Міжнародний фонд соціальної адаптації

Вищий навчальний заклад «Університет економіки і права «КРОК»

Зубок М.І.

Інформаційна безпека в підприємницькій діяльності

Підручник

м.Київ – 2014

УДК 366.56(075.8)
ББК 65.32я73
З-91

Рецензенти:

Рубцов В.С. – кандидат технічних наук, доцент
Марков С.Л. – кандидат психологічних наук, доцент
Легомінов В.І. – кандидат воєнних наук

Рекомендовано вченою радою Вищого навчального закладу «Університет економіки і права «КРОК»
(протокол № 4 від 24 грудня 2014р.)

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

ISBN 978-966-2760-20-0

В підручнику розкриваються особливості сучасного інформаційного розвитку та його вплив на підприємницьку діяльність. Основна увага приділена розгляду загроз та ризиків, які обумовлюються інформаційними взаємовідносинами суб'єктів підприємництва, організації їх інформаційної безпеки, використанню інформаційних переваг в бізнесі, діяльності з мінімізації інформаційних ризиків .

Підручник розраховано на студентів, які навчаються за спеціальністю «Управління фінансово-економічною безпекою», слухачів, що проходять підготовку за програмою підвищення кваліфікації зі спеціальності «Забезпечення безпеки підприємницької діяльності суб'єктів господарювання в Україні», проекту «Україна-Норвегія», а також фахівців, які професійно переймаються питанням інформаційної безпеки суб'єктів підприємництва.

УДК 366.56(075.8)
ББК 65.32я73
З-91

ISBN 978-966-2760-20-0

ЗМІСТ

Вступ 4
1. Сучасне інформаційне середовище підприємницької діяльності 7
1.1. Інформаційний розвиток і його сучасні особливості 7
1.2. Інфраструктура інформаційного середовища 18
1.3. Інформаційна економіка та її наслідки 24
1.4. Інформаційні взаємовідносини суб'єктів підприємництва 33
2. Безпека бізнесу в Україні: історія та сучасність 39
3. Інформаційні загрози та загрози інформації 52
4. Основи організації інформаційної безпеки суб'єктів підприємництва 77
5. Правові засади інформаційної безпеки суб'єктів підприємництва 88
6. Захист інформації в діяльності суб'єктів підприємництва 104
6.1. Інформація з обмеженим доступом в підприємницькій діяльності 104
6.2. Система захисту інформації суб'єктів підприємництва 113
6.3. Особливості захисту інформації в комерційній діяльності суб'єктів підприємництва та їх ділових взаємовідносинах 132
7. Інформаційне забезпечення підприємницької діяльності 143
7.1. Інформаційний ресурс суб'єктів підприємництва і його характеристики 145
7.2. Інформаційно-аналітична робота в діяльності суб'єктів підприємництва 152
7.3. Спеціальні інформаційні операції та комерційна розвідка в підприємницькій діяльності 171
8. Протидія інформаційно-психологічному впливу в підприємницькій діяльності ... 186
9. Управління інформаційними ризиками в діяльності суб'єктів підприємництва 192
Висновки 214
Інформаційні джерела 219
Додатки 223

Вступ

Зміни, що відбулись в останні роки у суспільному житті, політиці, економіці, науковій сфері призвели до значного зростання обсягів інформації. Поряд з останнім зросла і швидкість зміни інформації. За таких умов сформувалась ситуація за якої виник розрив між кількістю інформації, що характеризує сучасне буття і спроможністю її засвоїти та ефективно використати. Виникла проблема інформаційної дезорієнтації, яка значним чином ускладнила прийняття об'єктивних рішень та можливість формування адекватної поведінки. Всеохоплююча інформатизація зумовила нові форми політичних, економічних, соціальних відносин, виникнення т. з. інформаційної індустрії, пов'язаної з інформаційним забезпеченням різних видів життєдіяльності. Широкого поширення набули інформаційні і комунікаційні технології, змістом яких стало формування інформаційного ресурсу та його збереженням, передача інформації, надання різного роду інформаційних послуг. Така ситуація значним чином розширила можливості формування знань, які забезпечили для громадян, суб'єктів господарювання, суспільства, держави створення нематеріального капіталу. Останній по своїй потужності є суттєвим фактором створення переваг на будь-якому ринку чи у будь-яких взаємовідносинах.

Характеризуючи сьогоднішню ситуацію з позиції ролі інформації можна говорити, що у підприємницькій діяльності вона стала обов'язковою умовою формування додаткової вартості. Вкладання коштів з метою розвитку бізнесу вимагає конкретних і об'єктивних знань про сфери, об'єкти, види діяльності за яких вкладені кошти гарантовано можуть принести прибуток. Маючи на увазі відому формулу К. Маркса «Гроші – Товар – Гроші» , можна говорити, що сьогодні вона видозмінюється до виду: «Гроші – Інформація – Товар – Гроші».

За таких умов значно зросла привабливість інформації, особливо тієї її частини, яка характеризує певні технології, тому власники такої інформації поряд з демонстрацією своїх інтелектуальних переваг, вимушені вживати

заходів захисту своїх інтелектуальних об'єктів та інформації про них. Разом з тим, значного розвитку отримали технології збору і обробки інформації, механізми формування джерел інформації. Такі технології давно перестали бути прерогативою спецслужб, вони широко застосовуються в політичній, економічній та інших видах діяльності. З метою забезпечення розвитку своєї діяльності та самозбереження суб'єкти підприємництва вдаються до розробки та використання інформаційних технологій впливу, що започаткувало нові особливості їх взаємовідносин. Останні, перебуваючи лише у інформаційній площині, отримали самостійний статус, т. з. інформаційних відносин. Тобто, тотальне поширення інформації і її технологій у суспільстві, міжнародних відносинах зумовило залежність подальшого розвитку, а то і існування суб'єктів будь-якого бізнесу від неї. Більш того, можливість володіння інформацією та ефективного використання її технологій утворило умови для монополізації влади чи ринку, що значно загострило інформаційні відносини. Останні ж досить часто ставали не лише конкурентними, а і носили характер антагоністичних та агресивних. За таких умов інформаційні технології перетворювались у особливий вид впливу – інтелектуальну зброю, а відносини суб'єктів набули характеру інформаційної війни. Наявність та застосування інтелектуальної зброї у взаємовідносинах в т. ч. і суб'єктів підприємництва утворює необхідність вироблення адекватних заходів захисту від її вражаючих факторів та особливої поведінки суб'єктів у інформаційних відносинах, тобто будувати відповідну систему інформаційної безпеки. Остання ж має генерувати механізми захисту від заходів інформаційній агресії та протидії інформаційному впливу, забезпечувати захист власних інформаційних ресурсів суб'єктів та формування обсягу знань необхідного для ефективного розвитку їх бізнесу.

Враховуючи, що інформаційні проблеми, які постали перед суспільством в останні роки стали досить актуальними, їм було присвячено значну кількість досліджень, у різних сферах діяльності. Беручи до уваги підприємницьку діяльність можна звернути увагу на роботи Когута Ю.І., Марущака А.І.,

Кормича Б.А., Берлача А.І., Ніколаюка С.І., Никифорчука Д.Й., Позднишева Є.В., Вертузаєва М.С. (Україна), Циганова В.В., Бухарина С.Н., Ярочкіна В.Й, Одінцова А.Й., Шаваєва А.Г., Дороніна О.І., Нежданова І.Ю. (Росія), К. Богана, М. Інгліш, Д. Прескота, С. Міллера (Великобританія). Корисними можуть бути матеріали викладені в роботах вітчизняних науковців Панченко О.А. та Банчука М.В., Єщенко П.С. та Арсеєнко А.Г., Прибутько П.С. та Лук'янця І.Б., Остроухова В.В. Роботи зазначених авторів є цікаві не лише своїм змістом, головне це точки зору, міркування, позиції авторів, які вони обґрунтовують і які дають підґрунтя для творчого розуміння проблем, що виникли в інформаційному просторі вітчизняного підприємництва та вироблення підходів до їх подолання, побудови адекватних систем інформаційної безпеки.

Матеріали, використані у даному виданні містять позицію автора щодо забезпечення інформаційної безпеки в діяльності суб'єктів підприємництва. Маючи достатній досвід практичної роботи у сфері безпеки бізнесу та значні наукові напрацювання по дослідженню її проблем, автор подає своє бачення інформаційної безпеки суб'єктів підприємництва як такий стан їх інформаційної роботи за якого забезпечується надійний захист інформаційного ресурсу суб'єктів, ефективне інформаційне супроводження їх діяльності та результативна протидія інформаційно-психологічному впливу на них. Саме таке триєдине бачення змісту інформаційної безпеки, з погляду автора, забезпечує грамотний підхід до її організації в діяльності суб'єктів підприємництва, ефективне їх функціонування у сучасному інформаційному середовищі.

1. Сучасне інформаційне середовище підприємницької діяльності

1.1.Інформаційний розвиток і його сучасні особливості

На сьогодні уже ні для кого не є новиною думки та твердження про домінуючу роль інформації у розвитку суспільства. Інформаційний розвиток, пов'язаний із розвитком знань та інтелектуалізацією суспільства, обумовлює нові підходи у взаємовідносинах різних суб'єктів від безпосередньо громадян і до міжнародних відносин. Водночас необхідно звернути увагу на особливості інформаційної складової саме в сьогоднішніх умовах. Справа у тому, що інформаційна складова була завжди присутня в діяльності людства, будь-який вид громадського, економічного, технічного розвитку в тій чи іншій мірі був пов'язаний із інформаційним забезпеченням. Досягнення практично у всіх сферах життєдіяльності базувались на інтелектуальних здобутках, які перш за все характеризувались інформаційно. Більш того, наукові відкриття, передбачення, гіпотези з'являлись задовго до їх матеріального втілення, будучи основою для прогресу. Чому ж саме сьогодні мова іде про інформаційне суспільство, домінуючу роль інформації у його розвитку, основу удосконалення будь-яких політичних, технічних, економічних процесів?

Пояснюється це насамперед формуванням на сучасному етапі розвитку суспільства декількох факторів:

- значним чином збільшились обсяги інформації. Будь-яка діяльність, сфера, взаємовідносини характеризуються не просто великими обсягами інформації, а такими, що у звичайному режимі її сприйняття опанувати неможливо. Так, за останні 35 років у світі вироблено більше інформації, ніж за 5 тис. років до цього. Підраховано, що один примірник газети «Нью-Йорк Таймс» містить інформації більше, ніж її міг отримати мешканець Англії за все життя [1]. Подвоєння знань з 1900 р. здійснювалось кожні 50 років, з 1950 р.

подвоєння проходило вже кожні 10 років, з 1970 р. — кожні 5 років, а з 1990 р. — щорічно [2]. Якщо обсяги інформації будуть зростати такими темпами, то кількість знань для людини збільшиться в мільйони разів, виникне суттєвий розрив між обсягами інформації і спроможністю не тільки її засвоїти, а навіть зрозуміти. Більш того, інформаційні характеристики існують як об'єктивно, так і природньо чи штучно викривленими, що значно доповнює обсяги інформації та вимагає обов'язкової її обробки;

- в останні роки збільшились темпи зміни інформаційних характеристик. На відміну від минулих років повне оновлення інформації здійснюється один раз в 7 років. Така ситуація обумовлює необхідність швидкого впровадження в практику суспільної діяльності та використання інтелектуальних досягнень. В свою чергу швидкий обіг інформації вимагає постійного пошуку необхідних відомостей, що робить інформаційну роботу завжди актуальною та такою, що є невід'ємною складовою будь-якої діяльності в сучасних умовах;
- наявність великих обсягів не завжди об'єктивної інформації, швидка зміна інформаційних характеристик, а також можливість отримати певні переваги за рахунок інформації у суспільних взаємовідносинах зумовило необхідність формування суб'єктами зазначених відносин власного інформаційного ресурсу. Тобто, в даний час суспільний розвиток не може забезпечуватись лише фінансовими, матеріальними, кадровими ресурсами, а вимагає ще і відповідних інформаційних ресурсів;
- інформація на сьогодні існує не тільки як певна сума знань, а і які відповідний технологічний процес, який у поєднанні з іншими технологіями може суттєво впливати як на розвиток суспільства в цілому, так і на окремі його елементи. Зазначені технології здатні прискорювати або навпаки сповільнювати темпи суспільного розвитку, забезпечувати переваги розвитку окремих сфер, галузей чи концентрувати суспільні зусилля на певних напрямах. Більш того, інформаційні технології здатні формувати характер взаємовідносин у суспільстві, від мирного співіснування до суттєвих конфліктів. Здатність інформаційних технологій впливати на характер взаємовідносин у суспільстві

обумовила сьогодні появу нового виду зброї - інформаційної, застосування якої несе в собі не менш негативні насліди ніж від зброї в звичайному розумінні цього слова;

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

Однією з важливих особливостей сучасного інформаційного розвитку є те, що значне збільшення обсягів інформації та розширення можливостей її використання забезпечило становлення нового етапу суспільного розвитку, однією з характеристик якого є суттєве зростання інтелектуального потенціалу в структурі всіх його процесів. Це у свою чергу відбилось на здатності більш об'єктивно і повно сприймати ситуацію в різних видах діяльності, особливо в економіці та управлінні. Крім того, значне місце в суспільних та виробничих процесах посіли засоби штучного інтелекту, а сама діяльність отримала більш творчий підхід.

Зміни, що відбулись в останні роки в інформаційному середовищі суспільства призвели до нового ставлення до інформації. Остання стала необхідною складовою життєдіяльності , що сприяло формуванню т. з. інформаційного мислення, а з ним і нового виду відносин – інформаційних. Тобто, можна говорити, що зміни в інформаційному просторі призвели до формування інформаційного образу життя людини та інформатизації суспільства. Інформація стала зачіпати всі сторони суспільного життя. У суспільства, громадян, організацій, господарюючих суб'єктів з'явилась постійна потреба у інформації, її продуктах. У зв'язку з такою потребою з'явились відповідні види діяльності в основі яких є інформація, як то вироблення інформаційної продукції, забезпечення передачі інформації, формування інформаційних ресурсів, захист інформації, поширення інформації,

надання різного роду інформаційних послуг (збір інформації, її обробка, розробка інформаційних комп'ютерних програм, технологій та ін.). Таке активне зростання ролі інформації значним чином підвищило її цінність у взаємовідносинах та виробництві, а з цим і ціну її продуктів. Тобто, інформація, її продукти стали товаром, що зумовило появу інформаційного ринку та інформаційної індустрії, а властивість інформації впливати на індивідуальну чи колективну свідомість, утворила можливість здійснення т. з. інформаційних війн.

Під впливом масштабного розвитку інформації відбулися зміни трудової діяльності людини, господарської та інших видів діяльності юридичних суб'єктів, суспільних відносин. Серед основних характеристик таких змін можна назвати:

- відбулось скорочення часу у циклах управління та виробництва за рахунок інформатизації та автоматизації їх процесів;
- засобами виробництва стала комп'ютерна техніка, яка дозволила спростити процес вироблення продукції, а комп'ютерні технології зумовили мінімізацію участі людини в ньому і тим самим зменшили собівартість продукції;
- стала можливою технологічна і географічна інтеграція у всіх сферах життєдіяльності: економічній, суспільній, освітній, військовій та ін., наукові здобутки можуть швидко перетворюватись у реальні технології, засоби, поведінку, а можливості регіонів чи навіть країн оптимально поєднуватись для вирішення актуальних завдань життєдіяльності;
- підвищилась надійність технологій, заснованих на штучному інтелекті і запроваджених в управлінні та виробництві;
- відбулось становлення та розвиток єдиного інформаційного простору як певної сукупності інформаційних ресурсів та інформаційних технологій, які дозволяють використовувати їх у різних видах діяльності різними суб'єктами на основі регульованого доступу;

- розширився світогляд громадян та відбулось удосконалення їх інформаційної культури, з'явилась можливість застосування отриманих з інформаційних мереж знань для забезпечення їх життєдіяльності;
- відбувся перерозподіл видів трудової діяльності, значна її частина перебуває зараз в інтелектуальній сфері, що підвищує інтелектуальний потенціал суспільства і вимагає уточнення напрямів його подальшого розвитку;
- інформаційні зміни створили передумови для суттєвих перетворень в економіці, де вирішальну роль в економічній діяльності буде відігравати інформація і її технології.

Таким чином, можна говорити не лише про появу нового виду діяльності – інформаційної, а і про те, що вона є досить динамічною та з великим потенціалом розвитку, а і про те,що така діяльність має значні перспективи. Тобто, рівень інформаційного розвитку стає важливою характеристикою не лише сучасного суспільства, а і провідними показником конкурентоздатності суб'єктів підприємництва, якраз через нього може визначатись їх потужність на ринку.

Інформатизація суспільства активізувала проведення наукових досліджень у різних сферах його життєдіяльності, результати яких склали основу подальшого розвитку як окремих його суб'єктів, так всього суспільства. Наприклад, інформаційний вибух у засобах комунікацій, який відбувся у останні 15-20 років зумовив потребу у нових наукових розробках засобів зв'язку, насамперед мобільного. Компанії, які сьогодні здійснюють свою діяльність у даній сфері, значну частину свого бюджету витрачають саме на наукові дослідження (витрати виробника продукції з брендом «Nokia» на наукові дослідження складають 45% його прибутків [3]. В той же час, наукова складова діяльності суб'єктів господарювання відбилась на підходах до організації виробництва і життєдіяльності громадян. Останні все у більшому ступені вимагають наукового мислення, наукової культури, креативності. Новизна стає головним предметом управлінських процесів та модернізації суспільства.

Важливою характеристикою інформаційного розвитку є т. з. інформаційна експансія – активне поширення відповідними суб'єктами їх інформації, ідеології, поглядів, оцінок, інтерпретацій в межі конкретно обраного інформаційного простору. Інформаційна експансія може здійснюватись тривалий час забезпечуючи постійний вплив на суб'єктів інформаційного середовища або ж проводиться у вигляді інформаційних атак з метою пропаганди чи маніпулювання індивідуальною або громадською думкою. Прийнято вважати, що інформаційна експансія – прояв інформаційної політики країни у їх міжнародних відносинах. На сьогодні таку точку зору можна вже доповнювати тезою про застосування інформаційної експансії у конкурентній боротьбі суб'єктів підприємництва , в т.ч. і в межах однієї країни, внутрішнього ринку. Використовуючи різного роду засоби пропаганди, маніпулювання інформацію, інформаційно-психологічного впливу та концентруючи їх заходи на окремому ринку, регіоні певні суб'єкти здобувають необхідні їм переваги за рахунок переконання потенційних споживачів їх продукції у вигідності взаємовідносин з такими суб'єктами.

Окремо слід було б звернути увагу на те, що інформаційний розвиток, утворюючи сприятливі умови для суспільства та його суб'єктів, обумовив додатково різного роду проблеми, протиріччя, конфлікти, які здатні створювати значні небезпеки та загрози, причому як для окремих суб'єктів, так і для всього суспільства.

