучасного і майбутнього. *До зовнішніх факторів* відносяться: національне трудове законодавство; взаємовідношення з профспілкою; стан економічної кон'юнктури; стан і перспективи розвитку ринку праці. *Внутрішніми факторами* є: структура, цілі і стратегія організації; територіальне розміщення; технології виробництва; організаційна культура; кількісний і якісний склад наявного персоналу і можливі його зміни в перспективі; фінансові можливості організацій, які визначають допустимий рівень витрат на управління персоналом; існуючий рівень оплати.

В реалізації кадрової політики можливі альтернативи з врахуванням реального стану економіки. Тому вибір її пов'язаний не тільки з визначенням основної мети, але й з вибором засобів, методів, пріоритетів.

Типи кадрової політики. *Пасивний.* На підприємстві немає чітко вираженої програми дій стосовно персоналу, кадрова політика зводиться до ліквідації негативних наслідків. В організації немає прогнозу кадрових потреб, засобів оцінки праці персоналу. У плані фінансового оздоровлення кадрова проблематика, як правило, відображена на рівні інформаційної довідки про персонал без відповідного аналізу кадрових проблем і причин їх виникнення. *Реактивний.* Керівництво підприємства контролює симптоми кризової ситуації (виникнення конфліктних ситуацій, відсутність достатньо кваліфікованої робочої сили для вирішення завдань, відсутність мотивації до високопродуктивної праці) і вживає заходи до локалізації кризи. Мета кадрової

політики – забезпечення оптимального балансу процесів оновлення і збереження кількісного та якісного складу персоналу, його розвитку, у відповідності з потребами організації, вимогами діючого законодавства та станом ринку праці. *Превентивний.* Керівництво підприємства має обґрунтовані прогнози розвитку ситуації, однак не має засобів впливу на неї.

Кадрова політика спрямована на створення відповідального, згуртованого колективу, здатного своєчасно реагувати на постійно змінювані вимоги ринку з врахуванням стратегії розвитку організації. Вона включає такі елементи: тип влади в суспільстві; стиль керівництва (*авторитарний стиль* характеризується тим, що керівник у прийнятті рішень завжди орієнтується на власні цілі, критерії й інтереси, практично не радиться із трудовим колективом, обмежується вузьким колом однодумців; *демократичний стиль* заснований на сполученні принципу єдиноначальності й громадського самоврядування; *ліберальний стиль* – керівник у прийнятті рішень орієнтується на мети й інтереси окремих груп трудового колективу, постійно намагається маневрувати, щоб дотримати паритету інтересів; *змішаний стиль* передбачає сполучення перерахованих вище типів); філософія підприємства – сукупність моральних й адміністративних норм і правил взаємин персоналу, підлеглих досягненню мети підприємства. Філософія підприємства включає такі розділи: цілі й завдання підприємства, ділові та моральні якості персоналу; умови праці, робоче місце, оплата й оцінка праці; соціальні цінності та соціальні гарантії; правила внутрішнього розпорядку; колективний договір; статут організації.

Правила внутрішнього трудового розпорядку працівників і службовців є важливим нормативним документом, що регламентує найом і звільнення працівників, робочий час, порядок вирішення трудових спорів. Це внутрішній, нормативний документ, який повинен відповідати Кодексу законів про працю і Типовим правилам та враховувати специфіку підприємства. Він включає такі розділи: загальні положення; порядок найму і звільнення працівників; час праці і відпочинку; основні обов’язки працівників та адміністрації; служба і комерційна таємниця; міри заохочення і покарання.

Колективний договір – це правовий акт, що регулює соціально-трудові відносини між найманими працівниками і роботодавцями. У Колективному договорі встановлюються взаємні зобов'язання сторін щодо регулювання трудових, соціально-економічних відносин, зокрема: забезпечення рівноправності сторін, дотримання норм законодавства; встановлення форм, систем і рівня заробітної плати, режиму роботи й умов праці; забезпечення участі членів трудового колективу в управлінні організацією; реальність забезпечення прийнятих зобов'язань, контроль за виконанням колективного договору і відповідальність сторін.

Кадрова політика підприємства здійснюється стратегічними й оперативними системами. *Кадрова стратегія* – це комплекс організаційних рішень і заходів, спрямованих на розробку і реалізацію найбільш важливих кадрових цілей підприємства. Складовими частинами розробки кадрової стратегії підприємства є: планування потреби в кадрах; навчання й підвищення кваліфікації; система регулювання; оплата праці. *Кадрова тактика* – практичні дії по втіленню стратегії.

Інструментом реалізації кадрової політики є *кадрові служби* – основні структурні підрозділи в апарату керування, що виконують оперативну роботу з кадрами. Основними завданнями кадрових служб є: проведення конкурсів на заміщення вакантних посад; прогнозування та визначення поточної і перспективної потреби в кадрах і джерел її задоволення, уточнення потреб у підготовці спеціалістів за прямими зв'язками з навчальними закладами; розробка і реалізація заходів формування трудового колективу; планування та регулювання професійного й кваліфікаційного розвитку персоналу, процесів його звільнення та переміщення; забезпечення професійного, економічного навчання, підготовки і перепідготовки кадрів, стажування; вивчення професійних, ділових особистих якостей працівників на основі атестації, соціологічних дослідів; розробка рекомендацій щодо їх раціонального використання відповідно до здібностей і потреб організації; адаптація молодих спеціалістів, тощо.

1.2 Кадрова безпека: сутність та чинники впливу

Кадрова безпека – це процес запобігання негативних впливів на економічну безпеку підприємства за рахунок ризиків і загроз, пов'язаних з персоналом, його інтелектуальним потенціалом і трудовими відносинами в цілому.

Кадрова безпека залежить від трьох основних чинників.

Наймання – комплекс заходів безпеки при прийомі на роботу і прогнозування благонадійності. До даного фактора входить розгляд питань безпеки компанії на таких етапах в роботі менеджера по персоналу, як пошук кандидатів, процедури відбору, документальне і юридичне забезпечення прийому на роботу, випробувальний термін і навіть адаптація.

Лояльність – задоволеність співробітника умовами, винагородою, перспективами, колективом, захистом від зовнішніх загроз.

Контроль – являє собою комплекс заходів з встановлених для персоналу, в тому числі для адміністрації, регламентів, обмежень, режимів, технологічних процесів, оціночних, контрольних та інших операцій, процедур безпеки. Цей комплекс безпосередньо націлений на ліквідацію можливостей заподіяння шкоди та відпрацьовується, як правило, службою безпеки або іншими підрозділами, але в меншій мірі службою персоналу.

До питань кадрової безпеки належить: забезпечення підприємства необхідними співробітниками, заповнення вакансій; утримання співробітників, їх розвиток; розробка мотиваційних схем і схем оплати праці; усунення збитку у зв'язку з трудовими суперечками; підвищення лояльності співробітників; аналіз ситуації у конкурентів; робота із сайтами вакансій, кадровими агентствами; аналіз ситуації на ринку праці в регіоні; оцінювання підприємства як працедавця (погляд з боку співробітника); способи проектування кар'єри (також погляд з боку співробітника).

Кадрова безпека є комбінацією складових пов'язаних між собою складними зв'язками:

1) *Безпека життєдіяльності*, яка включає: безпека здоров'я (створення певних умов праці працівникам по запобіганню травматизму, захворювання на підприємстві); фізична безпека (виконання комплексу заходів, щодо недопущення порушень правил безпеки).

2) *Соціально-мотиваційна безпека*, яка включає: фінансова безпека (фінансова, грошово-кредитна платоспроможність працівників; впевненість в своєму робочому місці; оплата праці, яка враховує обсяг, кваліфікацію, професіоналізм і якість виконаної роботи); кар'єрна безпека (професійно-кваліфікаційне та посадове просування працівників, заохочення в пристосуванні своєї кваліфікації до вимог робочого місця, в гарантіях виробничого зростання (планування кар'єри): підвищення особистої мобільності на ринку робочої сили; отримання шансів для самореалізації на робочому місці; естетична безпека (проведення загальноосвітніх семінарів, конференцій, групових дискусій; мотивація задоволення персоналу своєю роботою; поліпшення власного іміджу кожного працівника); адміністративно-незалежна безпека (створення умов для відсутності можливості призначення непідготовлених і некомпетентних кадрів, що знаходяться у «родинних» стосунках з власниками, засновниками, акціонерами підприємства до керівництва трудового колективу персоналу);

3) *Професійна безпека*, яка включає: безпеку праці (система принципів, підходів, дій направлена на створення певних умов праці (рівень оплати раці, посада, обладнання робочого місця), з урахуванням новітнього, передового досвіду на ринку праці); інформаційну безпека (прогнозування структури персоналу, визначення потреби в кадрах, планування, залучення та розміщення персоналу; оцінювання результатів праці для виявлення потенціалу кожного працівника); пенсійно-страхова безпека (соціальний захист працівників (страхування,медичне обслуговування); інтелектуальна безпека (безпека володіння сучасними знаннями, впровадження новітніх технологій у розвиток персоналу, удосконалення рівня професійних знань, навичок,умінь, здібностей у зв'язку з розвитком науково-технічного прогресу).

Антиконфліктна безпека, яка включає: патріотична безпека (створення психологічного клімату в колективі на основі позитивного відношення до підприємства, що характеризується психологічними показниками об'єднаності працівників, яка забезпечує узгодженість, безконфліктність спілкування, відповідальність та обов'язок, товариську допомогу, вимогливість до себе та іншого в інтересах виробництва); психолого-комунікаційна безпека (сприяння міжособистісним комунікаціям і створенню сприятливого мікроклімату; врахування інтересів і побажань працівників, його особистого потенціалу; задоволеність міжособистісними стосунками по вертикалі (керівник-підлеглі) та горизонталі (виконавці)).