Як було помічено, стрімкий розвиток інформатизації суспільства, виробничого процесу зумовив ситуацію за якої інформаційні технології, при їх масовому поширенні, стали випереджувати можливості суб'єктів, окремих громадян по їх грамотному застосуванню, насамперед професійного опанування ними. При наявності окремої категорії фахівців знаної у сфері інформаційних технологій, переважна частина громадян залишається не повною мірою готовою до здійснення життєдіяльності в умовах навіть сьогоднішнього стану інформатизації, не говорячи уже про перспективи. Витрати на розробку та впровадження сучасних інформаційних технологій не

завжди швидко окуповуються, вигода не рідко обертається втратами. Інформаційні технології вступають у протиріччя з менталітетом громадян та професійними навичками сьогоднішніх фахівців, інколи, виходячи з під їх контролю та утворюючи негативні, а то і небезпечні ситуації. Існуючі тенденції інформаційного розвитку наполегливо вимагають інформаційної грамотності та інформаційної культури громадян, керівників усіх рівнів. Тобто, очевидною є необхідність інформаційної адаптації населення до рівня інформатизації суспільства.

Відсутність активної роботи у сфері такої адаптації формує страх та втому у працівників чи громадян, які вимушені застосовувати сучасні інформаційні технології, а в деяких випадках і залежність від них, або ж від фахівців, які професійно володіють такими технологіями.

Активне впровадження інформаційних технологій, заснованих на штучному інтелекті, в системі управління утворює небезпечну ситуацію залежності процесу управління від нього. При технічних, технологічних розладах чи збоях органи управління не здатні перебрати на себе керівництво певними процесами без зниження їх ефективності. Автоматизація управління без можливості дублювання його за певних умов «вручну» або створення високонадійних, багатоступеневих заходів її захисту завжди буде утворювати додаткові ризики захисту, а то і небезпеки, що, до речі, на сьогодні не рідко має місце.

Необхідність високонадійних інформаційних технологій обумовлюється ще і тим, що інформаційний розвиток сприяв формуванню технологій руйнування, штучних помилок та впливу як на системи управління та виробництва, так і на індивідуальну та суспільну свідомість. Такі технології несуть у собі пряму загрозу життєдіяльності суб’єктів чи суспільства.

Гострота взаємовідносин суб’єктів підприємництва зумовлює їх до використання у своїй діяльності не лише інформаційних технологій т. з. мирного співіснування, а і технологій інформаційної конкуренції, інформаційного суперництва та інформаційного протиборства, аж до

інформаційної війни. У зв'язку з такими можливостями інформації виникає необхідність звернути увагу на проблеми, які обумовлює інформаційний розвиток та сучасний стан інформатизації суспільства. Проблемний характер інформаційного розвитку проявляється насамперед у формуванні через нього різного роду досить суттєвих небезпек і загроз. Тут слід говорити не лише про створення інформаційних технологій впливу та комп'ютерних програм для проникнення і руйнування електронної інформації, а і про специфічне використання інформаційних продуктів та специфічну поведінку в інформаційному просторі. Принципи ринкової ідеології згідно з якими в конкуренції перемагає сильніший, зумовили конкуренцію інформаційних можливостей окремих суб'єктів для забезпечення монополізації інформаційної сфери. Поєднання ж вказаних можливостей з можливостями фінансовими формує підґрунтя для економічного зростання певних суб'єктів. Тому заволодіння найбільш впливовими інформаційними каналами та суб'єктами інформаційної інфраструктури є одним із головних завдань у інформаційних відносинах на будь-якому ринку. Саме інформаційні і фінансові можливості роблять сильнішими суб'єктів ринку. У погоні за посилення таких можливостей у інформаційних відносинах активно використовується дискредетація, дезінформація, компрометація, промислове шпигунство, різного роду ідеологічні та інформаційні диверсії. Рівень інформаційного розвитку дає можливості створювати інформаційні продукти, які діють, як то кажуть, без варіантів, поповнюючи інформаційний простір далекими від об'єктивності матеріалами. У таких умовах досить складно орієнтуватись та приймати об'єктивні рішення. Інколи певні суб'єкти навіть не помічають, що діють в ситуації далекій від об'єктивної реальності. Тому виникає проблема отримання саме об'єктивної інформації. Складність даної проблеми обумовлюється як наявністю великих обсягів інформації, якою наповнене інформаційне середовище, так і присутністю в ньому інформаційних продуктів спеціально призначених для викривлення об'єктивної інформації, введення споживачів

таких продуктів в оману. Тобто, у суб'єктів ринку чи інших осіб завжди існує можливість отримати недостовірну інформацію.

Поєднання фінансових і інформаційних можливостей здійснюється шляхом викупу або створення об'єктів інформаційної інфраструктури, насамперед засобів масової інформації. Заволодіння зазначеними об'єктами та територіальне і недійне їх розширення веде до монополізації окремих сегментів інформаційної сфери. У свою чергу, така монополізація утворює парадоксальну ситуацію, а саме - стримання темпів інформаційного розвитку. Інформаційні технології створивши умови для економічного розвитку, стають об'єктом посягань на них: викрадення, руйнування, компрометації та ін.. Чим вищий рівень володіння інформаційними технологіями у діяльності певних суб'єктів, тим активніше і наполегливіше стають спроби проникнення до них. Утворюється така собі війна інформаційних технологій. Як вказують науковці Державного університету інформаційно-комунікаційних технологій під керівництвом професора Остроухова В.В., в системі ринкових відносин отримало поширення використання методів і технологій інформаційної боротьби [2]. Вигоду у такій боротьбі отримують якраз ті суб'єкти, які монополізували інформаційну сферу і забезпечили контроль над нею. Деякі з фахівців, визначаючи роль контролю інформаційної сфери, вказують, що суттю війни інформаційних технологій є контроль над інформаційним полем [4].

Поряд з специфікою використання інформаційних продуктів та інформаційних технологій можна бачити і специфічну поведінку окремих суб'єктів в інформаційному просторі. Така поведінка обумовлюється насамперед тим, що окремі суб'єкти, в т. ч. і суб'єкти підприємництва, не рідко виступають учасниками інформаційного ринку, тобто виробляють, поширюють та використовують інформацію. За певних, вигідних для них, умов такі суб'єкти виступають третьою стороною у інформаційних відносинах здійснюючи інтерпретацію чи структурування інформації чи переводячи її з одного виду у інший. При необхідності такі суб'єкти створюють тимчасове чи постійне інформаційне лоббі, таких собі агентів впливу в певних комерційних,

громадських, політичних чи владних структурах. Будь-яка інформація може бути структурована та інтерпретована у необхідній для таких суб'єктів формі і через наявне лоббі подана в інформаційний простір чи до певних осіб та організацій. Крім того, тут можуть вироблятись відповідні інформаційні моделі поведінки як самих суб'єктів так і певних осіб, організацій та реакції інформаційного середовища. Така активізація інформаційної роботи спрямовується на створення сприятливих умов для діяльності та розвитку суб'єктів, що її проводять. Як правило, засобами, що забезпечують таку поведінку суб'єктів виступають засоби комунікації, різного роду перемовини, суспільна думка, результати наукових досліджень, заходи розвідки і контррозвідки та ін., що у сукупності утворюють мережу інформаційного впливу. За таких умов формується єдиний варіант поведінки, рішення, дій, який приймається, схвалюється, підтримується відповідним органом, громадою, особою і який саме і хоче отримати суб'єкт.

Звертає на себе увагу і те, що інформаційний розвиток не лише зумовив значне зростання обсягів інформації, швидкості її зміни та прибрав кордони її поширення, а і суттєво поновив інструменти застосування інформації, насамперед інформаційні технології. Характерною рисою сьогоднішніх інформаційних технологій є проникнення їх практично до всіх сторін життєдіяльності суспільства. Інформаційні технології стали застосовуватись у взаємозв'язку з технологіями та методиками інших сфер: економічної, соціально-психологічної, правової та ін. Від цього вплив інформаційного розвитку стає ще більш значним для суспільства та взаємовідносин суб'єктів. У зазначених взаємовідносинах та діяльності суб'єктів інформаційні технології можуть застосовуватись як одноосібно, так і у певній сукупності (Рис. 1.1.). Головне, що за сучасних умов необхідність їх застосування є безумовною, діяльність у будь-якій сфері поза такими технологіями немає перспектив. Звідси, опанування такими технологіями виступає обов'язковою умовою життєдіяльності та її розвитку. Особливо це характерно для ринкових умов, де діяльність суб'єктів підприємництва здійснюється під впливом конкуренції. А

конкурентні переваги якраз і базуються на сучасних та перспективних технологіях.

Рис.1.1. Інформаційні технології, що застосовуються в підприємницькій діяльності.

Як бачимо, сучасні особливості інформаційного розвитку обумовлюють потребу у т. з. інформаційній адаптації всіх суб'єктів підприємництва. В той же час, як випливає із вищевикладених характеристик сучасного інформаційного розвитку, адаптація має передбачати обов'язкове виконання наступних завдань:

- постійний пошук необхідної інформації і формування власного інформаційного ресурсу
- врахування неоднозначної структури та якості інформації, що перебуває в інформаційному середовищі, готовність до її постійного аналізу
- використання сучасних інформаційних технологій та досягнення інформаційного розвитку у виробничому процесі

- здатність ефективно захищати свій інформаційний ресурс, готовність до протидії інформаційному впливу та підтримання на необхідному рівні свого іміджу
- забезпечення інформаційного впливу на ринок з метою формування позитивних перспектив свого розвитку
- оволодіння методами здійснення інформаційного протиборства та інформаційної війни, забезпечення виживання в умовах їх проведення
- збереження інформаційної інфраструктури в умовах проведення актів кібертероризму.

Виконання зазначених завдань не може носити епізодичний характер. Тобто, суб'єкти підприємництва, з метою забезпечення свого виживання на ринку мають виділити інформаційну роботу в окремий, самостійний напрямок їх діяльності, яка має виконуватись постійно і виступає обов'язковим видом забезпечення їх бізнесу. Такі вимоги сучасного стану інформаційного розвитку.

1.2. Інфраструктура інформаційного середовища

Інформаційне середовище існує у сукупності певних елементів, які формують його інфраструктуру. Разом з тим, інформаційна інфраструктура має свої особливості, обумовлені специфікою функціонування та призначення інформації. Загалом інформаційне середовище пов'язане з діяльністю, яка являє собою створення, передачу та споживання інформації і діями, що супроводжують та забезпечують ці процеси. Тобто, можна говорити, що інформаційне середовище являє собою певну сукупність суб'єктів, засобів (технологій), ресурсів та зв'язків, які забезпечують вищевказані види діяльності і які можна було б вважати як його інфраструктуру. В той же час, незважаючи на існування визначення даного поняття в правових документах держави, серед фахівців та науковців точиться певна полеміка щодо найбільш оптимального та грамотного його розуміння. Так Б. Кормич наполягає, на тому що інформаційна інфраструктура України має розумітися як сукупність технічних засобів і

технологій підприємств, установ і організацій, які реалізують інформаційні процеси, на які поширюється юрисденція держави [5]. Даючи характеристику такому визначенню можна говорити, що інформаційна інфраструктура обмежується сукупністю технічних засобів: технологій та суб'єктів, які, як можна думати, виробляють, споживають, поширюють інформацію. Таке обмеження, з точки зору автора, робить інформаційну інфраструктуру не повноцінною, оскільки з неї виключено як саму інформацію (ресурс) та і інші її види, які функціонують поза технічними засобами та технологіями.

Створення ефективної інформаційної інфраструктури як розробку і реалізацію телекомунікаційних систем і мереж інформаційного обміну, широкомасштабну комп'ютеризацію процесів обробки інформації у всіх сферах діяльності на базі передових інформаційних технологій, подають Панченко О.А. та Бончук М.В. [6]. Їх точка зору хоча і є прогресивною, але все ж таки не зачіпає всіх елементів, які мають утворювати інфраструктуру інформаційного середовища і більш тяжіє до його обмеженення електронною інформацією. Такий підхід можна виправдати областю діяльності авторів, пов'язану з забезпеченням інформаційної безпеки людини в умовах широкого застосування електронних засобів інформації і інформаційних технологій впливу.

Прагнення до більш змістовного визначення поняття «інформаційна інфраструктура» можна бачити у матеріалах О. Нестеренка. Так, інформаційна інфраструктура розуміється ним як сукупність електронних інформаційних ресурсів, автоматизованих інформаційних систем як засобів збору, виробництва, накопичення, обробки, збереження та розповсюдження інформації, засобів доставки електронних інформаційних ресурсів до користувачів і засобів інформаційного обміну (лінії та засоби зв'язку, мережі телекомунікацій), відповідних інституційних складових (обчислювальні центри, інформаційні агенції, оператори, провайдери тощо), системи забезпечення інформаційної інфраструктури, що включає засоби нормативно-правового, економічного забезпечення, стандарти, інструктивні матеріали та документацію; система підготовки кадрів, людини як основного фактору

впливу на інформаційний простір [7]. Можна бачити, що таке визначення є досить громіздким, в ньому губиться основна суть поняття і яке, не зважаючи на свою об'ємність, вимагає додаткових пояснень.

З погляду автора, найбільш цілісним та змістовним є визначення інформаційної інфраструктури подане в Стратегії розвитку інформаційного суспільства в Україні. Зокрема, під інформаційною інфраструктурою пропонується вважати сукупність різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікації і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування [8]. В той же час, під інформаційним ресурсом в документі подається систематизована інформація або знання, що мають цінність у певній предметній області і можуть бути використані людиною в своїй діяльності для досягнення певної мети. А враховуючи, що:

- інформаційною (автоматизованою) системою є організаційно-технічна система в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [9];
- телекомунікаційна мережа це комплекс технічних засобів телекомунікації та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводних, оптичних чи інших електромагнітних системах між кінцевим обладнанням;
- канал передачі даних - комплекс технічних і програмних засобів, що забезпечують передачу цифрової інформації різними середовищами [10];
- засоби комунікації - засоби, що застосовуються для передачі, оголошення, обміну інформації в усному, письмовому чи візуальному видах поміж різними суб'єктами [10], можна робити висновок про наповнення інформаційної інфраструктури переважно електронними засобами роботи з інформацією. Разом з тим, згідно Концепції Національної програми інформатизації, національну інфраструктуру інформатизації мають складати:

міжнародні та міжміські телекомунікаційні і комп'ютерні мережі; система інформаційно-аналітичних центрів різного рівня; інформаційні технології; система науково-дослідних установ з проблем інформатизації; виробництво та обслуговування технічних засобів інформатизації; система підготовки висококваліфікованих фахівців у сфері інформатизації [11]. Тобто, інформаційна інфраструктура поєднує як технічні засоби та технології, так і різного роду установи, організації, які забезпечують інформаційний процес. В той же час, незважаючи на завантаження інформаційної інфраструктури технічними засобами та технологіями, домінуючу роль в ній займають власне інформація (інформаційний ресурс) та суб'єкти, які її виробляють, зберігають, поширюють, використовують та іншим чином забезпечують інформаційні процеси. За таких підстав є необхідність подати інформаційну інфраструктуру певною сукупністю інформаційного ресурсу та зазначених суб'єктів, які функціонують в інформаційному середовищі. Тут треба зазначити, що інформаційні ресурси, як складова інформаційної інфраструктури складає інформація вільного доступу, а суб'єктами є юридичні і фізичні особи, що відповідно до законодавства здійснюють легальну діяльність у сфері вироблення, збереження, поширення та використання інформації. За таких умов інформаційними ресурсами, які формують інформаційну інфраструктуру можна вважати: продукцію засобів масової інформації, правові документи, реєстри, наукові роботи та видання, матеріали соціологічних та інших досліджень, повідомлення органів статистики, державних органів та установ, архівні документи, навчальну літературу, матеріали мережі Інтернет, продукцію інформаційного ринку, аналітичні документи (огляди, прогнози), енциклопедичні та довідникові матеріали, рекламні продукти, агітаційні та пропагандиські матеріали, виставкові експозиції, індивідуальні та колективні знання, матеріали технологічного характеру та інше.

Особливістю суб'єктної частини інформаційної інфраструктури є те, що процес інформатизації сформував у суспільстві особливу галузь діяльності – інформаційну індустрію. Останню подають як широкомасштабне виробництво

інформаційних товарів і послуг на базі інформаційних технологій. Виходячи з даного визначення, можна вважати, що певна частина інформаційної інфраструктури представлена суб'єктами саме інформаційної індустрії. Класифікуючи зазначених суб'єктів за особливостями їх діяльності не складно прийти до висновку, що сегмент інформаційної інфраструктури складають: суб'єкти, які виробляють технічні засоби телекомунікації та автоматизації; суб'єкти, що розробляють програмні засоби та інші інтелектуальні продукти, які забезпечують функціонування засобів телекомунікації та автоматизації різних процесів виробничої та суспільної діяльності; суб'єкти, які формують та зберігають різноманітні бази даних і забезпечують доступ до них; суб'єкти, що здійснюють інформаційне забезпечення та упровадження певних видів діяльності, надають інформаційні послуги; суб'єкти, які збирають, обробляють та коментують інформацію, виробляють та реалізують інформаційні продукти; суб'єкти, що забезпечують вивчення та дослідження проблем інформатизації, функціонування інформаційного середовища; суб'єкти, що забезпечують потреби суспільства у комунікаціях. В той же час, даний перелік буде наповненим без врахування суб'єктів, які задовольняють свої інформаційні потреби із середовища інформаційної індустрії. Важливість та необхідність їх залучення до складу суб'єктів, які складають інформаційну інфраструктуру обумовлюється тим, що вони є своєрідним носієм інформаційного ресурсу, накопиченого у процесі взаємовідносин з різними суб'єктами, власної діяльності та перебування в різних сегментах інформаційного середовища. Як раз через даних суб'єктів інформація стає засобом масового застосування праці.

Важливою функцією, яку виконують всі перераховані вище суб'єкти у суспільстві є формування соціально-інформаційних відносин, які поширюються на різні сфери діяльності: матеріальну, духовну, соціальну, правову, політичну і т.д. Таким чином, інформаційна інфраструктура стає необхідним атрибутом всіх сфер суспільної діяльності, без якого подальший розвиток суспільства практично неможливий. Також неможливим є розвиток і підприємництва, яке у переважній більшості його складових засновано на інформаційних продуктах та

інформаційних технологіях. Останні ж вимагають досконалої інформаційної інфраструктури і грамотного використання її можливостей.

Характеризуючи інформаційну інфраструктуру вітчизняного інформаційного середовища та її можливості можна заключити, що вона відповідає сучасному стану становлення ринкових відносин в Україні. Домінуючими у ній виступають засоби масової комунікації, насамперед масмедійні засоби: преса, телебачення, радіо, мережа Інтернет. Основною особливістю вітчизняних масмедіа, як суб'єктів інформаційної інфраструктури, є концентрація їх під владою окремих осіб, а також держави, створення потужних об'єднань, т. з. медіа-холдингів. Останні, подаючи в інформаційний простір, як правило, структуровану інформацію, забезпечують значний вплив на формування громадської думки. На думку фахівців вітчизняні масмедіа здебільшого політично орієнтовані їх власниками, тому їх інформація не завжди може бути повністю об'єктивною, а за певних умов спрямовується на маніпулювання громадською думкою [12]. Враховуючи зазначене, рівень довіри населення до вітчизняних засобів масової інформації виглядає наступним чином: в цілому довіряють – 56% громадян, 38,6% - не довіряють [13]. Можна говорити, що ця група суб'єктів інформаційної інфраструктури в Україні є достатньо авторитетною. Характеризуючи структуру засобів масової інформації і беручи до уваги ефективність використання каналів поширення інформації, можна бачити, що перше місце займає телебачення (69,4%), друге – Інтернет (15,5%), третє – преса (7,9%), а четверте – радіо (7,2%) [14]. Тобто, серед засобів масової інформації, телевізійних медіа практично повністю домінують, інформація подана через телебачення є найбільш сприйнятною для аудиторії і впливовою на неї.