Визначаючи первинність працівників у діяльності організації, важливо зазначити, що саме від персоналу йдуть значні загрози підприємству. Ці загрози за місцем виникнення можна поділити на дві групи: внутрішні і зовнішні. *До внутрішніх загроз відносять*: невідповідність кваліфікації працівників вимогам до них; недостатня кваліфікація працівників; слабка організація системи управління персоналом; слабка організація системи навчання; неефективна система мотивації; помилки в плануванні ресурсів персоналу; зниження кількості раціоналізаторських пропозицій та ініціатив; відхід кваліфікованих працівників; працівники зорієнтовані на вирішення внутрішніх тактичних завдань; працівники зорієнтовані на дотримання інтересів підрозділу; відсутність корпоративної політики або вона «слабка»; неякісні перевірки кандидатів для приймання на роботу. *Зовнішні загрози* включають: умови мотивації у конкурентів кращі; настанова конкурентів на переманювання; тиск на працівників ззовні; потрапляння працівників у різні види залежності; інфляційні процеси (не можна не враховувати під час розрахунку заробітної плати і прогнозувати її динаміку).

До найпоширеніших видів порушень при недотриманні кадрової безпеки належать: афери з боку провідних спеціалістів (менеджерів і керівників середньої ланки, відповідальних за конкретний напрям бізнесу підприємства), в основному «за стінами» своєї фірми, зокрема у міжнародних організаціях;

фальсифікація сум «живих грошей» («готівки») у касі й сум на банківських рахунках, підробка чеків підприємства; несанкціонований продаж і використання майна (власності) підприємства із корисливою метою; оплата роботи підставних («фіктивних осіб»), так званих «пролісків»; фальсифікація документації підприємства за допомогою електронної техніки й Інтернету (наприклад, перерахування коштів підприємства на свій особистий рахунок, внесення «потрібних» змін у звітні документи); несанкціоновані операції із цінними паперами, матеріальними й нематеріальними активами підприємства; фальсифікація звітів про використання коштів, виділених на відрядження, «представницькі видатки», на інші потреби підприємства.

Мотивацію афер персоналу підприємства можна класифікувати так: особисті фінансові труднощі, неможливість задоволення життєвих потреб своїх та сім'ї; наявність слабких місць у системі управління діяльністю фірми (зокрема в системі бухгалтерського обігу); низька кваліфікація керівництва підприємства; нездоровий діловий клімат у колективі підприємства (наявність «скривджених»); психологічна готовність (схильність) працівника до зловживання службовим становищем; порочні зв'язки, вчинки, захоплення; відсутність налагодженого контролю з боку керівництва за діяльністю персоналу; слабкий кадровий менеджмент, що дає змогу займати відповідальні посади співробітникам-аферистам, неефективна персональна робота з кадрами.

Основними *суб'єктами кадрової безпеки* підприємства є служба управління персоналом і служба безпеки.

Тема 2 Робота з персоналом щодо забезпечення кадрової безпеки підприємства

План лекції

1.1 Людський фактор в системі забезпечення безпеки підприємства

1.2 Способи перевірки інформації про кандидатів на вакантну посаду

1.1 Людський фактор в системі забезпечення безпеки підприємства

Безпека системи визначається надійністю її найслабшої ланки. Найбільш складним і одночасно найбільш уразливим ланкою будь-якої системи, будь то людино-машинна система або підприємницька організація, є людина.

Негативний вплив людини на безпеку позначають поняттям «*людський фактор*», тобто сукупність соціально-економічних здібностей людини, ступінь реалізації яких обумовлена мотивацією і ставленням людини до процесу трудової діяльності, його моральної і матеріальної зацікавленістю у високопродуктивній праці.

Основними проявами людського фактора є наступні: людина в процесі своєї діяльності з тих чи інших причин може допускати помилки різного характеру; особа, яка приймає рішення, в умовах невизначеності може прийняти помилкові рішення; в процесі життєдіяльності людина може опинитися в екстремальній ситуації, коли фізичні і психологічні навантаження досягають таких рівнів, при яких індивідуум втрачає здатність до раціональних дій і рішень, адекватних ситуації, що склалася, тощо.

1.2 Способи перевірки інформації про кандидатів на вакантну посаду

Збирати та аналізувати інформацію про кандидатів на вакантну посаду необхідно для того, щоб попередньо оцінити та відібрати кандидатів за формальними характеристиками, перевірити надану ними інформацію і гарантувати кадрову безпеку підприємства.

Якісна перевірка кандидатів під час прийому на роботу знизить ймовірність зловживань зі сторони решти. Серед зловживань в наш час найчастіше зустрічаються випадки підробки документів, фальсифікації витрат, пов’язаних з виконанням трудових обов’язків (відрядження, представницькі витрати), так звані «відкати» (один із найпоширеніших способів) популярні при несанкціонованих продажах і використаннях майна підприємства і т.п.

Серед методів підбору персоналу слід виділити розроблення та проведення тестів на виявлення професійної орієнтації, ерудиції, інтелекту, здібностей і розуміння.

Головна мета попереднього оцінювання – відсіяти кандидатів, які не відповідають мінімальним вимогам вакантної посади, що допоможе в подальшому заощадити час і сили на підготовку і проведення інтерв'ю.

Попереднє оцінювання починається з аналізу резюме, вивчення якого є першим знайомством з кандидатом. За результатами аналізу резюме всіх кандидатів можна розділити на три групи: 1. кандидати, які мають значні конкурентні переваги в порівнянні з іншими. Таких кандидатів потрібно обов'язково запросити на інтерв'ю. 2. кандидати, поступаються за рівнем конкурентоспроможності представникам першої групи. Незважаючи на це, їх можна запросити на інтерв'ю, якщо не набереться достатньої кількості кандидатів, віднесених до першої групи. 3. кандидати, що не мають необхідної кваліфікації для виконання обов'язків за посадами, на які вони претендують. До цієї групи слід віднести і кандидатів, що надіслали резюме з граматичними помилками. Кандидатів з найбільш низьким рівнем конкурентоспроможності не варто запрошувати на інтерв'ю.

Резюме може містити інформацію про: посади, на яку претендує кандидат, його компенсаційних очікуваннях; біографічних даних: вік, стать, місце проживання, сімейний стан, освіта; місця роботи на займаних раніше посадах, дати прийняття і звільнення; функції та обов'язки, які виконувалися за посадами і місцях роботи; досягнення; індивідуально-особистісні характеристики; інтереси та захоплення; уявленнях про бажане місце роботи; можливостях надання рекомендацій, тощо. Резюме потрібно вивчати в напрямку знизу вгору, в порядку викладу кандидатом ланцюга важливих подій в навчанні і трудового життя. Особливо ретельно необхідно аналізувати інформацію про підготовку і підвищення кваліфікації: чи містить резюме дані про рівень освіти кандидата; чи відповідають дані висунутим вимогам; в якій послідовності отримано освіту; в якому навчальному закладі, за якою формою

навчався кандидат; чи відповідають посади, займані кандидатом, отриманою професією; наявність додаткової освіти; використовується чи додаткову освіту в трудовій діяльності; періодичність підвищення кандидатом кваліфікації; чи відповідає тематика семінарів, тренінгів, курсів профілем основної діяльності; чи володіє кандидат винятковими знаннями та навичками; наскільки цінною для підприємства є професія кандидата і чи буде зростати її цінність в майбутньому.

Аналізуючи трудову діяльність кандидата, необхідно акцентувати увагу на таку інформацію: наскільки точно описані функції та обов'язки; наскільки широкими або спеціалізованими є професійні інтереси; чим керувався кандидат, обираючи певне місце роботи; чи були в трудового життя кандидата злети і падіння.

Поряд з даними про досвід роботи, рівень освіти та іншими формальними характеристиками має значення форма подання інформації, логіка викладу, формулювання, грамотність. За наданою кандидатом інформації необхідно описати його життєвий шлях і відшукати важливі дані про особистісні характеристики, професійних і ділових якостях, мотиви поведінки.

Щоб отримати більш детальну інформацію про кожного кандидата і належним чином її структурувати, ретельно підготуватися до інтерв'ю, фахівці з управління персоналом розробляють *стандартні форми* (анкети, оціночні листи і т. д.). Заповнені стандартні форми кандидати можуть надсилати електронною поштою, попередньо отримавши бланки, або ж заповнювати їх на підприємстві. Зміст стандартних форм може бути різноманітним, залежно від специфіки підприємства, вакантної посади, вимог, які висуваються до кандидату, політики підприємства в області професійного підбору. Деякі підприємства використовують стандартні особисті листки з обліку кадрів, але більшість розробляє спеціальні деталізовані анкети.

Оптимальним, достовірним і об'єктивно найефективнішим напрямком діяльності з професійного відбору є застосування спеціальних психофізіологічних досліджень, як-то: діагностика нейродинамічних,

індивідуально-типологічних та особистісних характеристик індивіда, визначення його індивідуального психосемантичного поля значень, пов'язаних з мотивацією вступу на службу, ставленням до наркотиків та алкоголю тощо; проведення поглиблених поліграфних опитувань (поліграфний скринінг) за методиками, складеними на підставі попередньо отриманих даних.

Тема 3 Сучасні технології забезпечення надійності та лояльності персоналу

План лекції

3.1 Політика забезпечення надійності персоналу та критерії її оцінки

3.2 Психологічні чинники низької надійності персоналу

3.3 Шляхи забезпечення надійності персоналу

3.4 Лояльність персоналу та управління нею

3.1 Політика забезпечення надійності персоналу та критерії її оцінки

Надійність є однією з важливих складових професійної придатності *співробітників* як державних, так і недержавних організацій. Працівники, що володіють такою якістю, зберігають моральну стійкість і лояльність до компанії, в якій працюють, відчувають себе «прив'язаними» до неї, сама робота представляє для них високу мотиваційну значимість, а її втрата оцінюється як серйозна життєва невдача.

Ступінь *надійності* залежить від різних причин і може змінюватися у людей у зв'язку зі зміною умов, виникненням нестандартних і особливо екстремальних (надзвичайних), кризових ситуацій.