Інші категорії суб'єктів засобів масової комунікації (рекламні агентства, організації, які надають PR-послуги та послуги з пропаганди, агітації) хоча і займають певне місце в інформаційній інфраструктурі, але виступають лише як виробники специфічної інформаційної продукції.

Монополізація ринку масмедіа та значні можливості засобів масової комунікації обумовили ситуацію за якої окремі суб'єкти – власники зазначених засобів, отримали у вітчизняному інформаційному просторі т. з. інформаційну владу. Остання дозволила їм шляхом отримання, селекції, відповідного компанування та тлумачення інформації, поширювати її в інформаційному середовищі з метою впливу на формування суспільної думки, спонукання окремих груп громадян чи більшості з них до дій у заданому напрямку. В той же час, інформацію, яка подається таким чином в інформаційне середовище складно використовувати для забезпечення підприємницької діяльності і формування суб'єктами підприємництва їх інформаційного ресурсу без суттєвої її обробки. Таким чином, можна говорити, що вітчизняна інформаційна інфраструктура досить багата, наповнена різними видами інформаційних ресурсів, зв'язками, каналами поширення інформаційних продуктів, суб'єктами інформаційної діяльності. Разом з тим, у середовищі, яке вона утворює, досить складно і навіть небезпечно будувати інформаційні відносини, що викликає необхідність обережної поведінки суб'єктів підприємництва та високо професійної роботи з інформацією і обов'язкового вжиття заходів безпеки.

1.3. Інформаційна економіка та її наслідки

Вітчизняні науковці Панченко О.А. та Банчук М.В. вказують, що «… у суспільствах, які ідуть по шляху інформатизації… ситуація не просто змінюється, вона змінюється з швидкістю, яка постійно нарощується. Трудовитрати зазнають перерозподілу на користь сфери інформаційних послуг. З врахуванням наведеного, можна стверджувати, що сама політична економія, теорія управління і регулювання господарської діяльності підлягає серйозному перегляду. … Якщо сучасне виробництво управляється грошима, а визначальними факторами є попит і пропозиція, то інформаційна економіка або інформаційна політекономія можуть обґрунтовувати тезис про те, що

вирішальним фактором управління і регулювання економічної діяльності стає інформація.» [6, с.25]. Пояснюючи свою позицію науковці вказують, що вона обґрунтовується наступними чинниками:

- обмеженістю природних ресурсів;
- економічною катастрофою, що насувається;
- демографічним дисбалансом;
- зростаючою нерівномірністю в економічному, індустріальному і інформаційному розвитку різних країн та посилюючою їх нестабільністю;
- прискореним розвитком наукоємних технологій і інформаційних процесів у невеликій кількості найбільш розвинутих країн.

За таких умов, уникнути негативних явищ та їх наслідків в економіці можна лише шляхом масового впровадження нових методів управління нею, розумного регулювання збалансованого ринкового господарства і глобального моделювання та постійного моніторингу економічних та соціально-економічних процесів. Всього цього, з погляду науковців, можна досягнути через глобальну інформатизацію.

Не зовсім поділяючи таку думку слід було б зауважити, що з т. з. історії розвитку глобальних процесів, глобальна інформатизація можлива щодо окремих країн чи деяких регіонів. В той же час, з поширенням глобальної інформатизації можна очікувати і глобальної прірви поміж розвинутими країнами та країнами що розвиваються практично для всіх континентів. Така прірва буде обумовлювати постійне існування економічних, екологічних, соціальних та інших загроз для зазначених країн і тим самим підтримувати нестабільність у світі. Разом з тим, з думкою про формування ринку інформаційних технологій, продуктів, послуг, в т. ч. і на глобальному рівні можна погодитись. Тобто, в економічній сфері формується певний сегмент економічних відносин, заснований на виробленні та реалізації суто інформаційної продукції. На ринку з’являється новий вид товару – інформація у різних її формах. Тут слід звернути увагу на іншу думку. Як зауважують Єщенко П.С. та Арсеєнко А.Г. інформаційна економіка – це економіка,

заснована на інформації і знаннях, в якій переважна частина внутрішнього валового продукту забезпечується шляхом виробництва, обробки, збереження і поширення інформації і знань [14, с.250]. Мова іде уже не про інформацію як товар, а про інформаційне забезпечення вироблення внутрішнього валового продукту. Суттю ж інформаційного забезпечення є знання, при чому на знання взагалі, а нові знання, відмінні від минулих, існуючих чи тих, що використовуються іншими суб'єктами. Єщенко П.С. і Арсеєнко А.Г. називають їх «живими знаннями», знаннями, що з'явились з досвіду і які формують культуру повсякденності: розсудливість, здатність до координації, знаходження спільної мови. У сучасній інформаційній економіці такі знання утворюють нову продукцію у вигляді грошей. Останні ж утворюються, як вказують автори з фінансових та інших послуг, страхування, торгівлі ф'ючерсами, шоу-бізнесу і т. і.. В ринкових умовах така ситуація призвела до виникнення приватної власності на знання і інформацію, зумовила значне зростання прибутків суб'єктів, які володіють такою власністю. Зростання прибутків базується з одного боку на зменшенні витрат на їх формування (на відміну від матеріального виробництва), а з іншого на зростанні попиту на продукти, отримані в результаті застосування нових знань та інформаційних технологій. Практично необмежені можливості отримання надвисоких прибутків, які забезпечують нові інформаційні технології зумовлюють викривлення економічного розвитку, спрямовуючи його у бік нематеріальної сфери, втрачаються види діяльності, які забезпечують економічну могутність країн. Поширеною стає діяльність по наданню різного роду послуг, маркетингових досліджень.

В той же час, не слід думати, що інформаційна економіка цілком спрямовує свій розвиток у нематеріальну сферу. Як вважають Панченко О.А. та Банчук М.В. інформаційна економіка поступово стає фундаментом економічної основи всіх видів економічної діяльності, від фінансово-кредитної до промислового і сільськогосподарського виробництва, т. я. вона виконує досить важливу функцію інформаційного забезпечення господарської

діяльності і управління нею [6]. Тут маємо цілком погодитись з висновком науковців, оскільки сучасна господарська діяльність забезпечує свої переваги та розвиток якраз із інформаційних технологій та знань.

Таким чином, можна говорити про те, що інформаційний розвиток зумовив виникнення та становлення інформаційного суспільства в якому сформувався певний сегмент економічної діяльності, який отримав назву інформаційна економіка. Остання ж спеціалізується у таких напрямках як вироблення та реалізація інформаційної продукції та технологій, виробництва нової продукції у окремих видах економічної діяльності – як то фінанси, маркетинг, менеджмент, а також виконання інформаційного забезпечення різних видів діяльності економічних суб'єктів.

Беручи до уваги те, що переважна частина інформації існує і здійснює своє функціонування в електронному вигляді, у економічних взаємовідносинах з'явилось специфічне визначення, так звана електронна економіка. Її поняття розкривається у Стратегії розвитку інформаційного суспільства в Україні. Зокрема, під електронною економікою розуміється форма економічних відносин у сфері виробництва, розподілу, обміну, споживання товарів, робіт і послуг, наданих у електронному вигляді за допомогою інформаційно-комунікаційних технологій [8]. Очевидно, що така форма економічних відносин у бізнесі отримала назву електронної комерції. Остання набула значного поширення, аж до створення електронного ринку.

Говорячи про державницькі засади, Стратегія розвитку інформаційного суспільства в Україні одним з головних її напрямків розглядає саме розвиток електронної економіки. Тут держава передбачає стимулювання розвитку електронної економічної діяльності або інших її видів за допомогою інформаційно-комунікаційних технологій. Відповідно до Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» важливим завданням формування електронної економіки є розвиток електронного бізнесу [15]. Зокрема передбачається розвиток і застосування підприємствами технологій та інструментів електронної торгівлі, впровадження

систем дистанційного обслуговування, забезпечення інформаційної безпеки. Разом з тим, слід звернути увагу на те, що стрімкий інформаційний розвиток та отримання і застосування нових знань в економіці призвів до надмірних обсягів специфічних знань, пов'язаних насамперед з технологіями отримання надприбутків. Некероване застосування таких технологій формує загрозу неадекватно інтенсивного використання певних ресурсів: природних, енергетичних, людських. Уже зараз кожен із таких ресурсів знаходиться майже у кризовому стані, подальша інтенсифікація їх експлуатації призведе до незворотніх негативних явищ. Більш того, за умов коли сучасні та перспективні технології будуть обмеженні наявним ресурсним потенціалом, вони можуть спрямовувати свої зусилля на застосування силового варіанту в економічному розвитку, як нового світового порядку господарювання. Такому розвитку ситуації може сприяти цілеспрямований вплив інформаційних технологій на духовну сферу членів суспільства, формуючи в них відповідну поведінку. Остання ж, за відповідних умов, може спрямовуватись на необхідність боротьби за своє виживання, в т. ч. і за рахунок можливостей членів суспільства або ж народів інших країн під різного роду гаслами та закликами. Аналізуючи останні події у світі та нашій країні можна бачити, що сучасні інформаційні технології спроможні зумовити до боротьби не лише окремих громадян, а і цілі регіони чи країни.

Тобто, в економіці існує небезпека некерованого розвитку інформаційних технологій та надмірного накопичення знань і неадекватного існуючим умовам їх застосування. Відтак, в основу інформаційного розвитку і розвитку інформаційної економіки має бути покладено забезпечення інформаційної безпеки. Остання ж має бути орієнтована як на адекватне використання інформації для забезпечення економічного зростання суспільств, так і на адекватне регулювання інформаційного розвитку, особливо в тих напрямках, які можуть формувати загрозу суспільству (енергетичному, екологічному, духовному, культурному).

В той же час, говорячи про інформаційну економіку слід звернути увагу на її динаміку і темпи розвитку. Успіху досягає той, хто не лише отримав високі результати, а і постійно дбає про удосконалення засобів та технологій досягнення таких результатів. Так, американський дослідник Джон Перрі Барлоу, висловлюючи свою позицію щодо інформаційної економіки, зазначає, що бізнес уже не може розвиватись у відповідності до відомих постулатів класичного капіталістичного виробництва. Наші знання про економіку сьогодні є зовсім іншими в порівнянні з тими, що були в епоху К. Маркса. Тому сьогоднішнє підприємництво має зробити висновок про необхідність обов'язкового зв'язку його діяльності з сучасними знаннями і не лише в економіці, а і в усіх сферах суспільної життєдіяльності. Досягти успіху можна тільки за умов глибокого розуміння суті сьогодення і перспектив майбутнього [16]. Тут маємо зробити два висновки: 1. Об'єктивне розуміння суті сьогодення і перспектив майбутнього не може бути досягнуто за рахунок лише професійних знань, виникає необхідність більш широкого пізнання соціальних, економічних, політичних процесів, аналізу їх наслідків, які відбуваються у суспільстві і світі. 2. Сучасну економіку стабілізувати в принципі неможливо, вона повинна постійно трансформуватись у залежності від того наскільки глибокими стають наші знання.

Беручи за основу зазначені висновки, маємо акцентувати наступне: суттю матеріального виробництва є отримання продукції, яка потрапляючи на ринок приносить виробнику певні вигоди, виражені в коштах, долі ринку, іміджу і т. і.. В той же час ресурси (сировина, енергія, праця) витрачені на вироблення продукції втрачаються на завжди. Тобто, кожного разу виробник має розпочинати все спочатку, доводячи тим самим ресурсну базу до знищення. Більш того, сама продукція, у більшості її видів, також не використовується для вироблення нового товару, виробник, подавши її на ринок, втрачає її назавжди. Інформаційна ж економіка, як вказує Д.П. Барлоу, базується на ідеї, яка має т. з. інформаційну енергію і потенційно може бути перетворена у вартість. З передачею ідеї її власник не втрачає її назавжди, а лише передає відповідне

право на неї. Враховуючи, що здатність до пізнання є безкінечною, інформація і процес формування на її основі ідей є також безкінечним. Тобто, в інформації, на відміну від матеріальної продукції, закладена енергія саморозвитку. Ідея ж в силу своєї новизни, виступає стимулом удосконалення і розвитку як самого підприємництва, так і життєдіяльності суспільства взагалі. В той же час, рушійною силою виступає не сама ідея, а саме її відмінність, новизна: відмінність від минулого, від іншого сучасного, у будь-якому випадку це щось інше, можна сказати нове. Тобто, головним в інформаційній економіці виступає відмінність, нова ідея, яка несе в собі потенційну цінність незалежно від того стане вона товаром чи використається для створення іншого блага. Іншими словами нова вартість утворюється із відмінності інформаційного потенціалу суб'єктів підприємництва.

Разом з тим, розуміння відмінності може бути лише за умов відкритості інформації. Ідея, яка нікому не відома не може нести в собі переваг або такі переваги будуть тимчасові. У невідомості досить складно орієнтуватись, а тим більше досягати успіху. Рівень переваг буде залежати в т. ч. наскільки той чи інший суб'єкт підприємництва інформаційно потужний. У цьому випадку потужним буде той, хто поширює свої ідеї, започатковані на високому інтелектуальному рівні і реалізує їх у своїй діяльності. Відкритість же таких ідей не може позбавити їх власника переваг, оскільки справа не стільки в сутності ідей, скільки у творчому підході до їх застосування та можливості отримати вигоду від такого підходу. Ідея чи нові знання з яких неможливо отримати вигоду нікому не потрібні, незалежно від того відомі вони чи зберігались у таємниці. Більш того, ідеї, нові знання формуються без гарантії на успіх, але з надією на нього. Нові знання отримує багато хто, але результати від їх використання є різними, оскільки у всіх такі знання отримали різне творче удосконалення. У такому випадку суб'єкту підприємництва для того щоб використати ідею чи знання необхідно буде привести у відповідність свої творчі можливості, тобто створити нову ідею (нові знання). Необхідність розкривати інформацію з метою виявлення її відмінностей виступає важливою

умовою функціонування інформаційної економіки, а швидкість зміни таких відмінностей зумовлює прогрес в т. ч. і у підприємницькій діяльності. Такий висновок може підтверджується ще і тим, що підприємці прагнучи наростити свій творчий потенціал вимушені будуть об'єднувати свої зусилля та інтелектуальні можливості і таким чином забезпечувати високу їх стійкість на ринку. Створення такого спільного потенціалу неможливе без дотримання принципу відкритості інформації, наданої кожним із суб'єктів, що прагнуть до об'єднання.

Однією із властивостей інформаційної економіки є зростаюча її віртуалізація. Останнє дає можливість моделювати різні ринкові ситуації, аналізувати потреби ринку і швидко його наповнювати необхідною продукцією, причому продукція може мати різні характеристики, аж до індивідуальних замовлень. Тобто, в інформаційній економіці ринок відходить від продукції масового споживання і починає орієнтуватись на конкретного споживача. Можна говорити, що тут присутній постійний реінжиніринг.

Інформація виробничих процесів зумовила перехід від колективної до індивідуальної праці, створила таку собі автономізацію роботи, її незалежність і самостійність у виробничих процесах, що підвищило безпеку самого виробництва і в той же час посилило відповідальність кожного працівника за рівень його знань і результати роботи. Сьогоднішні фахівці мають бути здатні працювати автономно, самостійно приймати відповідні рішення, для цього бути професійно високо компетентними, грамотно оцінювати виробничу і суспільну ситуацію та готовими брати на себе відповідальність за прийняті рішення. Такі якості фахівців стають основополагаючими у їх здатності виконувати посадові обов'язки на виробництві. Враховуючи ж дуже високу динаміку зміни інформації, фахівці мають постійно забезпечувати свій саморозвиток та самовдосконалення [17].

Необхідно звернути увагу ще на одну властивість інформаційної економіки. Для останньої характерним є те, що розрахунки суб'єктів здійснюються не безпосередньо грошима, а інформацією про них. Значна доля

грошей, що знаходяться в обігу не що інше, як інформація про них. Крім того, у більшості своїй така інформація крім самих грошей більш нічим не забезпечена. Доля таких розрахунків (руху грошей) постійно зростає. Національний банк України послідовно вводить обмеження на розрахунки готівкою, зумовлюючи громадян і юридичних осіб до використання сучасних інформаційних технологій. Перспективою такої властивості інформаційної економіки очевидно буде значне зменшення готівкових розрахунків навіть у побуті.

Разом з тим, окремі фахівці занепокоєні таким стрімким розвитком інформатизації економічних відносин, особливо з урахуванням перевиробництва інформації. Вони порівнюють таку ситуацію з перевиробництвом товарів, що призводить до відповідної кризи в економіці. Тут вбачається дві таких загрози: 1. Складність, а то і неможливість взагалі забезпечувати ефективне управління економічним розвитком чи діяльністю окремих суб'єктів господарювання. Роботизація виробництва і управління ним при нездатності людини активно і своєчасно втручатись у виробничі процеси може призвести до серйозних техногенних негараздів. 2. Конкуренція суб'єктів інформаційних відносин все більшим чином виділяє мотивовану інформацію. Конкретні характеристики продукції підмінюються комп'ютерними відгуками про її використання. Чим більше має враження така інформація, тим більш привабливою стає продукція [18]. Тобто, інформаційна економіка все більше стає економікою вражень, як раз через те, що інформаційні технології у економічній сфері знайшли нове застосування інформації. Ми вже сьогодні можемо спостерігати як окремі ринки запровадили низькоякісні товари щодо яких активно поширюється інформація про бренд виробника, престиж використання його продукції, сервісне (не безоплатне) обслуговування, супутні послуги. Така характеристика інформаційної економіки вказує на те, що поряд з позитивними її якостями існують і певні негативні, які можуть формувати досить специфічні ризики та загрози у економічній сфері.

1.4. Інформаційні взаємовідносини суб'єктів підприємництва

Здійснюючи свою діяльність суб'єкти господарювання, різні організації, громадяни безумовно перебувають у певних взаємовідносинах один з одним, в т. ч. і в інформаційній сфері. У останньому випадку їх відносини можна назвати інформаційними. З практики застосування термінів, слів та словосполучень у юриспруденції під інформаційними відносинами розуміють суспільні відносини, що виникають у всіх сферах життя і діяльності суспільства й держави при одержанні, використанні, поширенні і зберіганні інформації [19]. Вільна енциклопедія «Вікіпедія» подає майже ідентичне тлумачення даного поняття: інформаційні відносини — суспільні відносини, які виникають при збиранні, одержанні, зберіганні, використанні, поширенні та захисту (охороні) інформації [10].

Виходячи з основного призначення Закону України «Про інформацію» (закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, захисту інформації). Можна говорити, що інформаційні відносини виникають там де їх предметом є будь-які дії з інформацією [20]. Причому, не має значення вид інформації чи її стан (електронна, документована інформація, знання і т. д.). Відповідно до зазначеного закону основними принципами інформаційних відносин мають бути: гарантованість права на інформацію, відкритість, доступність інформації, свобода обміну інформацією, достовірність і повнота інформації, свобода вираження поглядів і переконань, правомірність одержання, використання, поширення, зберігання та захисту інформації, захищеність особи від втручання в її особисте сімейне життя. Суб'єктами інформаційних відносин є: фізичні та юридичні особи, об'єднання громадян, суб'єкти владних повноважень. Об'єктом інформаційних відносин є інформація.