Серед першочергових завдань підвищення ефективності функціонування управлінських та виконавчих структур найважливішими є укомплектування їх працівниками, які мають необхідні якості для успішного оволодіння обраною професією, створення системи, що дозволяє зберігати та розвивати їх працездатність та надійність. Виконання таких завдань неможливе без періодичного

контролю функціонального стану працівника та визначення об'єктивних критеріїв, які характеризують якісний склад таких органів та підрозділів.

Одним із критеріїв, що вказує на реальний стан професійної відповідності та надійності персоналу, є *плинність кадрів*. Характеризуючи цей показник, можна виділити такі складові: звільнення працівників із досягненням граничного віку перебування на службі; звільнення за станом здоров'я відповідно до середньостатистичних показників захворюваності в цілому по країні; небажання продовжувати працювати на конкретному робочому місці через різноманітні соціальні й професійно значущими мотивами; дискредитація звання працівника установи, відомства, фірми тощо; дисциплінарні провини і посадові злочини, професійна деформація тощо.

Надійність роботи персоналу визначається величиною можливих збоїв у роботі всіх підрозділів підприємства через несвоєчасне надання інформації, помилки у розрахунках, порушення трудової дисципліни тощо.

Комплекс технічних, програмних, математичних та інформаційних засобів називають комп'ютерним поліграфом або «детектором брехні».

Поліграфні опитування – це комплекс спеціальних тестів, технічних засобів, програмного, математичного та інформаційного забезпечення. Взаємодія цього комплексу з обстежуваним дає можливість виявити приховану ним інформацію.

Під час *планових перевірок* проводять, як правило, тільки поліграфні опитування, причому їх регулярність регламентована відомчими нормативними актами. *Позапланові перевірки* проводять у випадках посадових змін, проведення службових розслідувань, при оформленні допуску до робіт, що вимагають більш високого рівня таємності. Інформація про методики проведення поліграфних опитувань, технічні можливості спеціальних поліграфів є державною таємницею.

До складу загальної кількості перевірок входять: перевірки, пов'язані з процедурою профвідбору кадрів, планові та позапланові скринінги, службові розслідування та заходи боротьби зі злочинністю.

3.2 Психологічні чинники низької надійності персоналу

Ненадійність, тобто моральна вразливість людини, може визначатися різними факторами і причинами. До їх числа можна віднести наступні:

1. Нехтування і навіть презирство по відношенню до загально визнаних моральних норм.

2. Індивідуалістична спрямованість особистості, невміння і небажання працювати в єдиній команді, стійке прагнення протиставити себе колегам, відсутність корпоративних почуттів, прихильності до місця роботи і колективу.

3. Завищена самооцінка, яка не відповідає реальним можливостям людини, віра у власну непогрішність, непомірне марнославство, незадоволені амбіції, заздрісність. Істотну роль при цьому може грати незадоволеність кар'єрою, протиріччя між високими намаганнями і реальним просуванням по службі.

4. Риси характеру, обумовлені психопатією, що характеризуються мстивістю, злопамятностью, підвищеної уразливістю. Такі люди довго не можуть звільнитися від своїх негативних переживань, їм зазвичай властива конфліктність з оточуючими. Особливо небезпечний стійкий конфлікт «по вертикалі», коли працівник надовго зберігає бажання помститися за нанесені образи своєму керівнику.

5. Інфантилізм (особистісна незрілість), відсутність самостійності суджень, орієнтація на інших, більш сильних в психологічному відношенні людей, в прийнятті рішень і діях (легка добровільна підпорядкованість впливу з боку).

6. Імпульсивність, яка є домінуючою в поведінці. Вона проявляється в тому, що людину легко привести до втрати самоконтролю і необдуманих, нерозважливих дій. Їм притаманні слабкості особистого характеру (наприклад, зловживання спиртними напоями, пристрасть до азартних ігор та ін.). Вчинки таких людей визначаються не усвідомленими цілями і намірами, а внутрішніми імпульсами або зовнішніми обставинами (наприклад, нав'язаними ззовні

бажаннями).

7. Невлаштованість в особистому житті, відчуженість від інших, самотність, «втрата коренів», відсутність близьких людей, зв'язку з ними.

8. Гостра ситуативна життєва потреба (наприклад, в дорогому лікуванні), яку людина не може реалізувати самостійно. Даний фактор є найменш прогнозованим, а значить і найменш керованим. У той же час оперативне отримання повної і достовірної інформації про виникнення такої ситуації може знизити її негативний вплив на надійність працівника.

9. Наявність зв'язку даної людини з будь-ким з представників конкуруючих фірм. Це дуже небезпечний фактор, оскільки найбільш значних збитків в умовах жорсткої конкуренції можуть нанести саме ті, хто можуть бути спеціально впроваджені конкурентами в компанію для з'ясування інформації про стан справ в ній «зсередини» або використаний в інший спосіб завдяки родинним або іншим близьким зв'язкам.

3.3 Шляхи забезпечення надійності персоналу

Напрямки роботи, що сприяють підвищенню надійності та попередження нелояльності працівників :

проведення серйозного і всебічного відбору кадрів, при якому: не допускається прийняття на роботу осіб, що мають серйозні особистісні недоліки, соціальні зв'язки, що порочать їх; біографію, яка свідчить про наявність у них моральних дефектів; обов'язково встановлюється випробувальний термін для всіх найманих працівників;

наявність випробувального терміну дозволяє більш точно оцінити особисті та ділові якості співробітника, визначити його придатність до виконання тих завдань, які перед ним планується поставити. Доцільно доповнити загальні умови такими заходами, як особисту поруку працівників, за рекомендацією яких береться на роботу кандидат, отримання інформації з колишніх місць навчання або роботи, аналіз результатів його попередньої

діяльності тощо;

створення умов, при яких працівнику буде невигідно здійснювати дії, що завдають шкоди організації і її керівництва. Ці умови повинні включати цілу систему заходів щодо морального та матеріального стимулювання, формування престижності роботи саме в цій компанії, турботи про зовнішній і внутрішній імідж компанії, створення в ній такого соціально-психологічного клімату, який був би сприятливим для кожного працівника;

формування корпоративності працівників, тобто вжиття заходів зі створення у них почуття приналежності до організації з тим, щоб вважати її «своєю», і в разі ускладнень звертатися за допомогою до компанії, а не шукати її на стороні;

попередження ситуацій, при яких працівник або близькі йому люди можуть опинитися в безвихідному критичному положенні при виникненні гострих життєвих проблем;

введення прогресивної системи матеріального та інших видів стимулювання, додатково «прив'язують» працівника до компанії, які він не зможе отримати в конкуруючих організаціях. Така система може включати заохочення за сумлінну працю, дотримання трудової дисципліни і лояльність компанії (вручення премій, цінних подарунків чи інших нагород, туристичних путівок та ін.);

забезпечення змішаного стилю керівництва. Це означає, що стиль роботи керівників будь-якого рангу в організації не повинен бути жорстко авторитарним, приводити до приниження гідності підлеглих з тим, щоб не провокувати зворотний негативний реакції;

створення і зміцнення в компанії морально-психологічного клімату, що перешкоджає виникненню надзвичайних подій (тобто не допускає виникнення випадків порушення лояльності), а також сприятливого для ефективної роботи кожного;

проведення періодичних атестацій працівників, за допомогою яких необхідно отримати об'єктивні відповіді на наступні питання: чи людина хоче

працювати в компанії, чи може вона працювати на тому рівні, який від нього вимагається, наскільки вона в змозі виконувати покладені на неї обов'язки, чи справляється своїми обов'язками, як ставиться до своєї роботи, чи задоволена вона роботою, наскільки вміє працювати в колективі, чи здатна вона слідувати корпоративній культурі, чи не є вона джерелом постійних конфліктів, сварок, суперечок тощо;

формування «командного духу», згуртованості;

взяття підписки про нерозголошення службової інформації та необхідності дотримання правил поведінки, що перешкоджають випадків прояву ненадійності. В підписку обов'язково повинен включатися пункт про те, що у випадках прояви моральної ненадійності керівництво залишає за собою право залучити працівника до відповідальності відповідно до чинного законодавства;

періодичне (щорічне або щоквартальне) нагадування працівникам про необхідність дотримання певних правил поведінки з відновленням відповідної підписки;

організаційні заходи, що сприяють збереженню комерційної та іншої службової таємниці;

звільнення працівника за грубі порушення дисципліни і нелояльність - «розставання» має бути «мирним». У разі нанесення компанії значного матеріального або морального збитку працівник (діючий або колишній) може бути притягнутий до відповідальності.

3.4 Лояльність персоналу та управління нею

Існує точка зору, що кадрова безпека визначається трьома показниками: 1) рівнем професіоналізму, 2) належністю частини співробітників до «груп ризику» (співробітники з різними аддикціями, з розладами особистості та схильні до делінквентної поведінки) і 3) лояльністю персоналу. Остання складова є універсальною за своєю направленістю: ставлення людини до

власної організації є фактором, який або зміцнює, або руйнує систему кадрової безпеки. Тобто чим менш лояльний робітник, тим більшої потенційної шкоди своїми діями чи бездіяльністю він може завдати.

Лояльність персоналу – це доброзичливе, коректне, щире, поважне ставлення до керівництва, працівників, інших осіб, їх дій, до компанії в цілому; свідоме виконання працівниками своєї роботи відповідно до цілей і задач та в інтересах компанії, а також дотримання норм, правил і зобов'язань, включаючи неформальні, відносно компанії, керівництва, працівників та інших суб'єктів взаємодії.

Основні чинники лояльності персоналу наступні: досвід роботи, відповідність цінностей, підтримка організації, організаційна справедливість, відношення до підприємства і поведінка співробітника, кадрова безпека, економічна ефективність персоналу. Основні складові лояльності персоналу – задоволення роботою, залучення, відданість.

З позиції служби економічної безпеки, яка вважає персонал «слабким місцем організації», всі працівники вважаються потенційно нелояльними. Під «нелояльною» поведінкою розуміють свідоме або несвідоме завдання шкоди діяльності суб'єкту господарської діяльності.