Враховуючи зміст поняття «інформаційних відносин» та їх суб'єктно-об'єктну сторону, можна говорити про об'єктивність виникнення таких відносин і поміж суб'єктами, що здійснюють підприємницьку діяльність. Тут

слід звернути увагу на те, що інформаційні відносини виникають не лише у зв'язку з інформаційною діяльністю як видом підприємництва, вони можуть виникати у будь-якій сфері діяльності. Згідно чинного законодавства, право на інформацію (вільне одержання, використання, поширення, зберігання, захист інформації, необхідної для реалізації законних інтересів) не обмежується видом діяльності в т. ч. і у сфері підприємництва. В той же час, реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб. Стосовно підприємницької діяльності важливим є неприпустимість порушення економічних та інших прав і інтересів суб'єктів підприємництва у процесі одержання, використання, поширення, зберігання, захисту інформації.

Такі особливості реалізації права на інформацію є важливими у випадках регулювання доступу до інформації суб'єктів підприємництва, яка має обмежений доступ, їх захисту при поширенні інформації, що шкодить їх діловій репутації, обмежує діяльність на ринку, а також протидії використанню інформаційних технологій для викривлення інформаційних характеристик суб'єктів в конкурентній боротьбі.

Говорячи про економічні права необхідно зазначити, що такі права передбачають: право здійснення будь-якої суспільної діяльності не забороненої законом, в т. ч. і в підприємництві, право вільно обирати вид і місце діяльності, її обсяги, бути незалежним у такій діяльності, право на захист своєї діяльності і власності, право вільного розпорядження результатами діяльності, інші права.

Як показує практика підприємницької діяльності реалізація зазначених прав здійснюється в т. ч. і через інформаційну сферу. Крім суто економічного змісту діяльності остання наповнена великою кількістю інформаційних характеристик. Тому вступаючи у економічні (виробничі, фінансові, комерційні) відносини суб'єкти підприємництва обов'язково торкаються таких характеристик. Більш того, інколи зазначені характеристики відіграють провідну роль у взаємовідносинах, оскільки розкривають економічний зміст,

природу, напрямки розвитку діяльності суб'єктів та їх взаємовідносин. Тому економічні взаємовідносини, в які вступають суб'єкти підприємництва одночасно передбачають і взаємовідносини інформаційного характеру. Зазвичай у таких взаємовідносинах мають місце:

- передача інформації від одного суб'єкта до іншого, оскільки взаємовідносини неможливі без взаємоінформування суб'єктами один одного про певні аспекти своєї діяльності;
- зберігання та захист інформації: у процесі взаємовідносин суб'єкти забезпечують захист своїх технологій, знань, інтелектуальних надбань;
- поширення інформації: з метою впливу на ринок суб'єкти розробляють рекламні, іміджеві заходи та технології подачі їх в інформаційний простір;
- використання інформації, що передбачає встановлення правил користування інформаційними продуктами, загалом інформацією. Основним тут виступає принцип «не зашкодити», тобто інформація яка використовується суб'єктами не повинна шкодити їх репутації і діяльності.

Підтримуючи взаємовідносини суб'єкти підприємництва стосовно інформації можуть виступати її джерелами, споживачами (користувачами), власниками (авторами). Основними умовами інформаційних взаємовідносин можуть виступати: умови доступу до інформації, умови конфіденційності, вимоги до об'єктивності інформації, умови її використання та поширення, умови відповідальності, контроль інформації та дій щодо неї.

Таким чином, інформація є одним із головних атрибутів діяльності не лише самих суб'єктів підприємництва, а і взаємовідносини поміж ними.

Разом з тим, така роль інформації обумовлює досить високу уразливість суб'єктів підприємництва. Останні, як суб'єкти інформаційних відносин, можуть зазнавати шкоди суто через порушення таких відносин: неправомірне використання чи поширення критичної (небезпечної) для них інформації; незкоординоване або неузгоджене використання технологій інформаційного впливу, або ж їх використання на шкоду одній із сторін. Причому шкода може

наступати як матеріального, так і морального (іміджевого) характеру. Більш того, подібні порушення в інформаційних взаємовідносинах згодом можуть призводити до їх руйнування, конкуренції, в т. ч. і недобросовісної, а то і протиборства в інформаційному просторі. Така ситуація є досить небезпечною для суб'єктів підприємництва принаймні двома факторами:

1. Функціонування інформації зачіпає значні маси суспільства і будь-які події у взаємовідносинах бізнес-партнерів, конкурентів чи взагалі підприємців можуть швидко ставати відомими широкому загалу. Механізми функціонування суб'єктів підприємництва в інформаційному просторі зачіпають саме головне для бізнесу – зв'язки, як у економічній, так і в політичній, владній сферах.

2. Враховуючи, що інформаційні відносини носять масовий характер всі події, які в них відбуваються обов'язково когось зачіпають, для когось стають цікавими, а для когось є предметом широкої дискусії та оцінки.

Наявність вказаних факторів і їх значна роль у інформаційних взаємовідносинах обумовлює необхідність досить обережної поведінки суб'єктів таких відносин, продуманого вибору партнерів, створення відповідних засобів інформаційного захисту та протидії, вироблення балансу прав на інформацію і її захист.

Інформаційні відносини у залежності від ролі, яку їх суб'єкти придають інформації, можуть проявлятись різними стосунками поміж ними. Останні можуть перебувати у площині певного порозуміння, ставати досить напруженими, антагоністичними чи навіть агресивними. Стосунки суб'єктів у сфері інформаційних відносин визначають якісний стан останніх і формують поведінку суб'єктів в інформаційному просторі.

Аналіз інформаційного середовищу, в якому здійснюють свою діяльність вітчизняні суб'єкти підприємництва, показав, що їх інформаційні відносини можуть набувати різного за якістю стану: інформаційного співробітництва чи інформаційної взаємодії, інформаційного суперництва, інформаційного протиборства або ж інформаційної війни [21, 22, 23].

Під інформаційним співробітництвом можна розуміти спільну роботу суб'єктів інформаційних відносин щодо збору, використання та поширення інформації в інтересах досягнення спільної мети.

Інформаційну взаємодію розуміють як обмін наявною інформацією чи інформаційними технологіями з метою задоволення інформаційних потреб кожного із суб'єктів інформаційних відносин.

Інформаційне суперництво – боротьба суб'єктів інформаційних відносин за кількісне і якісне отримання інформації, найбільш ефективне її використання та поширення у інформаційному просторі з метою впливу на ринок чи окремих суб'єктів.

Інформаційне протиборство – використання суб'єктами інформаційних відносин інформації, її продуктів та технологій з метою впливу один на одного задля досягнення інформаційної переваги.

Інформаційну війну можна розуміти як активні дії суб'єктів інформаційних відносин (конкурентів) в інформаційному просторі по використанню різноманітних технологій інформаційного впливу, спрямовані на дискредитацію окремих суб'єктів, їх діяльності чи продукції з метою створення їм негативного іміджу та отримання переваг на ринку. Фахівці вказують, що інформаційні війни включають у себе чотири компоненти: руйнування систем зв'язку конкурентів, перехоплення повідомлень, несанкціоноване проникнення до комп'ютерних мереж, вплив на суспільну думку через поширення дезінформації [6]. Погоджуючись з даною тезою слід додати: у інформаційних війнах головним об'єктом є імідж конкурента, тому основні зусилля механізмів інформаційної війни спрямовуються на формування в інформаційному середовищі негативного враження про нього та сприйняття його як поганого суб'єкта підприємництва. Зазвичай інформаційні технології впливу в інформаційних війнах доповнюються технологіями психологічного впливу на масову та індивідуальну свідомість. У даному випадку мова іде не про ринкову оцінку суб'єкта, а про формування щодо нього суспільної думки, а з нею і суспільної поведінки. Враховуючи, що інформація є основним механізмом

подачі в маси технологій психологічного впливу, інформаційні війни можна сприймати як активне та широкомасштабне використання інформаційних технологій з метою цілеспрямованого впливу на психічний стан і діяльність людей. Інформаційні війни можуть застосовувати акти інформаційного тероризму, причому останні здебільшого зачіпають психоінтелектуальну сферу суб'єктів, на яких спрямовуються такі акти. В результаті впливу таких актів у інформаційного оточення суб'єктів можуть формуватись протирічні уявлення, негативне обурення, помилкове розуміння, тобто дезінформація громадської думки чи думки певного колективу.

Інформаційні відносини виникають не обов'язково поміж суб'єктів, які мають якісь договірні чи інші стосунки. Вони можуть формуватись поміж різними суб'єктами, які використовують інформацію. Такі відносини є постійним атрибутом життєдіяльності будь-якого суб'єкта чи фізичної особи. У переважній більшості вони носять мирний характер. Разом з тим мирні відносини потенційно здатні до перетворення в напружені чи антагоністичні. Дисбаланс у інформаційні відносини можуть вносити протиріччя інтересів, що виникають від зміни умов діяльності або ж бути результатом різного роду провокацій. Існуюча можливість перетворення інформаційних відносин у напружені, антагоністичні чи агресивні (суперництво, протиборство, інформаційна війна) вимагає від суб'єктів підприємництва постійного контролю інформаційного середовища та інформаційної поведінки своїх партнерів, не говорячи уже про конкурентів. Крім того, суб'єкти інформаційних відносин мають постійно дбати про свій імідж, в обов'язковому порядку проводити заходи реклами, агітації та пропаганди, спростування негативної інформації про них.

2. Безпека бізнесу в Україні: історія та сучасність

Безпека бізнесу, як і багато інших питань, зумовлені переходом України до ринкових відносин, виявилася для неї не тільки новим явищем, але і одним з найнеобхідніших умов подальшого розвитку суспільно-економічних відносин. Молодий український бізнес вже з самого початку свого зародження став відчувати гостру потребу в захисті. Вітчизняне підприємництво опинилося в оточенні величезної кількості різноманітних загроз, здатних загубити його на самому початку розвитку. Значне зростання злочинності в країні і активний вплив злочинного світу, на початку 90-х років минулого століття, практично на всі складові життєдіяльності країни, відсутність необхідного правового регулювання підприємницької діяльності, несприйняття більшою частиною населення підприємництва як виду економічних взаємин, жорстка конкуренція, чиновницьке свавілля ставили бізнес в умови боротьби за виживання. Дуже швидке збагачення і не менш швидке розорення, часті бандитські розборки у підприємницькій сфері, вбивства підприємців стали дуже актуальними питаннями української дійсності і висунули проблему захисту бізнесу на одне з провідних місць в суспільно-економічних відносинах. У той же час, в 1992-1994 роках правоохоронна система незалежної України, з якої пішла значна кількість професіоналів, не могла забезпечити ефективний захист бізнесу і останній змушений був шукати шляхи забезпечення його безпеки власними силами.

Становлення і розвиток безпеки українського бізнесу здійснювалось у декілька етапів. Перший етап починається з 1992 року і досягає 1996-1997 років. Основною характеристикою даного етапу є специфічність і особлива жорстокість загроз, які на той час мали місце в підприємницькому середовищі. Це переважно були погрози фізичного характеру, пов'язані з замахами на вбивство, розбійними нападами, знищенням матеріальних об'єктів, рекетом. Якщо, приміром, у 1996 році підрозділами МВС України було припинено діяльність 953 організованих злочинних угруповань, у складі 5,3 тис. осіб, які вчинили понад 6 тис. злочинів, то вже в 1997 році таких угруповань виявлено

1072 у складі 9,4 тис . осіб, якими було скоєно 7,4 тис. злочинів. Крім того, цього року було зареєстровано 4529 умисних вбивства, 5359 розбійних нападів, 2829 випадків здирництва, 177900 крадіжок приватного майна [24, 25]. У період з 1995 по 1997 безробіття в Україні зросло з 3,7% до 6,1% [26]. У той же час відомо, що збільшення безробіття на 1% дає приріст злочинності у 5%. В даний період в країні з'являється бандитизм (1993р. - 2 випадки, 1996р. - 93 випадки), активізуються злочини із застосуванням вогнепальної зброї (1993р. - 865 випадків, 1996р. - більше 1500 випадків), тероризм (1996р. - 308 випадків, загинуло 50 осіб) [27].

Природньо, що така ситуація не могла не позначитися і на підприємницької діяльності. Саме підприємці виявилися найменш захищеними від нападу кримінальних елементів і серед втрат від замовних вбивств вони займали в ці роки перші місця. Створена в 1993 році Державна служба охорони при МВС України з одного боку була дорогою, а з іншого її зусилля в першу чергу спрямовувались на захист державних об'єктів.

Одним з напрямків вирішення проблеми захисту українського підприємництва стало формування приватних охоронних підприємств, що надавали послуги з охорони об'єктів та фізичних осіб, а також створення на підприємствах бізнесу власних охоронних підрозділів. Активна діяльність цих структур трохи знизила напруженість ситуації, а в подальшому у взаємодії з правоохоронними органами і зовсім стабілізувала її. Кримінальне свавілля припинилось, рівень загроз фізичного насильства спав. Таким чином, можна вважати, що з утворенням приватних охоронних структур в українському бізнесі відбулося зародження його безпеки. Водночас, вирішення проблеми мінімізації загроз фізичного характеру у підприємницькій діяльності, хоча і стало важливим кроком на шляху формування системи безпеки бізнесу, проте останній продовжував залишатися підданим великій різноманітності загроз економічного, інформаційного, кадрового характеру. Конкуренція, яка є важливим атрибутом ринкових відносин, змушувала підприємців до розробки нових технологій виробництва, створення нової конкурентоспроможної

продукції, особливих відносин на ринку. Інтелектуальні продукти, які все частіше стали застосовуватися у вітчизняному бізнесі як його перевага, одночасно ставали об'єктами загроз з боку конкурентів. З часом стало очевидним, що охоронні дії, хоча і є важливою складовою захисту інтересів бізнесу, проте не можуть ефективно впливати на схоронність його комерційних і промислових секретів. Виникла необхідність підняти безпеку бізнесу на інтелектуальний, інформаційний рівень. І тому з початку 1998 року безпека бізнесу вступає в новий етап - формування та розвиток інформаційної безпеки. Починають активно використовуватися положення існуючих правових актів (Закони України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про захист від недобросовісної конкуренції» та ін.), з'являються нові нормативні документи, якими здійснюється регулювання взаємовідносин у сфері захисту інформації. Активізується діяльність підприємницьких структур в питаннях категоріювання інформації, які знаходять своє відображення в регулюванні доступу до їх таємної та конфіденційної інформації, формуванні режимів функціонування інформації в процесі комерційної діяльності. У той же час, у забезпеченні інформаційної безпеки український бізнес все більше схилявся до питань захисту інформації та практично не приділяв уваги мінімізації інформаційних ризиків, інформаційного забезпечення підприємницької діяльності, протидії негативному впливу інформаційних технологій. Дані питання залишалися неврегульованими і в правовому полі. Тим не менш, на ринку інформаційних послуг з'являються підприємства, що надають послуги в сфері технічного захисту інформації, криптографії, інформаційного забезпечення та супроводу бізнесу. У той же час, за відсутності правового регулювання питань збору інформації та її надання зацікавленим особам (детективна діяльність) на платній основі, приватні структури діють напівлегально. У такому стані розвиток безпеки продовжується приблизно до 2004-2005р.р., якими і завершується другий етап.

Третій етап розвитку безпеки українського бізнесу характеризується, перш за все, активним впровадженням інформаційних технологій, переносом

акцентів з захисту підприємницької діяльності від різних загроз до їх попередження, недопущення їх негативного впливу на бізнес. Важливою особливістю третього етапу є інтеграція інформаційних технологій захисту бізнесу в економічні процеси підприємницької діяльності. Інформаційні технології, акцентуються насамперед, на мінімізації інформаційних ризиків при прийнятті бізнес - рішень, формуванні знань про те куди можна було б вкласти гроші, щоб гарантовано отримати прибуток. Одночасно інформаційні технології спрямовуються на запобігання економічних втрат в діяльності суб'єктів підприємництва та забезпечення роботи, з відшкодування нанесеного їм збитку.

У діяльності суб'єктів, що надають послуги з безпеки з'являються різні інструменти інформаційної роботи, розширюється арсенал економічних методів, проводиться активне впровадження сучасних методів роботи з персоналом. Якщо в попередніх двох етапах технології розвитку бізнесу випереджали технології забезпечення його безпеки, то в процесі третього етапу це відставання значно скоротилося. З'явились нові правові акти (Нова редакція Цивільного Кодексу України, Закони України «Про захист персональних даних», «Про доступ до публічної інформації» та ін.), внесено зміни до низки інших актів, що дозволило більш ефективно працювати силам безпеки. У системі освіти розпочинається підготовка фахівців в сфері забезпечення безпеки бізнесу з різних напрямків («Правове забезпечення безпеки підприємницької діяльності», «Управління фінансово-економічною безпекою», «Інформаційна безпека», «Економічна безпека фінансових установ» та ін.) Тобто, в забезпеченні безпеки бізнесу формується комплексний і системний підхід.

У той же час події світової фінансово-економічної кризи 2008 -2009 років виявили нові загрози для вітчизняного бізнесу та нові завдання в забезпеченні його безпеки. Головною особливістю тут було формування для глобального характеру загроз [28]. Поширення кризових явищ за межі національних кордонів, широке використання фінансових спекулятивних операцій, поява

фінансового бізнесу, функціонуючого поза реальною економікою, посилення агресивності інформаційно-психологічного впливу в конкурентних відносинах на міжнародному ринку зумовило необхідність перетворення безпеки бізнесу в один з елементів національної безпеки. Активну участь у даному напрямку почав Проводити Український Союз промисловців та підприємців, при якому було Створено Раду корпоративної безпеки і яким було ініційовано низку правових актів щодо забезпечення безпеки вітчизняного бізнесу в нових умовах.

Актуалізацією цього питання в 2010р. починається четвертий етап розвитку безпеки українського бізнесу. Даний етап характеризується активним проведенням наукових досліджень в сфері безпеки окремих видів бізнесу, появою нових напрямків у забезпеченні безпеки підприємницької діяльності (забезпечення безпеки на основі корпоративного інтересу; агітація, пропаганда та контрпропаганда у забезпеченні безпеки; активна розробка засобів безпеки на основі штучного інтелекту та ін.).

Разом з тим, незважаючи на більш ніж 20-річний шлях, пройдений українським підприємництвом, його безпека залишається далекою від досконалості, причому не тільки з причин об'єктивного характеру.

Тут варто було б звернути увагу на умови, в яких проходило становлення і здійснюється розвиток безпеки підприємницької діяльності в Україні, що робить істотний вплив на її характер. В першу чергу слід відзначити, що найбільш стійким до різного роду підприємницьких катаклізмів виявився великий бізнес, і не тільки тому, що в ньому зосереджений серйозний фінансовий капітал. Найважливішою гарантією його безпеки є політична і владна надбудова. Провідні бізнесмени, власники великого бізнесу, в більшості своїй досить тісно пов'язані з політичними силами (партіями, провідними громадськими об’єднаннями та рухами). Частина таких бізнесменів самі є депутатами різних рівнів, частина мають своїх представників у депутатському корпусі. Певні їхні сили представлені і в органах влади. Звичайно, ж не можна говорити, що політичне життя країни повністю піддане впливу інтересів

великого бізнесу, але лобіювання таких інтересів на окремих етапах його розвитку або в ході прийняття політичних і економічних рішень безумовно присутнє.

Середній бізнес найбільш динамічний в питаннях забезпечення своєї безпеки. Зазвичай він залежний від лояльності до нього політиків, чиновників, просто впливових осіб. А враховуючи часту їх ротацію, зміну поглядів і кумирів середньому бізнесу доводиться посилено лавірувати між інтересами таких суб'єктів, прикриваючи свої вразливі місця добрими взаєминами з ними. Тобто, безпека і живучість для середнього бізнесу в Україні в кожен момент його розвитку є особливо актуальними.