З позиції служби управління персоналом лояльність, розглядати як емоційну прихильність до організації, рівень якої залежить від ступеня сприйнятливості персоналом зовнішніх (зарплата, пільги, робочі умови тощо) та внутрішніх (зміст виконуваної роботи, можливості професійного зростання, визнання і оцінка досягнень) стимулів, які пропонує роботодавець.

Обов'язкові атрибути лояльності: чесність по відношенню до об'єкта лояльності; поділ з об'єктом лояльності основних переконань, цінностей; · вболівання за успіх лояльності; відкрита демонстрація лояльності, доброзичливе ставлення; готовність попередити небезпеку для об'єкта лояльності; готовність при необхідності йти на певні жертви на користь об'єкта лояльності; почуття гордості за причетність до об'єкту лояльності (наприклад, за приналежність до числа співробітників компанії); прагнення найкращим

чином виконувати обов'язки, функції, місію, покладені на людину об'єктом лояльності.

Виділяють *три головні складові лояльності:* довіру персоналу до керівництва компанії; справедливість відносин, що складаються у співробітника з представниками адміністрації компанії; задоволеність роботою.

Рівні лояльності персоналу: нульова лояльність; нелояльність (прихована і демонстративна; лояльність на рівні зовнішніх атрибутів; лояльність на рівні вчинків; лояльність на рівні переконань; лояльність на рівні ідентичності (є найвищим рівнем).

В якості об'єктивних «зовнішніх» показників лояльності можна розглядати якість і продуктивність праці, рівень дисципліни співробітників, кількість або відсутність доган тощо. В рамках комплексного обстеження об'єктивні показники варто сполучати з суб'єктивними індикаторами, що виражають стан свідомості індивіда (табл. 3.1).

Таблиця 3.1– Основні показники, покладені в основу методики вимірювання рівня лояльності персоналу організації

Показники солідарності	Показники залученості	Показники ідентичності
1	2	3
Солідарність з успіхом організації	Залученість у систему обміну (наявність зобов`язань)	Відчуття задоволення від приналежності до організації
Солідарність з нормами: а) додержання робочого режиму, встановленого в організації (розклад робочого дня, пунктуальність); б) додержання регламентів у виконанні завдань; в) використання ресурсів компанії виключно у робочих цілях	Залученість: а) готовність до додаткових зусиль в інтересах організації, не обмежуючись посадовими інструкціями; б) виконання корисної для організації роботи, яка безпосередньо не заохочується або невиконання якої не засуджується; в) ступінь докладання робітником зусиль при виконанні своєї роботи; г) ініціативність при виконанні завдань	Сприйняття символів та атрибутів, пов'язаних з організацією (символіка, спеціальна робоча форма одягу, обов'язкові атрибути інтер'єру в організації)

Продовження таблиці 3.1

1	2	3
Солідарність з керівництвом: а) солідарність з позицією керівництва; б) повага до рішень керівництва та ретельність у їх виконанні	Участь в позавиробничих відносинах: а) схвалення участі в корпоративних заходах; б) налагоджені комунікативні зв'язки з колективом	Ідентичність з трудовим колективом (групова ідентичність). Відчуття себе невід'ємною (важливою) частиною організації

Управління лояльністю персоналу – це процес, що дозволяє підприємству оптимізувати наявний людський ресурс, підвищити ефективність діяльності підприємства за рахунок підвищення якості виконуваних робіт і включення персоналу в роботу підприємства, тобто формування високого ступеню лояльності персоналу.

Етапи розробки системи управління лояльністю персоналу:

формування концепції управління лояльністю персоналу, що визначає основні принципи роботи з персоналом, які пов'язані з кадровою стратегією підприємства;

аналіз внутрішнього і зовнішнього середовища підприємства, аналіз ресурсної системи – визначає, на які ринки робочої сили необхідно виходити і в якій кількості залучати додаткових працівників, у випадку якщо внутрішніми ресурсами неможливо забезпечити досягнення результату;

визначення проблемних зон підприємства – в процесі управління персоналом дозволяє визначити пріоритетні напрями дій зі зміни цієї ситуації і приведення роботи з персоналом відповідно до розробленої концепції;

вироблення цілей роботи з персоналом, тобто визначення конкретних показників і способів їх досягнення співробітникам. Цілі роботи з персоналом мають бути сформовані у рамках загальних цілей підприємства;

формування набору заходів щодо створення лояльного персоналу. Повинне враховувати специфіку підприємства, бути спрямоване на готовність співробітника застосувати додаткові зусилля в інтересах підприємства, з метою підвищення ефективності й продуктивності своєї праці;

процес реалізації заходів. Забезпечує скоординовану розробку і реалізацію планів підприємства та системи управління персоналом;

контроль – забезпечує визначення відповідності (чи невідповідності) напрямів управління, що реалізуються, стану зовнішнього і внутрішнього середовища, формування напряму змін.

СПИСОК ЛІТЕРАТУРИ

1. Андрощук Г. А. Экономическая безопасность предприятия : защита коммерческой тайны : монография / Г. А. Андрощук, П. П. Крайнев; ред. А. Д. Святоцкий. – Київ : ВД «Ін Юре», 2000. – 400 с.