Малий бізнес, хоча і має чисельну перевагу, проте з т. з. безпеки бізнесу, не має практично ніякого впливу на її стан. Його безпека базується зазвичай на знаннях і діях самих підприємців, які не завжди вміють професійно себе захищати.

Характеризуючи умови, в яких проходив своє становлення і розвиток український бізнес і його безпеку необхідно виділити найбільш впливові з них, а саме - внутрішньополітичні, економічні, соціальні і правові.

Найважливішою особливістю внутрішньополітичних умов протягом усього пострадянського розвитку України, які впливали на безпеку вітчизняного бізнесу є перманентна боротьба за владу. Така боротьба формувала різного роду антагонізми у відносинах політичних угрупувань, а з ними і в їх економічній складовій, представленій, передусім бізнеселітою. Антагонізми і протистояння в політичній боротьбі формувало відповідні загрози її учасникам в різних сферах, в т. ч. і в економічній. Бізнес, час від часу опинявся в ситуаціях більше політичного, ніж економічного вибору, іноді навіть з чималими втратами для нього, що природньо гальмувало його розвиток. Така ситуація обумовлювалась насамперед тим, що рушійною силою практично всіх політичних угрупувань, що борються за владу був економічний інтерес, в реалізації якого важливе значення мали владні важелі впливу. Тому в бізнесі, в т.ч. і в певний час процвітаючому, нерідко спостерігаються масштабні

скандали з переслідуванням окремих бізнесменів, обмеження діяльності суб'єктів підприємництва, їх дискредитація, штучне створення невигідних умов діяльності. Загострення взаємин політичних конкурентів позначається і на їх бізнесі як головному факторі їхньої політичної стійкості.

Характеризуючи дану ситуацію, професор Крутов В.В. взаємовідносини бізнесу з політичними угрупованнями і владою називає головною проблемою в забезпеченні його безпеки. Корупція, незаконні дії влади, дискредитація суб'єктів підприємництва, підрив їх ділової репутації і т. д. – інструменти, які, як вважає Крутов В.В., використовуються політичними противниками для впливу на бізнес [29].

На думку Нездолі А.І. держполітика в Україні нерідко диктується кланами і приватними особами, які перебувають при владі або пов'язані з нею. А говорячи про причини такої ситуації Нездоля А.І. серед інших акцентує увагу на слабкості державної влади та корумпованості значної частини політичної еліти, переважанні корпоративних інтересів над державними [30]. Такі особливості внутрішньополітичних умов формують для бізнесу загрози особливого роду, не пов'язані з його комерційною діяльністю, а виникають з політичних відносин. Небезпека зазначених загроз полягає в тому, що вони, як правило, роблять свій вплив комплексно, масштабно, активно і зазвичай безкомпромісно. В умовах дії таких загроз бізнес змушений враховувати розстановку і інтереси політичних сил, їх спрямованість та перспективи. Необхідність же обліку таких обставин вимагає побудови відповідних систем безпеки бізнесу та використання специфічних механізмів його захисту, а також особливої поведінки на ринку, що і є відмінною особливістю організації безпеки вітчизняного підприємництва.

Говорячи про економічні умови, слід сказати, що Україна попри деякі заяви залишається все таки бідною країною. Природньо, що в такій країні не може бути безпечного бізнесу, оскільки відсутня необхідна економічна база, здатна забезпечити ефективний його розвиток. Незважаючи на значну пострадянську спадщину, ефективне реформування планової економіки в

ринкову з різних причин не відбулося. В результаті економіка України досі перебуває в стані становлення, їй складно протистояти різним кризовим явищам, тискові економічної експансії інших держав, природним катаклізмам, вона складно піддається управлінському впливу. Сформована економічна ситуація в поєднанні з податковим та адміністративним тиском змусила підприємців іти в тінь. Так, за оцінкою Державної податкової служби України, обсяги тіньового сектору економіки складають мінімум 350 млрд. грн. на рік [31].

Тіньова економіка є досить потужною сферою незаконної, неофіційної і кримінальної діяльності до якої залучаються і бізнесструктури, ризикуючи отримати дуже серйозні наслідки аж до ліквідації свого бізнесу.

Специфікою економічних умов є і наявність дисбалансу між великим, середнім та дрібним бізнесом. Створюючи могутні бізнес-угрупування, що об'єднують різні види діяльності, великий бізнес формує напівзамкнуті цикли підприємництва, обмежуючи при цьому життєві простори для середнього та дрібного бізнесу. В результаті в поведінці суб'єктів ринку виникає агресивність, що формує взаємовідносини суперництва і протиборства між ними і є підгрунтям для недобросовісної конкуренції.

Слід також звернути увагу і на таку особливість економічної ситуації як криза платежів. Остання обумовлюється невисокою платіжною здатністю значної частини суб'єктів підприємництва і особливою їх поведінкою на ринку. Під особливою поведінкою розуміється недотримання платіжної дисципліни та взятих на себе зобов'язань окремими суб'єктами підприємницької діяльності. Мають місце випадки ведення бізнесу за рахунок несвоєчасного повернення коштів, поставки товарів, затягування термінів виконання робіт і т. д., в результаті чого завжди існує підвищений ризик взаємовідносин суб'єктів бізнесу.

Даючи характеристику соціальних умов організації безпеки бізнесу не можна не звернути увагу на стан злочинності в країні. Щорічно в Україні реєструється понад 500 тис. злочинів, 40% яких вчиняється у сфері економіки

[23]. Однією з особливостей сучасної злочинності в Україні є її організований характер. У зв'язку з періодичним скороченням робочих місць на підприємствах і в держустановах, невисокими заробітками рядових громадян, можливістю практично легально здійснювати в економіці злочинну діяльність, проникненням злочинності у фінансову і державну сфери у злочинних угрупувань з'явилася не тільки потужна інтелектуальна, фінансова та матеріальна база, а й зв'язки у владних колах. В останні роки значно підвищився професійний рівень економічних злочинів, все більш часто вони відбуваються на високій науковій основі. Злочинність стала більш небезпечною, зухвалою і агресивною.

Значне розшарування громадян у доходах призвело до того, що більша їх частина має достаток, що межує з бідністю. Хронічні життєві негаразди, нестійке фінансово-матеріальне становище, відсутність перспектив відбилися на моральній стороні поведінки громадян, готових забезпечувати своє виживання способами, в т. ч. і такими, що є не зовсім законними. Вдаючись до шахрайських дій, крадіжок, обману, такі громадяни завжди виправдовують свою поведінку крайньою необхідністю.

Характерним для соціальних умов є наявність двох прошарків населення: молодих людей у віці до 30 років ніколи і ніде не працюючих і які забезпечують своє існування за рахунок рідних, випадкових підробітків, дрібного рекету, жебрацтва. Тривалий час такого їхнього існування сформувало менталітет утриманців, ледарів, пасивності, байдужості, готовності до антисоціальної поведінки, особливо під впливом зовнішніх сил. Другим прошарком є дрібні торговці - люди, що займаються торгівлею на ринках. Вся Україна покрита ринками, величезна маса людей щодня чимось торгує і щоб реалізувати свій, не завжди якісний товар, ринкові торговці вдаються до його фальсифікації, обману, підміни і т.д. З поведінки таких людей поступово зникає доброзичливість, толерантність, їх вчинки у великій мірі диктуються вигодою, отриманням доходу будь-яким способом.

Як про прошарок можна говорити і про нелегальних мігрантів в Україні. Проживаючи в країні практично незаконно, вони створюють свої угрупування, спільноти, генерують особливі взаємини, іноді чужі національним традиціям українців. Як правило, такі особи не збагачують країну ні своїм інтелектуальним потенціалом, ні трудовими досягненнями.

Враховуючи щорічне скорочення населення України приблизно на 300 тис. чоловік і більше, можна говорити, що в недалекому майбутньому вітчизняний бізнес очікує кадровий голод, і підприємці будуть змушені заповнювати свої вакансії іноземними громадянами, в т. ч. і з складу зазначених вище мігрантів.

Характеризуючи соціальні умови, не можна обійти увагою трансформацію особистості самого українця, яка сталася в ньому за роки незалежності. При відсутності раціональної ідеологічної складової в державній політиці, істотному зниженні виховної роботи в сім'ї, школі, вузі, колективі українські громадяни особливо у віці до 30 років значною мірою знизили моральні якості. Такі показники моралі, як доброта, людяність, співпереживання, терпимість, порядність, відповідальність, не завжди є основою їхньої поведінки і взаємин. Це, безумовно, відбивається і на ставленні до роботи, колективу, громадської діяльності. Тобто, порушилася моральна безпека, як окремого громадянина, так і суспільства в цілому. За таких умов в частини людей сформувалися переконання в обґрунтованості їх аморальної поведінки в сучасних умовах, їх життєдіяльність поступово перетворюється на боротьбу за виживання з усіма атрибутами саме боротьби. Якраз на основі боротьби і будуються їхні взаємини і поведінка в сім'ї, колективі, суспільстві.

Правові умови організації безпеки українського бізнесу характеризуються, перш за все, тим, що незважаючи на більш ніж як 20-річну його історію, в Україні тільки починається зароджуватися правове поле для регулювання цього виду діяльності. З 2012 року існує поки що єдиний спеціальний законодавчий акт, що регулює один із видів безпеки - охоронну діяльність. Всі інші види безпеки регулюються загальними законодавчими

нормами або підзаконними актами. В таких умовах суб'єкти підприємництва прагнуть врегулювати свою діяльність у сфері забезпечення їх безпеки власними нормативно-правовими актами. Враховуючи ж, що далеко не всі фахівці, які займаються безпекою бізнесу є професіоналами у сфері нормотворчої роботи, такі документи не завжди є якісними і не завжди можуть ефективно впливати на організацію безпеки бізнесу.

У той же час відсутність правових актів, регулюючих діяльність із забезпечення безпеки бізнесу не створює умов для формування особливого статусу працівників недержавної системи безпеки, їх прав, обов'язків, відповідальності. Ефективність їх роботи стримується саме відсутністю правового регулювання діяльності, якою вони займаються.

Існуючий стан справ призвів до того, що в країні відсутнє єдине розуміння суті безпеки бізнесу, її цілей і завдань. У зв'язку з цим всі суб'єкти підприємництва, організовуючи безпеку власної діяльності кожного разу винаходить «новий велосипед». Тому, на сьогодні вельми складно дати об'єктивну оцінку організації безпеки бізнесу в українському виконанні. Проте, слід зазначити, що в Україні забезпечення безпеки бізнесу склалося в самостійний вид діяльності, придбало легальний характер, признано практично всіма суб'єктами державної влади. Безпека є найважливішим атрибутом і умовою підприємницької діяльності. Вона здійснює істотний вплив на бізнес, передусім з т. з. захисту інтересів його власників.

Разом з тим, безпека бізнесу в Україні не набула системного характеру. Як правило, забезпечення безпеки того чи іншого суб'єкта обмежується функціями спеціально створеного для цієї мети підрозділу. В окремих випадках забезпечення безпеки суб'єкта підприємництва здійснюється на договірній основі підприємствами, що надають послуги охорони, захисту інформації, перевірки персоналу, інформаційного забезпечення. У той же час, в забезпечення безпеки не втягується персонал суб'єктів підприємництва, функції безпеки не трансформуються всім їх працівникам, які зазвичай сприймаються лише як суб'єкти загроз. Діяльність у сфері безпеки здійснюється за окремими

напрямами і не завжди концентрується на головних завданнях суб'єктів підприємництва. Заходи безпеки носять умовно - комплексний характер і не завжди націлені на попередження загроз і небезпек. Структури безпеки, як правило, заповнені колишніми працівниками правоохоронних органів, які маючи добрі знання та досвід захисту законності та інтересів держави, автоматично перенесли їх на забезпечення безпеку бізнесу. У той же час, активна конкурентна боротьба суб'єктів підприємництва, багатопрофільність їх діяльності, а також відсутність правового регулювання взаємовідносин у сфері безпеки бізнесу формують зовсім інші умови, в яких доводиться працювати колишнім правоохоронцям. Тільки знаннями та досвідом правоохоронної діяльності її представники не завжди в змозі забезпечувати ефективний захист суб'єктів бізнесу. Система ж підготовки кадрів для роботи в сфері забезпечення безпеки бізнесу тільки проходить своє становлення.

В таких умовах безпека вітчизняного бізнесу більшою мірою є пасивною, здатна лише до захисту інтересів підприємництва і не завжди готова діяти на упередження загроз, до того ж її дії сильно залежні від точки зору керівників суб'єктів господарювання на ту чи іншу ситуацію, які не завжди добре розуміють специфіку забезпечення безпеки.

Підводячи підсумок можна акцентувати наступне:

- в країні існують загрози вітчизняного бізнесу, природа яких не обумовлюється сферою підприємницької діяльності та взаємовідносинами в ній;

- певним чином можна говорити про наявність умов для формування загроз бізнесу, що випливають з особливостей соціально-економічних відносин і матеріально-економічного стану населення, в т. ч. і тієї його частини, яка представляє персонал суб'єктів підприємництва;

- відсутність спеціального законодавства в сфері регулювання безпеки бізнесу змушує сили безпеки діяти на межі правової і неправової поведінки, з вельми високим ризиком і не завжди ефективно;

- існування значного і потужного тіньового сектора обумовлює втягування окремих суб'єктів бізнесу в незаконну економічну діяльність, суттєво збільшуючи її ризик і посилюючи агресивність боротьби за більш безпечні та ефективні умови діяльності;

- обмежені економічні можливості суб'єктів бізнесу змушують їх фінансувати свою безпеку по мінімально-необхідному принципу;

- дисбаланс великого, середнього і малого бізнесу загострює взаємовідносини суб'єктів внутрішнього ринку, посилюючи недобросовісну конкуренцію, нездорове суперництво і протиборство;

- специфічні умови та недостатні можливості суб'єктів бізнесу сприяли тому, що їх безпека обмежується функціями спеціальних підрозділів, носить шаблонний характер і не завжди є професійною;

- не дивлячись на велику кількість потенційних кандидатів на роботу в сфері безпеки, вітчизняний бізнес відчуває нестачу в професіоналах, здатних ефективно, відповідно до сучасних вимог, забезпечувати його безпеку;

- безпека бізнесу в Україні не має державної підтримки, іноді вступаючи в конфлікти з державною правоохоронною системою діє не системно і не створює активної протидії загрозам підприємницької діяльності.

Таким чином, можна говорити, що вітчизняний бізнес здійснює свою діяльність в потужному силовому полі. На нього здійснює тиск держава, змушуючи діяти в умовах недосконалого законодавства та відсутності ефективних інструментів захисту. Крім того, бізнес суттєво відчуває силу корумпованого чиновництва, яке спирається на недосконалу нормативно-правову базу, владні можливості та міць державного апарату. Силове поле доповнюють інтелектуальні і фінансові можливості конкурентів, злочинні дії криміналу, що спирається на організовану злочинність. В таких умовах український бізнес особливо відчуває необхідність і актуальність забезпечення його безпеки, роблячи її обов'язковою умовою своєї діяльності, максимально докладаючи зусиль до підвищення її ефективності.

3. Інформаційні загрози та загрози інформації

Інформаційний розвиток, що зумовив кардинальні зміни в економіці, праві, соціальному житті одночасно сприяв формуванню нових видів загроз, в т. ч. і в підприємницькій діяльності. Суспільство опинилось в умовах тотального інформаційного пресингу, який по різному проявляє себе як до самого суспільства, так і до його суб'єктів. З одного боку значно розширились межі пізнання нашої дійсності, створились умови для активної творчої роботи, а з іншого, інформаційний розвиток, зачіпаючи практично всі сфери життєдіяльності створює досить суттєвий вплив на них через які у даних сферах відбуваються значні трансформації. Широкі можливості для творчого розвитку у свою чергу дали потужний поштовх науково-технічному прогресу, результати якого забезпечили суттєві переваги окремим суб'єктам. В той же час, зазначені переваги в умовах ринкових відносин досить швидко стали об'єктом інтересу інших осіб. Тобто, науково-технічні досягнення як об'єкти інтелектуальної власності, що мають інформаційні характеристики виявили потребу у захисті.

Разом з тим, інформаційний розвиток, викликаючи певні трансформації у різних сферах життєдіяльності, не завжди має позитивні наслідки. З різних причин зазначені трансформації можуть формувати специфічні, та як виявилось, досить небезпечні загрози.

Тобто, можна говорити про існування в сучасному інформаційному середовищі двох видів загроз: інформаційних, які надходять від власне інформації та її технологій і загроз самій інформації, пов'язаних з різного роду посяганнями на інформацію та її об'єкти. Таким чином, під інформаційними загрозами можна розуміти наявність в інформаційному середовищі шкідливої або небезпечної для його суб'єктів інформації, інформаційної продукції та технологій, здатних негативно впливати на їх стан, поведінку та взаємовідносини. Загрози ж інформації можуть розумітись як дії, пов'язані з

несанкціонованим доступом до об'єктів інформації або спрямовані на її викрадення, знищення, модифікацію, копіювання, блокування чи іншим чином позбавлення власника інформації переваг від її використання.

Характеризуючи інформаційні загрози можна бачити, що останні утворюються насамперед від тих досягнень і переваг якими характеризується сучасний інформаційний розвиток. Перш за все мова має іти про значні обсяги інформації, якою наповнене інформаційне середовище. Його інформація всебічно характеризує різного роду об'єкти, події, ситуації. В той же час, враховуючи диверсифікований стан інформації ми можемо отримати в певний проміжок часу лише відповідну частку інформації, знаючи, що існує достатньо необхідної нам інформації до якої з різних причин ми поки що не маємо доступу. Розуміння того, що отримана нами інформація є далеко не повною, формує відчуття постійної потреби в додатковій інформації.

Більш того, необхідна нам інформація постійно доповнюється, оновлюється і наші знання швидко старіють. Така ситуація зумовлює загрозу інформаційної залежності, ми постійно відчуваємо нестачу знань, а з ним і сумнів щодо свого рівня обізнаності в т. ч. і в професійній сфері. Разом з тим, прагнення до нової інформації збуджує у нас підвищену довіру до будь-якої новизни, що в умовах існування в середовищі великих обсягів необ'єктивної, але яскравої інформації, формує небезпеки отримання помилкових знань.

Слід також зауважити, що загроза інформаційної залежності має подвійний характер. З одного боку це залежність від інформаційних технологій, а з іншого – залежність від постійно існуючої потреби в новій інформації. Залежність від інформаційних технологій проявляється у формуванні прихильності до різного роду інформаційних продуктів та способів їх подання в інформаційне середовище. Насамперед мова іде про продукти та технології засновані на комп'ютерній чи іншій електронній інформації. Першість тут тримають комп'ютерні ігри. Гра є одним із найбільш ефективних методик пізнання світу.

З розвитком інформаційних технологій з’явилась можливість перетворити гру в особливу, т. з. віртуальну реальність, яка усуває людину від реалій сьогодення. Віртуальна реальність та перебування в ній стає більш цікавим, захоплюючим чим існуюче життя. Розвиток ігрової індустрії значним чином базується на надвеликих прибутках, які вона отримує. Більш того, надприбутки характеризуються параметрами часу знаходження в грі та параметрами адекативності (сили впливу). Зазначені параметри в своїх тенденціях можуть призводити до того, що людина втрачає над собою контроль. Особа, що знаходиться у комп’ютерній залежності не може бути ефективним працівником, у неї втрачається професійна реакція, знижується сприйняття відповідальності за прийняті рішення, зміщуються акценти в оцінках ситуацій. Формуванню залежності від комп’ютерних ігор значним чином сприяє піратство, яке на пострадянському просторі досягло катастрофічних масштабів. За таких умов доступ до комп’ютерних ігор не є проблемою, а самі ігри утворюють досить суттєву загрозу залежності від них не лише для громадян, а і для життєдіяльності всіх субєктів, в т. ч. і у сфері підприємництва.

Розвиток глобального інформаційного простору в останні роки, отримав тенденцію до інтеграції, можливості одночасного використання веб-платформ багатьма користувачами. Зазначені платформи дають змогу практично безмежного спілкування, перегляду новин, читання інформації, розважання (кіно, музика) і т. д. У наступному такі платформи з їх наповненням отримали назву соціальних мереж. Останні, як і комп’ютерні ігри володіють великим адекативним потенціалом і можуть загрожувати формуванням залежності від них. Залежність від перебування в соціальних мережах призводить до втрати продуктивного часу, зниження концентрації уваги на інформаційних повідомленнях, послаблення можливості приймати адекватні, зважені та обґрунтовані рішення. Крім того, наявність в соціальних мережах різних, зазвичай не повністю компетентних але переконливих точок зору, міркувань, коментарів може призводити до помилкових оцінок і рішень, якщо користувачі соціальних мереж будуть занадто "прив’язані" до них. Більш того, нерідко

через соціальні мережі спеціально подається неправдива, викривлена інформація з метою формування відповідного уявлення, переконання, поведінки стосовно певних подій чи суб'єктів. Сформоване під впливом такої інформації уявлення про ситуацію призведе до неправильних рішень, в т. ч. і у підприємницькій діяльності.

Слід також звернути увагу і на те, що сучасні соціальні мережі сприяють формуванню т. з. самотності у юрбі користувачів таких мереж. Спілкування у соціальних мережах полишено реальних, заснованих на емоційних відчуттях відносин, вона перетворюється у відносини роботів. Враховуючи, що середньостатистичний офісний працівник протягом робочого часу проводить наодинці з комп'ютером 5-6 годин щоденно, а його комунікації здійснюються в основному за допомогою технічних засобів, спілкування у соціальних мережах аж ніяк не замінює йому живих стосунків [32]. Така ситуація формує і відповідну поведінку людини, у неї поступово зникає необхідність у живому спілкуванні, вона залишаючись у суспільстві, колективі все більше стає самотньою, навіть не помічаючи цього оскільки у віртуальному просторі почуває себе більш комфортно ніж у колективі і навіть у сім'ї. Виходячи з того, що спілкування у соціальних мережах буде розвиватись та поширюватись, захоплюючи все більшу частину людей можна очікувати, що останні все більше будуть перебувати у стані ілюзій від результатів такого спілкування, які лише з далека будуть нагадувати реальну дійсність.

Сформована потреба спілкування за допомогою соціальних мереж зазвичай супроводжується наданням до неї певної інформації, власних оцінок, коментарів, що при сучасних методах контролю інформаційного простору формує для суб'єктів підприємництва загрозу втрати інформації.

Сучасні комунікаційні мережі, побудовані на досягненнях інформаційного розвитку, також зумовило суттєву залежність від них. Насамперед мова іде про телефонну залежність, т. з. телефономанію, особливо з врахуванням сучасних можливостей мобільних засобів зв'язку. Телефонна залежність поступово стає соціальною хворобою, яка набула масового явища.

Сучасна людина відчуває дискомфорт без телефону, де б вона не знаходилась. Більш того,офісні працівники прагнуть мати не один телефон, а два а то і три, причому найсучасніших типів, навіть не використовуючи весь спектр можливостей таких телефонних апаратів. На розмови по телефону витрачається значний час, зазвичай людина не контролює себе під час такої розмови (що говорить, з ким, де, як довго). У разі коли телефон з якихось причин відсутній (залишився вдома, на роботі) чи зникло його живлення людина відчуває тривогу, а то і паніку, їй складно думати про щось інше поки не буде вирішене питання з телефоном. Слід звернути увагу, що така нездорова пристрасть до засобів мобільного зв'язку (телефони, смартфони, інші засоби телефонії) може прогресувати і викликати тривалий хворобливий стан людини. Це вже не кажучи про те, що за певних обставин телефонний апарат мобільного зв'язку може ставати засобом витоку інформації, яка передається абонентами при їх спілкуванні. Постійна присутність телефонного апарату з його власником дає можливість контролювати не лише розмови власника, а і місце його розташування і пересування.

Як було уже згадано вище, інформаційна залежність проявляється і як постійна потреба у новій інформації, тривозі та страху отримання необ'єктивної, а то і дезінформуючої інформації. Безумовно, що загроза отримання такої інформації присутня завжди, безумовним є і те, що використання такої інформації може нанести шкоди діяльності підприємців. Але тут мова про інше – формування зверх обережної поведінки, в якій немає місця ризику, який є ключовим фактором підприємництва, ринкових відносин. Почуття пізнання дійсності, присутнє людям в епоху стрімкого інформаційного розвитку, нерідко переростає у залежність від абсолютної правди, якою характеризуються певні події, ситуації, об'єкти.

В управлінську діяльність сучасного підприємництва все частіше приходить розвідка, на яку покладаються завдання добування абсолютної правди і зникає або суттєво зменшується аналітична діяльність, пов'язана з обробкою інформації, формуванням комерційних гіпотез, припущень та

методик мінімізації ринку. Ми стаємо свідками різного роду скандалів в основі яких прослуховування комерційних перемовин, несанкціоноване отримання інформації з обмеженим доступом, таємних документів і т. і. Тобто, прагнення до абсолютної істини у інформаційному просторі за великих обсягів швидкозмінюючої інформації нерідко ігнорує моральні та правові норми бізнес-поведінки, що і є кінцевим результатом залежності від нової інформації. Мені можуть зауважити, що порушення зазначних норм у бізнесі було присутнє завжди. Погоджуючись з таким зауваженням, хочу наголосити на сьогоднішніх особливостях таких порушень: масштабності, зухвалості, збільшенні питомої ваги подібних методів у інформаційно-аналітичному забезпеченні підприємницької діяльності.

Продовжуючи тезу про інформаційну залежність і безпосередньо залежність від нової інформації, яка стала доступна її споживачам, не можна не помітити, що остання не сприймається ними як цінна. Знецінення інформації здійснюється через те, що споживачі прагнуть перетворити її у знання, які в умовах швидкої зміни інформації досить скоро старіють і стають мало придатними для застосування у реальній діяльності. Невміння працювати з наявною інформацією, упорядковувати її, класифікувати, виділяти головне, формувати бази даних є однією з причин виникнення загроз інформаційної залежності. Сучасний інформаційний розвиток зумовив певне протиріччя між існуючими інформаційними тенденціями і можливостями споживачів інформації, в т. ч. і суб'єктів підприємництва, використовувати їх у забезпеченні своєї діяльності. Інформаційна компетентність сучасних фахівців бізнесу в сьогоднішніх умовах має базуватись не лише на глибоких професійних знаннях, а насамперед вмінні працювати з великими потоками інформації, знаходити в них головне, враховуючи можливі перспективи її трансформації. Відсутність такої поведінки в інформаційному просторі не лише породжує залежність від нової інформації, а і не дає можливості відчути, бачити проблему, яка утворюється від такої залежності. В інформаційній роботі формується лише діяльність по отриманню інформації і ігнорується її

аналітична частина, яка замінюється постійними пошуком нової інформації. Поступово інформаційні бази суб'єктів підприємництва заповнюються інформаційним сміттям, перетворюючись у непридатні до ефективного використання.

Слід звернути увагу ще на один із наслідків інформаційної залежності, а саме залежність від технічних засобів, що використовуються у інформаційно-аналітичній роботі. Останні з допоміжних перетворились у самостійні елементи, які спільно з людиною виконують певні, досить складні функції зазначеної роботи. Програмована поведінка таких елементів побудована на схемах штучного інтелекту не є абсолютно надійною і незалежною і, як показує досвід, може бути непередбачуваною і загрозливою. В той же час інформаційний розвиток не дає можливості змінити ситуацію і примушує суспільство і його суб'єктів до адаптації до такої ситуації. За таких умов існує загроза виникнення залежності не лише від конкретно інформації як такої, а і від засобів, що використовуються при її збору, обробці, зберіганні, застосуванні.

Суттєвою особливістю інформаційних загроз є їх вплив на фізичне та психічне здоров'я людини, у зв'язку з чим в останні роки навіть з'явився такий термін "інформаційне здоров'я". Фахівці розуміння даного терміну подають як частину загального стану психічного, фізичного і соціального благополуччя, яке формується і залежить від інформації [33]. Тобто, в умовах інформаційного розвитку, панування інформаційних технологій, відбуваються певні зміни не лише в інтелектуальній сфері людини, але і у її організмі, що викликає різного роду негаразди з її здоров'ям.

Сучасний ритм життєдіяльності як людини взагалі, так і конкретного фахівця, працівника, характеризується безперервним потоком інформації, яка певним чином (позитивно чи негативно) впливає на людину, що безумовно відбивається на її нервовій системі і почуттях. Наприклад, російські дослідники встановили, що такі телепрограми як "Новости", "Вести", "Сегодня"

викликають у 60% телеглядачів почуття тривоги, у 49% - почуття страху, а у 45% - розчарування [34].

Інформаційні загрози щодо здоровя людини проявляють себе як безпосередньо, так і побічно. У першому випадку фахівці виходять з того, що сприйняття людиною будь-якої інформації ніколи не буває суто пасивним. Всякий процес пізнання здійснюється шляхом поєднання уже відомої інформації з новою. І тут можна спостерігати зміну емоційної складової процесу пізнання: протиріччя нової інформації тій, до якої людина була адаптована, недостатність інформації, наявність інформації, яка не сприймається людиною у зв'язку з її суб'єктивним світоглядом обов'язково викликають відповідну емоційну реакцію. Остання, у свою чергу, може сприяти виникненню емоційних розладів таких як страх, депресія, а то і агресія. Як вказують Панченко О.А. та Бончук Н.В., значуща інформація може впливати на виникнення психо-емоційного перенапруження, розвиток стресу і його наслідків у вигляді захворювань серцево-судинної, імунної систем, органів травлення, а також різного роду психічних хвороб [6, с.535].

Побічний характер загроз для здоров'я, пов'язаний з тим, що сучасні інформаційні канали подають в інформаційне середовище інформацію, яка руйнує нервову систему людини, змінює її психіку та емоційну складову захисту індивідуального та суспільного інформаційного здоров'я. Якраз завдяки такій інформації ми маємо сьогодні говорити про зростання малолітніх алкоголіків, наркоманів, курців, активізацію нездорової сексуальної поведінки, збільшення кількості неповнолітніх крадіїв, самогубств і т. і. Все частіше психіка людини, особливо молодої, формує протестну поведінку, постійне невдоволення. У подальшому це стає постійним фактором, душевним станом, який формує і відповідне ставлення до роботи. У останньому випадку така ситуація прямо впливає на безпеку взаємовідносин роботодавця і працівника, так як говорити про необхідність та лояльність з працівника буде проблематично за всіх умов.

Під впливом сучасних інформаційних продуктів, які є досить популярними серед сучасної молоді, останні не завжди сприймають працю як головний пріоритет у досягненні матеріального благополуччя та власного задоволення. Всі хочуть бути матеріально незалежними, а то і взагалі багатими, але не всі хочуть працювати. Кумирами нерідко виступають герої сучасних кінобойовиків, поведінка яких характеризується аморальністю, агресивністю, нахабством, вседозволеністю. Така інформація виступає моральною отрутою, в чому і полягає її головна загроза.

До інформаційних загроз можна віднести і наявні, практично безмежні обсяги необ'єктивної інформації, що наповнюють інформаційне середовище. Такими обсягами збагачується необхідна нам інформація, її досить складно не лише шукати, а і відрізняти від об'єктивної. За таких умов події та явища, що відбуваються у процесі життєдіяльності, на ринку стають малозрозумілими, інформація про них може виявитись непридатною для прийняття рішень. Виконання ж роботи щодо більшої об'єктивності інформації потребує додаткового часу та фінансових витрат, більш професійних кадрів, на що підприємці не завжди погоджуються.

Таким чином, інформаційна безпека суб'єктів підприємництва за сучасних умов має брати до уваги не лише загрози інформації, а і загрози, які надходять безпосередньо від самої інформації, її технологій та продуктів.

Говорячи ж про загрози інформації суб'єктів підприємництва необхідно зазначити, що в умовах ринкової економіки головною формою взаємовідносин зазначених суб'єктів є конкуренція. Остання ж передбачає боротьбу виробників за найвигідніші умови діяльності, більш якісну продукцію, послуги, роботи, ефективний їх збут. За таких умов конкуренція виступає не як одноразовий акт, а як правило, тривалий, а то і постійний процес. Тобто, у конкурентній боротьбі не буває постійних переможців, а тому така боротьба безперервна. Серед форм цієї боротьби не останнє місце посідає добування конфіденційних відомостей, розкриття виробничих і комерційних таємниць, отримання й використання різної інформації без згоди її власників. Для виконання таких дій створено цілу

індустрію полювання за інформацією, в арсеналі якої є найсучасніші технічні, програмні засоби та технології, психотехнічні комунікації, заходи психологічного та соціального характеру, різні методики добування інформації.

Тобто, ми можемо говорити про наявність загроз посягання на інформацію суб'єктів підприємництва. В той же час, враховуючи, що суб'єкти підприємництва у ході конкурентних відносин не лише утворюють нову інформацію, яка є об'єктом посягань з боку конкурентів, а і самі досить часто вдаються до заходів отримання чужої інформації, в т. ч. і з метою поповнення власного інформаційного ресурсу. Враховуючи, що інформаційне середовище наповнене не лише об'єктивною інформацією, а отримання чужої інформації може мати негативні наслідки, у інформаційній діяльності суб'єктів підприємництва можуть виникати певні ризики, які можна назвати інформаційними.

Водночас слід звернути увагу на те, що інформація згідно з чинним законодавством є об'єктом права власності, а також об'єктом володіння, використання та розпорядження. Тобто, на інформацію, її продукти та технології поширюється режим інституту майнових прав власності. Ураховуючи зазначене, необхідно вказати, що ризики, які виникають під час інформаційної діяльності (інформаційні ризики) суб'єктів підприємництва, виходять за межі загальновідомого технічного поняття і набувають властивостей суто майнових чи фінансових ризиків. У зв'язку з цим, виходячи із загальної класифікації ризиків і враховуючи введення інформації в систему товарних відносин, інформаційні ризики слід відносити і враховувати як майнові або виробничі ризики. Враховуючи, що інформаційні ризики мають особливий характер, дії підприємств, банків, пов'язані з урахуванням і мінімізацією таких ризиків, мають також певні особливості.

Отже, що ж слід розуміти під інформаційними ризиками? Ураховуючи всі вищезазначені аспекти інформаційної діяльності та інформаційних взаємовідносин суб'єктів підприємництва можна дійти висновку, що інформаційні ризики — це ймовірність витоку, руйнування та втрати наявної

у суб'єкта та необхідної для його діяльності інформації, використання ним необ'єктивної інформації, відсутність необхідної для прийняття правильних рішень інформації, а також можливість поширення в інформаційному середовищі невигідної, негативної чи небезпечної для суб'єкта підприємництва інформації, що в кінцевому рахунку може завдавати йому збитків, матеріальної або моральної шкоди.

Ураховуючи, що сучасна діяльність-суб'єктів підприємництва значною мірою перебуває в інформаційній площині, вони завжди перебувають у полі різного роду небезпек і загроз, тобто є об'єктами інформаційних загроз і впливу інформаційних ризиків.

Інформаційні ризики за своїм походженням поділяються на три категорії:

- ризики, пов'язані з втратою (витоком, руйнуванням, знищенням) інформації. Особливо це небезпечно, коли існує ризик втрати такої важливої для діяльності суб'єктів підприємництва інформації, як банківська та комерційна таємниця, або іншої інформації з обмеженим доступом;
- ризики, пов'язані з формуванням інформаційного ресурсу (використання неповної, неправдивої інформації, відсутність необхідної інформації, дезінформація);
- ризики, пов'язані з інформаційним впливом на діяльність суб'єктів підприємництва (поширення неправдивої та негативної інформації, інформаційно-психологічний вплив на працівників, клієнтів та акціонерів, інформаційний тероризм).

Враховуючи, що в умовах ринкової економіки ризик є однією із властивостей економічної діяльності, а для підприємницької діяльності ризик стає однією із її складових, то можна зазначити, що виключити ризик з інформаційних взаємовідносин суб'єктів підприємництва, та і взагалі з будь-яких відносин – неможливо.

Існування конкурентної боротьби та наявність вищезазначених ризиків породжує певні загрози для відомостей, які використовуються суб'єктами

підприємництва. Водночас діяльність останніх супроводжується безперервним процесом планування та прийняття рішень, що, своєю чергою, вимагає надійного інформаційного забезпечення. Разом з тим участь населення в економічному житті формує потребу об'єктивного та всебічного інформування його про діяльність суб'єктів підприємництва, позаяк довіра населення відіграє неабияку роль не лише у формуванні попиту на їх продукцію та послуги, а й загалом зумовлює перспективи розвитку.

На жаль, під час конкурентної боротьби існує загроза не лише неправомірних посягань на інформацію конкуруючих суб'єктів, але постійно здійснюється інформаційний вплив на споживачів продукції та послуг, який не завжди є об'єктивним і таким, що сприяє правильному формуванню уявлення про продукцію, послуги та суб'єктів, що їх виробляють чи надають.

Таким чином, у інформаційних взаємовідносинах суб'єктів підприємництва можуть виникати: загрози, пов'язані з посяганням на їх інформаційні ресурси (переважно ту частину, яка має обмежений доступ) та загрози, що виникають під час формування середовища, умов діяльності таких суб'єктів. У першому випадку інформація виступає об'єктом загроз, а у другому – інструментом їх реалізації.

Як свідчить досвід, основними способами реалізації таких загроз є:

- маніпулювання інформацією (дезінформація, викривлення інформації, подання в інформаційне середовище неповної або неправдивої інформації);
- порушення встановленого порядку інформаційного обміну, несанкціонований доступ або необґрунтоване обмеження доступу до інформаційних ресурсів, протиправне збирання і використання інформації;
- руйнування та використання з протиправною метою чужих інформаційних ресурсів;
- інформаційний тероризм (поширення комп'ютерних «вірусів», установлення програмних та апаратних закладних пристроїв, упровадження радіоелектронних приладів перехвату інформації, незаконне використання чи

порушення роботи інформаційних і телекомунікаційних систем, нав'язування фальшивої інформації, оприлюднення компрометуючої інформації та ін.).

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

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

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

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

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

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

Несанкціонованим буде також доступ до інформації з порушенням встановлених правил доступу до неї.

Вказані загрози носять загальний характер і однаково стосуються всіх видів інформації: документованої, електронної, знань та ін. Звичайно, що кожному із видів інформації притаманні додатково і інші, властиві тільки конкретним видам інформації загрози. Розглядати кожен з таких випадків мабуть буде недоцільним, оскільки вжиття заходів щодо захисту та протидії зазначеним видам загроз забезпечить безпечний стан будь-якої інформації з високим ступенем гарантії. Водночас, враховуючи, що сучасна підприємницька діяльність тісно пов'язана з комп'ютерними інформаційними технологіями, деякі особливості загроз таким технологіям слід було б навести, перш за все з врахуванням подальшої інформатизації суспільства та перспектив його розвитку.