2. Ареф'єва О. В. Планування економічної безпеки підприємств / О. В. Ареф'єва, Т. Б. Кузенко. – Київ : Видавництво Європейського ун-ту, 2004. – 169 с.

3. Барановський О. І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення) / О. І. Барановський ; Київ. нац. торг.-екон. ун-т. – Київ : КНТЕУ, 2004. – 759 с.

4. Бланк И. А. Управление финансовой безопасностью предприятия / И. А. Бланк. – Київ : Ника-Центр, Эльга, 2004. – 784 с.

5. Бондарчук Ю. В. Безпека бізнесу: організаційно-правові основи: науково-практичний посібник / Ю. В. Бондарчук, А. І. Марущак. – Київ : Видавничий дім «Скіф», КНТ, 2008. – 372 с.

6. Веретенникова Г. Б. Економічна безпека підприємства: планування й організація : конспект лекцій / Г. Б. Веретенникова. – Харків : ХНЕУ, 2008. – 83 с.

7. Донець Л. І. Економічна безпека підприємства : навчальний посібник для студентів вищих навчальних закладів / Л. І. Донець, Н. В. Ващенко. – Київ : ЦУЛ, 2008. – 239 с.

8. Єрмошенко М. М. Економічні та організаційні засади забезпечення фінансової безпеки підприємства : препринт наукової доповіді / за наук. ред. М. М. Єрмошенка. – Київ : Нац. академія управління, 2005. – 77 с.

9. Зубок М. І. Безпека банківської діяльності: навч.-метод. посібник для самостійного вивчення дисципліни / М. І. Зубок. – Київ : КНЕУ, 2003. – 156 с.

10. Користін О. Є. Економічна безпека : навч. посібник / О. Є. Користін, О. І. Барановський, Л. В. Герасименко. – Київ : КНУВС, 2010. – 368 с.

11. Кузенко Т. Б. Фінансова безпека підприємства: навчальний посібник / Т. Б. Кузенко, О. В. Грачов, О. Ю. Литовченко. – Харків : Вид. ХНЕУ, 2010. – 300 с.

12. Куркін М. В. Контроль та захист економічної безпеки діяльності підприємства : навч. посібник / М. В. Куркін, В. Д. Понікаров, Д. В. Назаренко. – Харків : ІНЖЕК, 2010. – 297 с.

13. Моделювання економічної безпеки: держава, регіон, підприємство : [монографія] / [В. М. Геєць, М. О. Кизим, Т. С. Клебанова та ін.] ; за ред. В. М. Гейця. – Харків : ВД «ІНЖЕК», 2006. – 240 с.

14. Мойсеєнко І. П. Управління фінансово-економічною безпекою підприємства : навч. посібник / І. П. Мойсеєнко, О. М. Марченко. – Львів : ЛДУВС, 2011. – 380 с.

15. Орлов П. І. Основи економічної безпеки фірми : навч. посібник / П. І. Орлов, В. Є. Духов. – Харків : ТОВ «Прометей-Прес», 2004. – 284 с.

16. Основи економічної безпеки : підручник / О. М. Бандурка, В. Є. Духов, К. Я. Петрова, І. М. Червяков. – Київ : Вид-во нац. ун-ту внутр. справ, 2003. – 236 с.

17. Отенко І. П. Економічна безпека підприємства : навч. посібник / І. П. Отенко, Г. А. Іващенко, Д. К. Воронков. – Харків : ХНЕУ, 2012. – 251 с.

18. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур / Н. Й. Реверчук. – Львів : ЛБІ НБУ, 2004. – 196 с.

19. Соснин А. С. Менеджмент безопасности предпринимательства : учеб. пособие / А. С. Соснин, П. Я. Прыгунов. – Киев : Изд-во Европ. ун-та, 2002. – 559 с.

20. Стрельбицька Л. М. Основи безпеки банківської системи України та банківської діяльності : [монографія] / Л. М. Стрельбицька, М. П. Стрельбицький. – Київ : Кондор, 2004. – 168 с.

21. Фоміна М. В. Проблеми економічно безпечного розвитку підприємства: теорія і практика : [монографія] / М. В. Фоміна. – Донецьк : ДонДУЕТ, 2005. – 140 с.

Навчальне видання

ЛИТОВЧЕНКО Олена Юріївна

КОНСПЕКТ ЛЕКЦІЙ

з навчальної дисципліни

«КОМПЛЕКСНЕ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ»

(для студентів денної і заочної форм навчання освітнього рівня магістр спеціальності 073 – Менеджмент)

За авторською редакцією

Відповідальний за випуск *Г. І. Кизилов*

Комп'ютерне верстання *Є. Г. Панова*

План 2017, поз. 193Л

Підп. до друку 05.07.2017. Формат 60×84/16.
Друк на ризографі. Ум. друк. арк. 8,8.
Тираж 50 пр. Зам. № .

Видавець і виготовлювач:
Харківський національний університет
міського господарства імені О. М. Бекетова,
вул. Маршала Бажанова,17, Харків, 61002.
Електронна адреса: rectorat@kname.edu.ua.
Свідоцтво суб'єкта видавничої справи:
ДК № 5328 від 11.04.2017.