Насамперед слід звернути увагу на загрози, пов'язані з глобалізацією інформаційних і телекомунікаційних технологій. У зв'язку з процесом міжнародної інтеграції та глобалізації обсяги та різноманітність загроз значно розширились. Підприємства, банки можуть зазнавати інформаційного удару щодо своїх інформаційних та фінансових ресурсів із глобального інформаційного простору. Серед найбільш поширених глобальних загроз — комп'ютерний тероризм і комп'ютерне хуліганство. Значне розповсюдження Інтернет-технологій і відносна анонімність користувачів спровокували появу так званих хакерів, крекерів, телефонних фанатиків — людей, які вважають своїм обов'язком здійснити певні протиправні дії в мережі Інтернет як самовираження на глобальному рівні. Як правило, такі особи є добре обізнаними з комп'ютерними технологіями, є їх фанатами і тому можуть на досить професійному рівні проникати в комп'ютерні системи. Вони є катастрофічно небезпечні для комп'ютерних технологій суб'єктів підприємництва, особливо банків, оскільки не тільки руйнують системи їх захисту, а можуть отримати досить важливу інформацію. Поширене останнім часом комп'ютерне хуліганство зумовило появу фактів, пов'язаних з так

званим електронним пограбуванням, насамперед банків. Останні щороку від протиправних дій різного роду хакерів, крекерів, комп'ютерних хуліганів зазнають мільярдні збитки та втрачають величезні обсяги інформації.

В реалізації загроз суб'єктів підприємництва важливе місце займають канали її витоку, до яких можна віднести: візуально-оптичні, акустичні та акустоперероблювальні, електромагнітні (в тому числі і магнітні та електричні), матеріально-речові (магнітні носії, папір, фотографії і т. д.).

Візуально-оптичні канали створюються як оптичний шлях від об'єкта інформації до її отримувача. Для цього необхідні енергетичні, часові та просторові умови і відповідні технічні засоби. Створенню таких каналів сприяють відповідні характеристики об'єкта інформації: конфігурація, поведінка, діяльність і т. і. Особлива цінність інформації, отриманої через такий канал, заключається в тому, що вона є максимально достовірною, оперативною і може служити документальним підтвердженням отриманих відомостей.

Джерелом створення акустичного каналу є тіла та механізми, які здійснюють вібрацію або коливання, такі як голосові зв'язки людини, елементи машин, що рухаються, телефонні апарати, звукопідсилювальні системи, гучномовні засоби, засоби звукозапису та звуковідновлення та ін.

Звукові коливання від голосу людини, інших звуків створюють акустичні хвилі, які розповсюджуючись у просторі і взаємодіючи з відповідними перешкодами викликають у них перемінний тиск (двері, вікна, стіни, підлога, різноманітні прилади) приводячи їх в коливальний режим. Впливаючи на спеціальні прилади (мікрофони) звукові коливання створюють у них відповідні електромагнітні хвилі, які передаються на відстань і несуть в собі створену звуковими коливаннями інформацію.

Акустичні канали створюються:

- за рахунок розповсюдження акустичних (механічних) коливань у вільному повітряному просторі (переговори на відкритому просторі, в приміщенні при відкритих вікнах, квартирках, дверях, витік через вентиляційні ка-

нали);

- за рахунок впливу звукових коливань на елементи і конструкції будівель (стіни, стеля, підлога, вікна, двері, вентиляційні системи, труби водопостачання, опалення, мережі кондиціонування);
- за рахунок дії звукових коливань на технічні засоби обробки інформації (мікрофонний ефект, акустична модуляція і т. і.).

Електромагнітні канали за своєю фізичною природою та експлуатаційними особливостями технічних засобів, які забезпечують виробничу діяльність є найбільш небезпечними і досить розповсюдженими для отримання інформації. Такі канали створюються через наявність у технічних засобах, які використовуються у виробництві джерел небезпечних сигналів. Перш за все до таких джерел відносяться перетворювачі – прилади, які трансформують зміни однієї фізичної величини в зміни іншої. В термінах електроніки перетворювач визначається як прилад який перетворює неелектричну величину в електронний сигнал або навпаки. Хороші знання можливостей перетворювачів дозволяють визначати неконтрольовані прояви фізичних полів, які і створюють електромагнітні канали витоку (передачі) інформації. В той же час, враховуючи ідентичність технічних та конструктивних рішень, електронних схем технічних засобів обробки інформації і забезпечення виробничої діяльності підприємств і банків, всім їм потенційно властиві електромагнітні канали витоку (передачі) інформації. Тому у всякому випадку використання технічних засобів обробки та передачі інформації створює загрозу її безконтрольного витоку (передачі).

Матеріально-речові канали отримання інформації створюються через вивчення відходів виробничої діяльності (зіпсовані документи або їх фрагменти, чернетки різного роду поміток, записів, листів і т. д.), викрадення, несанкціоноване ознайомлення, копіювання, фотографування, відеозапис документів, креслень, планів, зразків технічних або програмних засобів.

Водночас доцільно звернути увагу, що найчастішими і найбезпечнішими за розміром збитків є загрози, що утворюються помилками персоналу

суб’єктів підприємництва, працівниками, які працюють з різними видами інформації або обслуговують інформаційні системи. Наприклад, до 65 % втрат банків є наслідком ненавмисних помилок, некоректності та недбалості банківських працівників при роботі з інформацією [35]. Крім того, до факторів, які створюють умови витоку (передачі) інформації за дослідженнями спецслужб відносяться фактори, наведені в таблиці 3.1.

.

Таблиця 3.1.

Фактори, що створюють умови витоку інформації [23].

№ п/п	Фактори	% співвідношення
1.	Надмірна теревенливість співробітників підприємств, фірм, банків	32
2.	Прагнення працівників підприємств, фірм, банків заробляти гроші будь-яким способом і будь-якою ціною	24
3.	Відсутність на підприємстві, фірмі, у банку системи заходів, направлених на захист інформації	14
4.	Звичка співробітників підприємств, фірм, банків ділитись один з одним почутими новинами, чутками, інформацією	12
5.	Безконтрольне використання інформаційних ресурсів та засобів обробки і передачі інформації	10
6.	Наявність передумов для виникнення серед співробітників конфліктних ситуацій	8

До інформаційних загроз, пов’язаних з впливом на суб’єктів

підприємництва та їх середовище, слід віднести дискредитацію суб'єктів (поширення негативної неправдивої інформації про суб'єктів, маніпулювання індивідуальною та колективною свідомістю працівників, клієнтів, акціонерів, споживачів або просто громадян, дезінформація різних осіб у взаємовідносинах з суб'єктами, поширення негативних чуток про останніх, здійснення актів інформаційного тероризму та провокування інформаційних конфліктів, втягування суб'єктів в інформаційну війну).

Особи, які таким чином здійснюють вплив на суб'єктів підприємництва виходять із того, що людина живе в реальному світі, але сприймає його через систему комунікацій. Тому створивши нові комунікаційні технології та включивши в них відомі стандарти надання інформації можна викривити реальний світ замінивши його інформаційним в уявленні споживачів інформації. Тобто, інформаційний простір суб'єктів підприємництва є досить керованим і в залежності від того хто має можливість ним керувати, таким буде виступати і сам простір, а з ним і певний суб'єкт підприємництва. Вплив на споживачів інформації в таких умовах здійснюється шляхом формування відповідних схем надання інформаційних повідомлень, коментарів, точок зору експертів, поширення чуток, наведення прикладів та порівнянь, як правило, досить актуальних та гострих. В інформаційний простір суб'єкта підприємництва протягом певного терміну по багатьох каналах подається об'ємна інформація. Знаходячись під впливом стандартної побудови системи подачі інформації споживачі останньої сприймають її як реальну, а не штучно створену. Метою таких дій є формування умов, в яких субєкту складно буде здійснювати свою діяльність, він буде втрачати свій імідж, а з ним і конкурентоспроможність на ринку.

Конкретизуючи загрози підприємницькій діяльності у інформацій сфері, особливо слід було б акцентувати увагу на промисловому шпигунстві, яке охоплює практично всі складові ринкової економіки. Промислове шпигунство передбачає отримання інформації, яка тим чи іншим чином

характеризує відповідні технології, плани, розробки, ідеї, рішення, що є цікавими для конкурентів. Не обов'язково, щоб інформація була таємною або конфіденційною, головне, щоб вона була корисною для конкурента або іншого суб'єкта. За допомогою такої інформації можна значно зекономити час та ресурси для отримання ринкової переваги. Підприємці часто не усвідомлюють наскільки цінною вони володіють інформацією. Методи визначення ціни на свою продукцію, плани маркетингу і реклами, аналіз робочої сили, якості клієнтів та споживачів, оцінка конкурентів і т. і. зазвичай не є інформацією з обмеженим доступом, але тим не менш є цінною для суб'єктів промислового шпигунства. Сучасні технічні, фінансові, інтелектуальні можливості утворюють сприятливі умови для розвитку промислового шпигунства. Останнє є у сучасному бізнесі, в т.ч. і у вітчизняному постійним його супутником. Переважна більшість суб'єктів підприємництва здійснює збір інформації про конкретні підприємства, банки, фахівців, керівників з тим, щоб використати її у своїй діяльності. І не обов'язково щоб цим питанням займався суперпрофесіонал, достатньо мати професійні економічні знання і певний рівень знань з інформаційної роботи. Загрозлива сутність промислового шпигунства полягає ще і в тому, що це явище отримує практично масовий характер, особливо в діяльності середнього і великого бізнесу, а також у міжнародній економічній діяльності. На проведення заходів промислового шпигунства витрачаються значні суми коштів, у цій сфері задіяно сотні тисяч фахівців. У деяких країнах це питання отримало провідне значення у боротьбі за лідерство в економічному протиборстві.

Насамперед такими країнами є США, Великобританія, Франція, Німеччина, Росія, Японія. В останні роки до цих країн примкнувся Китай, у якому було відкрито технічний коледж, де його студенти опановують теорію науково-технічної розвідки. Після навчання випускники коледжу в рамках культурного обміну між країнами направляються до найбільш розвинутих країн для збору інформації [36]. З практики захисту від промислового

шпигунства можна бачити, що найбільшу зацікавленість промислові шпигуни проявляють до:

- фінансових звітів, планів та прогнозів;
- методик маркетингових досліджень і формування стратегії цін;
- технічної специфікації продукції, особливо тієї, що планується до виробництва;
- умов контрактів, угод;
- перспективних планів розвитку виробництва та комерційної діяльності;
- фінансового стану суб'єктів господарювання, їх виробничих потужностей;
- організаційної структури бізнесу суб'єктів підприємництва;
- системи безпеки діяльності суб'єктів.

Очевидно, що така інформація має значну цінність для суб'єктів підприємництва і тому втрата її, а особливо використання конкурентами формує достатньо серйозну для них загрозу.

Бізнес, що проходить своє становлення та розвиток на пострадянському просторі досить швидко опанував прийоми і способи промислового шпигунства, додавши йому національного колориту. Об'єктами діяльності пострадянських промислових шпигунів зазвичай стають: науково-дослідні та експериментально-конструкторські роботи; фінансові операції; фінансування проектів, інвестиційна політика суб'єктів підприємництва; особливості технологічного процесу; специфікація продукції, результати випробувань; режим поставок, списки замовників, відомості про угоди; організація виробництва; комерційна політика і стратегія. Беручи до уваги зазначені об'єкти шпигунської діяльності неможливо сказати, що пострадянський простір ринкової економіки є менш ризиковим і безпечним ніж подібний йому у розвинутих країнах. За таких умов, забезпечення інформаційної безпеки, в т. ч. і з точки зору протидії промисловому шпигунству є досить актуальним завданням суб'єктів

підприємництва.

Ще однією загрозою, яка є досить небезпечною для сучасного підприємництва в інформаційній сфері є уже відомий кібертероризм. Особлива небезпечність кібертероризму полягає в тому, що він одночасно несе в собі загрозу інформаційним ресурсам суб'єктів підприємництва і загрозу їх іміджу, суспільній оцінці їх діяльності. Крім того, як вказують фахівці, в останні роки кібератаки досить урізноманітнились, з'явилось кібершпигунство, хактивізм, кіберрекет і т. д.. Кібератаки стали більш масштабними, організованими і масовими. Значна їх частина поширюється на суб'єктів бізнесу. Об'єктами атак більш за все стають підприємства нафтової промисловості, телекомунікаційної індустрії, компанії аерокосмічної галузі, суднобудівні компанії, а також суб'єкти, які зайняті розробкою високих технологій. Втрати світової економіки від кібертероризму у 2013р. склали 113 млрд. дол. США. З 2004 по 2009 р.р. прибутки світової кіберзлочинності зросли в 10 разів і досягли 1 трлн. дол. США. В Україні дохідність кібертерористів перевищує доходи від наркоторгівлі і торгівлі зброєю разом узятих [37]. Найбільш поширеними загрозами тут виступають розповсюдження вірусів та різних шкідливих програм, що не лише руйнують програмне забезпечення, а і не дають можливості їх відновлювати. Зазвичай кібератакам передує збір інформації про об'єкти нападу за допомогою т. з. вірусів-шпигунів. Слід звернути увагу на те, що кібератаки поширюють свою дію як на стаціонарні комп'ютери, так і на мобільні пристрої, що зв'язані з комп'ютерними мережами. Україна, за даними 2013р. входила у трійку лідерів серед країн по кількості заражених мобільних пристроїв. За ступенем ризику зараження вірусами через Інтернет наша країна займає дев'яте місце серед країн з підвищеним ризиком (45,6% користувачів). Тобто, сучасна ІТ-інфраструктура підприємництва є досить уразливою і вимагає ефективного захисту. Натомість, забезпечення такого захисту з часом стає все більш дорогим і складним. На сьогодні в інформаційному просторі будь-якого бізнесу поширеними є проникнення до

баз даних, викрадення логінів, паролей до електронної пошти, ознайомлення з поштовими повідомленнями, іншими інтернет-ресурсами суб'єктів підприємництва. Особливо поширеним є викрадення грошей з банківських рахунків, пластикових платіжних засобів.

Не можна не звернути уваги і на т. з. офісні загрози інформації суб'єктів підприємництва, а саме загрози інформації, що міститься в документах та інформації, якою володіють і використовують у процесі роботи офісні працівники. Якщо дати відповідь на зміст поняття офісна діяльність, то вона може бути такою: це відповідним чином організована у просторі та часі сукупність дій персоналу певного суб'єкта, спрямована на забезпечення управління його діяльністю [39]. Тобто, офісна діяльність – це частина управлінського процесу. І у разі, коли у такій діяльності існують певні загрози, то це все буде відбиватись на процесі управління, у даному випадку діяльністю суб'єкта підприємництва. Оскільки управління значним чином пов'язане з інформаційними технологіями, то офісна діяльність спрямована на виконання різного роду завдань, робіт, процедур та операцій інформаційного забезпечення процесу управління. Структура, методика та зміст такого забезпечення формує т. з. офісну технологію. Об'єктом останньої є відповідний інформаційний ресурс, що оброблюється, інтерпретується та використовується для забезпечення управлінської діяльності. Звідси можна бачити, що в основі офісної діяльності є робота з інформацією суб'єкта підприємництва, причому робота в ланці управління, що визначає особливу важливість такої діяльності. Основними компонентами в офісній діяльності виступають знання працівників офісу і документи, які її супроводжують. За таких умов, зусилля суб'єктів, які прагнуть заволодіти інформацією суб'єктів підприємництва або нанести шкоди суспільній оцінці його діяльності будуть зосереджені саме навколо персоналу та документів.

Реалізація задумів щодо отримання офісної інформації через персонал може формувати відповідні загрози як самому персоналу, так і суб'єкту

підприємництва. Найбільш поширеними тут можуть бути наступні загрози: зманювання офісних працівників, що володіють офісними технологіями інформаційного забезпечення управлінських рішень для роботи у конкуруючих суб'єктів; залучення до роботи таких працівників та третіх осіб; шантаж офісних працівників з метою отримання доступу до офісних інформаційних ресурсів; провокація ініціативи працівників до неправомірного використання чи розголошення офісних технологій та інформації, яка в них використовується. У останньому випадку провокації можуть формуватися у самому офісі чи середовищі з якого працівники офісу забезпечують свої потреби та інтереси. Невдоволеність умовами, які впливають на забезпечення зазначених потреб і інтересів якраз і буде провокувати до поведінки, що може формувати загрози офісній інформації. І тут необов'язково щоб працівник був попередньо недобросовісним чи не лояльним до підприємства, банку. Такі риси можуть бути спровоковані атмосферою офісу, стилем взаємовідносин, режимом роботи, що само по собі може бути загрозливим явищем і формувати в кінці кінців суттєві загрози інформації суб'єкта підприємництва. Тим більше, що такі загрози, як правило, не пов'язані з матеріальними цінностями і людина не завжди відчуває провину від того, що якраз через неї сталось розголошення інформації. Необхідність документування діяльності суб'єктів господарювання утворює додатковий ризик для інформаційних ресурсів. Тут можуть існувати наступні загрози для офісної інформації:

- втрата чи неправильне знищення документів;
- ігнорування працівниками офісу вимог щодо розробки, виконання, обліку, пересилання, зберігання документів;
- робота з документами обмеженого доступу в присутності осіб, які не мають доступу до них, несанкціоноване передавання таких документів зазначеним особам;
- використання інформації обмеженого доступу у негрифованих документах, публікаціях, особистих записах;

- внесення в документи зайвої інформації, що має обмежений доступ;
- порушення режиму спеціального діловодства;
- копіювання службових, конфіденційних, таємних документів в кількості, яка перевищує службову необхідність;
- несвоєчасна передача документів в архів, порушення правил їх архівного зберігання;
- усний переказ документів при спілкуванні, в т. ч. і засобами зв'язку, наведення уривків тексту документів при листуванні або передачі їх електронною поштою.

Організовуючи інформаційну безпеку у своєму офісі слід мати на увазі, що переважна частина загроз формується саме через його працівників, незалежно від того, чи це інформація у вигляді знань працівників, чи це інформація, що міститься в документах. Звідси важливо знати основні фактори, що обумовлюють поведінку працівників за якої вони можуть вдатись до розголошення офісної інформації. Такими факторами можна вважати об'єктивні умови за яких працівники є основним джерелом інформації. Об'єктивним є і непередбаченість, малокерованість поведінки працівників в різних ситуаціях. До того ж, прогноз це лише ймовірність, сподівання на те, що вчинки, реакції людини можуть бути саме такими як ми передбачаємо. Факторами також виступають недоліки виховання працівників, особливості їх характеру, що у свою чергу може стати мотивацією працівників до невідповідної поведінки та вчинків. Недоліки професійної підготовки працівників, особливо щодо роботи з документами та інформацією обмеженого доступу, а також такі якості, як безвідповідальність, недисциплінованість та інші негативні вади теж можуть обумовлювати розголошення інформації офісними працівниками. Як випливає із наведених особливостей офісної роботи та умов, за яких можуть виникати загрози інформації, останні обумовлюються причинами як об'єктивного так і суб'єктивного характеру. Тому побудова системи

інформаційної безпеки будь-якого офісу має включати заходи спрямовані на формування безпечних умов функціонування інформації в офісі, а також заходи, що виключають або суттєво обмежують можливості неправомірної поведінки персоналу щодо офісної інформації.

4. Основи організації інформаційної безпеки суб'єктів підприємництва.

Як видно із викладеного у попередніх розділах, сучасні особливості інформаційного розвитку суттєво відбились на всі сфери суспільного життя в т. ч. і на підприємницькій діяльності. Формування, в результаті такого розвитку, інформаційних відносин є постійним атрибутом не лише діяльності, а і взагалі існування суспільства, громади, організацій, суб'єктів економічної діяльності. Така ситуація зумовила як певний прогрес, так і створила передумови до появи нового виду ризиків, небезпек та загроз – інформаційних. У процесі взаємовідносин суб'єктів підприємництва інтенсивність інформаційних ризиків, небезпек та загроз характеризується якістю самих взаємовідносин. Якщо в умовах інформаційного співробітництва та взаємодії можливість їх виникнення є мінімальною, то у інших видах взаємовідносин підстави виникнення інформаційних ризиків, небезпек та загроз будуть суттєво зростати. У такому випадку суб'єкти підприємництва мають бути готовими вживати адекватні заходи захисту та протидії таким ризикам, небезпекам та загрозам. Безумовно, що захист та протидія зазначеним небезпекам та загрозам, мінімізація інформаційних ризиків в діяльності суб'єктів підприємництва мають формувати окремий напрямок забезпечення їх безпеки – інформаційну безпеку.

Дослідження, проведені автором у сфері інформаційної безпеки підприємницької діяльності, показали, що сучасні уявлення про безпеку бізнесу взагалі і інформаційну зокрема є досить різноманітними, єдине бачення суті та змісту інформаційної безпеки відсутнє. Не вдаючись до детального аналізу точок зору різних авторів щодо розуміння інформаційної безпеки підприємництва, можна бачити наявність в них певних засад, якими автори ідентифікують інформаційну безпеку. Такими засадами виступає захист інформації. Якраз захист інформації є притаманним позиції переважної

більшості авторів у їх розумінні суті інформаційної безпеки. Віддаючи належне таким міркуванням слід звернути увагу на багатофункціональність інформації, яка проявляється у підприємницькій діяльності. Як уже говорилося вище, інформація є основою знань, тобто інтелектуального потенціалу суб'єктів підприємництва і які безумовно необхідно захищати. В той же час інформація є умовою ефективного здійснення підприємницької діяльності, вона використовується як засіб впливу на ринкову ситуацію, взаємовідносини суб'єктів, інформація має комерційну цінність і може виступати окремим видом економічної діяльності. Тобто, відтотоження інформаційної безпеки лише з захистом інформації при такій різноманітності її властивостей і функцій буде мабуть не логічним. За думкою автора, інформаційна безпека, крім захисту інформації (інформаційного ресурсу суб'єкта підприємництва), має бути спрямована на мінімізацію інформаційного ризику, ще має вирішальне значення для управління господарюючими суб'єктами та забезпечення їх розвитку. Враховуючи, ще інформаційні технології можуть являти собою вид інтелектуальної зброї і негативно впливати на підприємницьку діяльність окремих суб'єктів. Інформаційна безпека має включати в себе функції з протидії інформаційно-психологічному впливу, використанню технологій маніпулювання індивідуальною та колективною свідомістю. При тому підході *інформаційну безпеку підприємницької діяльності можна розуміти, як стан інформаційної роботи суб'єктів підприємництва за якого забезпечується ефективне інформаційне супроводження їх діяльності, надійний захист інформаційного ресурсу та результативна протидія негативному інформаційно-психологічному впливу на них.*

Тобто, структуру інформаційної безпеки суб'єкта підприємництва складають три складові, наведені на рис. 4.1.

Враховуючи динамічний характер сучасного інформаційного простору, такий підхід до розуміння суті та змісту інформаційної безпеки забезпечує суб'єктам підприємництва необхідний рівень живучості у їх конкурентній боротьбі, більш оптимальну поведінку у взаємовідносинах поміж собою,

іншими організаціями та інституціями. Інформаційна безпека у такому розумінні виступає формою існування суб'єктів підприємництва у інформаційному середовищі.

Рис. 4.1. Структура інформаційної безпеки суб'єкта підприємництва

Метою інформаційної безпеки у такому випадку є виключення можливості втрати суб'єктами підприємництва свого інформаційного ресурсу чи його руйнування, заподіяння шкоди їх іміджу, а також формування умов для ефективної діяльності і отримання прибутку. Критерієм же ефективності інформаційної безпеки є стабільність оцінки діяльності суб'єктів підприємництва на ринку та позитивні перспективи їх розвитку.

Очевидно, що досягнення визначеної мети інформаційної безпеки має забезпечуватись *виконанням певних завдань*, серед яких:

- організація відповідного режиму функціонування інформації в діяльності суб'єктів підприємництва;
- формування, необхідного для забезпечення ефективної діяльності суб'єктів підприємництва, інформаційного ресурсу;
- своєчасне виявлення загроз інформаційному ресурсу та іміджу суб'єктів підприємництва, їх інформаційним відносинам;
- оперативне реагування суб'єктів підприємництва на зміни та порушення умов інформаційних відносин, спроби посягань на їх інформаційні ресурси та імідж;

- забезпечення інформаційного впливу в необхідних суб'єктам підприємництва сегментах ринку;
- підготовка персоналу суб'єктів підприємництва з питань їх інформаційної безпеки;
- оптимізація заходів та витрат пов'язаних з забезпеченням інформаційної безпеки підприємницької діяльності.

Зазначені завдання мають бути інтегровані у повсякденну діяльність суб'єктів підприємництва шляхом планової роботи як спеціальних підрозділів інформаційної безпеки, так і всіх інших, що входять до складу організаційної структури суб'єктів. Останні мають забезпечувати свою інформаційну безпеку всією сукупністю своїх економічних, інтелектуальних, технічних, кадрових можливостей.

Організація інформаційної безпеки суб'єктів підприємництва здійснюється на основі принципу централізованого управління стратегічним розвитком суб'єктів і їх безпеки, як правило, у сукупності заходів, що виконуються ними у сфері забезпечення їх безпеки.

Основними принципами тут виступають:

- *законність* – заходи, що виконуються в межах організації та здійснення інформаційної безпеки мають вкладатись в межі чинного законодавства, не порушувати права та свободи громадян, законні інтереси інших суб'єктів та держави;
- *самостійність та відповідальність* – заходи інформаційної безпеки обираються суб'єктами підприємництва самостійно, в межах своїх можливостей і повинні бути адекватними загрозам їх інформаційній безпеці; за результати вжитих заходів відповідальність покладається на суб'єктів підприємництва та уповноважених ними на проведення таких заходів осіб;
- *компетентність* – виконання заходів інформаційної безпеки має здійснюватись грамотно, на високому професійному рівні, підготовленими для цього фахівцями;

- *економічна доцільність* – витрати на організацію та виконання заходів інформаційної безпеки повинні бути адекватними її ефективності, не завдавати шкоди економічному стану суб'єктів підприємництва;
- *цілеспрямованість* – заходи інформаційної безпеки мають здійснюватись у строгій відповідності основним завданням і напрямком діяльності суб'єктів підприємництва;
- *конфіденційність* – переважна сукупність заходів інформаційної безпеки проводиться на конфіденційній основі, інформування про їх проведення та результати, здійснюється лише обмеженому колу осіб.

Надійність та ефективність інформаційної безпеки суб'єктів підприємництва визначається через її відповідність встановленим вимогам, якими можуть бути:

- *безперервність забезпечення інформаційної безпеки* – заходи інформаційної безпеки проводяться з початком її організації і продовжуються протягом всього часу існування суб'єкта підприємництва, посилюючись та послаблюючись в окремих ситуаціях, але без їх припинення;
- *плановість інформаційної безпеки* – встановлення відповідного порядку застосування заходів інформаційної безпеки, який б забезпечував запобіжний характер їх впливу на виникнення небезпек і загроз;
- *конкретність інформаційної безпеки* – заходами безпеки мають бути охоплені конкретні об'єкти та дії суб'єктів підприємництва; заходи безпеки повинні бути пов'язані з конкретними операціями, угодами, відносинами, які здійснюються на даний час суб'єктами підприємництва;
- *активність інформаційної безпеки* – в арсеналі заходів інформаційної безпеки повинні бути як такі, що забезпечують захист інформаційного ресурсу та іміджу суб'єктів підприємництва, так і ті, які спрямовуються на протидію заходом негативного впливу та розкриття їх джерел;

- *комплексність інформаційної безпеки* – передбачає необхідність застосування у забезпеченні безпеки різних форм, методів, засобів, заходів щодо різних видів інформації та інформаційних відносин.

Реалізація принципів і вимог до інформаційної безпеки неможлива без конкретизації самого об'єкта безпеки. Враховуючи багатофункціональність інформації можна бачити її присутність у будь-якому матеріальному чи нематеріальному об'єкті або у будь-якому виду діяльності. Тобто, будь-який об'єкт чи діяльність можна подати інформаційно, зробити уявлення про нього на основі його інформаційних характеристик. Таким чином, беручи за об'єкт інформаційної безпеки інформацію, маємо обов'язково пов'язати її з певним об'єктом (людиною, підприємством, установою, організацією, предметом) або ж з відповідним видом діяльності. Тоді об'єктом буде виступати уже не інформація як така, а інформація про щось (об'єкт чи діяльність). Разом з тим, інформація про щось може бути об'єктом інформаційної безпеки лише тоді коли вона буде мати певну цінність (для підприємництва – комерційну цінність) і щодо неї буде проявлена зацікавленість з боку інших осіб. Враховуючи наведене, інформацію як об'єкт інформаційної безпеки можна подати наступним чином – Рис. 4.2.

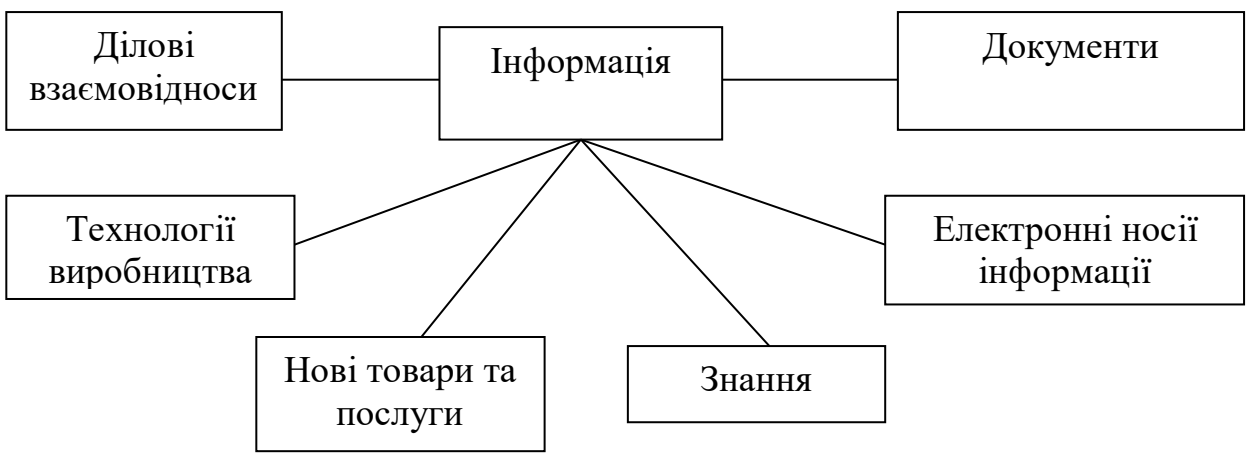


Рис. 4.2. Інформація як об'єкт інформаційної безпеки

У практиці забезпечення інформаційної безпеки суттєве значення має визначення її видів. Особливо це необхідно з т. з. організації інформаційної безпеки в діяльності суб'єктів підприємництва.

Аналізуючи практику інформаційних відносин суб'єктів підприємницької діяльності та беручи до уваги роль інформації в такій діяльності, можна говорити, що інформаційна безпека підприємництва включає наступні її види: комп'ютерну безпеку, інформаційно-психологічну безпеку, комунікаційну безпеку та документаційну безпеку.

Комп'ютерна безпека передбачає: захист засобів комп'ютеризації, комп'ютерних технологій і інформації, що знаходиться на електронних носіях; отримання необхідної суб'єктам підприємництва інформації із глобального інформаційного простору (мережі Інтернет) для формування їх інформаційного ресурсу; протидія інформаційним загрозам в середовищі електронної інформації(комп'ютерні віруси, шкідливі програми,комп'ютерний тероризм і т. п.)

Інформаційно-психологічна безпека зосереджує свої зусилля у сфері знанієвої інформації та її носіїв (працівників, клієнтів, споживачів продукції суб'єктів підприємництва). Основними напрямками забезпечення інформаційної безпеки є захист знаннєвої інформації (організація захисту інтелектуальної власності, режиму використання інформації працівниками та іншими особами у процесі інформаційних відносин); збереження інформаційного здоров'я працівників суб'єктів підприємництва в умовах інформатизації виробництва; розробка технологій отримання знаннєвої інформації (наукові дослідження, конференції, семінари, курси, сімпозіуми і т. п.) для формування інформаційного ресурсу суб'єктів підприємництва; протидія технологіям маніпулювання інформацією, індивідуальною та колективною свідомістю.

Комунікаційна безпека включає захист інформації в процесі взаємообміну (електронна пошта, мобільний зв'язок) та ділового спілкування (зустрічі, перемовини); проведення заходів пропаганди, контр-пропаганди та агітації в інформаційному середовищі суб'єктів підприємництва; протидія поширенню негативної інформації засобами масової комунікації.

Документаційна безпека спрямована перш за все на захист документованої інформації та її носіїв, насамперед через запровадження надійної системи загального і спеціального діловодства, розробки нормативних документів з питань інформаційної безпеки; запровадження технологій отримання необхідних даних з різного роду документів (правових актів, звітів, звичайних публікацій, виступів, описів і т. п.) для формування інформаційного ресурсу суб'єктів підприємництва;документальне супроводження протидії інформаційним загрозам та інформаційно-психологічному впливу щодо суб'єктів підприємництва, їх діяльності та персоналу(документування фактів порушення інформаційного режиму, поширення неправдивої інформації чи маніпулювання нею, документальне спростування негативної інформації, документи щодо вимог відшкодування моральної шкоди і т. і.)

Підвалинами успіху інформаційної безпеки є грамотна її організація в діяльності суб'єктів підприємництва. На жаль необхідно констатувати, що саме організація на сьогодні є одним із найбільш слабких місць у забезпеченні інформаційної безпеки підприємницької діяльності. Немає таємниці в тому, що саме грамотно організована інформаційна безпека є запорукою успіху суб'єктів підприємництва у їх інформаційних відносинах і діяльності взагалі. Організація інформаційної безпеки є елементом управління безпекою кожного із суб'єктів підприємництва. Тому цим питанням має опікуватись насамперед їх керівництво. Так, з питань організації інформаційної безпеки керівники установ суб'єктів підприємництва мають визначити мету безпеки, її основні завдання та напрямки зосередження основних зусиль; створити сприятливі умови для діяльності сил інформаційної безпеки відповідно до функцій покладених на неї; забезпечувати контроль ефективності функціонування системи інформаційної безпеки суб'єктів підприємництва. Безпосереднім організатором інформаційної безпеки є керівник підрозділу безпеки суб'єкта підприємництва, а там де він відсутній – сам керівник суб'єкта.

Аналіз практики забезпечення інформаційної безпеки в підприємницькій діяльності показує, що питанням її організації не придається необхідного

значення, в більшості випадків керівники підрозділів безпеки ними володіють майже на примітивному рівні. Процес організації практично відсутній у керівництві інформаційною безпекою суб'єктів підприємництва. Здебільшого організація безпеки зводиться до реакції на негаразди, які виникають у інформаційних відносинах суб'єктів підприємництва. Потенціал, закладений у грамотній організації інформаційної безпеки, не сприймається як перевага в інформаційному середовищі, конкурентній боротьбі, ринкових відносинах взагалі.

За результатами узагальнення діяльності суб'єктів підприємництва по забезпеченню їх інформаційної безпеки автором запропоновано відповідну структуру процесу її організації на підприємствах, у банках та інших організаціях(Рис. 4.3).

Процес організації інформаційної безпеки суб'єкта підприємництва виконується на підставі глибокого вивчення умов та змісту діяльності суб'єкта, характеру його взаємовідносин на ринку та поведінки в інформаційному середовищі. Крім того, процесу організації мають передувати вивчення можливостей суб'єкта підприємництва щодо забезпечення відповідного рівня інформаційної безпеки та правових умов в яких здійснює свою діяльність суб'єкт. Процедура та зміст організації інформаційної безпеки обов'язково має бути узгоджена з точкою зору керівника установи суб'єкта підприємництва. Точка зору керівника має бути сформована як його рішення з даного питання.

Важливим в організації інформаційної безпеки суб'єктів підприємництва залишається створення відповідної системи. Остання має розумітись як певна сукупність сил, засобів, заходів і технологій, спрямованих на забезпечення високої стійкості суб'єкта підприємництва до інформаційних загроз та ефективне інформаційне супроводження його діяльності.

Основними принципами побудови системи інформаційної безпеки мають виступати:

- *стійкість* – система має ефективно протистояти будь-яким діям, спрямованим на її руйнування чи дестабілізацію функціонування;

Рис. 4.3. Структура процесу організації інформаційної безпеки суб'єкта підприємництва

- *адаптація* – система має оперативно реагувати на будь-які зміни в інформаційному середовищі та інформаційних відносинах суб'єкта підприємництва;
- *трансформація* – система має працювати з різними видами інформації, в різних інформаційних середовищах, в будь-яких комунікаційних

мережах без втрати ефективності забезпечення інформаційної безпеки суб'єкта підприємництва;

- *відновлення* – система має бути здатною в оптимально короткі терміни відновлювати свою живучість та забезпечувати виконання необхідного обсягу заходів інформаційної безпеки суб'єкта підприємництва обмеженим складом сил і засобів;
- *автономність* – система має бути максимально незалежною від зовнішніх джерел та суб'єктів, забезпечувати своє функціонування власними силами та засобами.

Таким чином, враховуючи структуру та зміст завдань інформаційної безпеки, обсяг заходів, які покладаються на неї, можна стверджувати, що вона займає одне із провідних місць у забезпеченні безпеки діяльності суб'єктів підприємництва. В той же час, забезпечення інформаційної безпеки це досить складний і трудомісткий процес, який вимагає значних фінансових, матеріальних, інтелектуальних зусиль. Останні ж мають спиратись на грамотні, науково обґрунтовані та підтверджені підприємницькою практикою погляди професіоналів, здатних реалізувати визначену певним суб'єктом підприємництва концепцію інформаційної безпеки.

5. Правові засади інформаційної безпеки суб'єктів підприємництва

Забезпечення інформаційної безпеки підприємницької діяльності здійснюються під впливом різноманітних умов, серед яких провідне місце займають правові умови. Останні, у свою чергу, утворюються чотирма джерелами правових норм: Конституцією України, законодавчими актами, підзаконними актами, нормативно-правовими актами суб'єктів підприємництва. Важливість правових умов у забезпеченні інформаційної безпеки полягає у тому, що без правових актів, які складають такі умови процес організації інформаційної безпеки неможливий взагалі. Саме за допомогою зазначених актів здійснюється регулювання інформаційних відносин та застосування заходів інформаційної безпеки, визначається правомірність тих чи інших дій щодо інформації, формуються підстави для відповідальності за дії в інформаційному просторі. В решті решт правові норми забезпечують захист суб'єктів підприємництва від неправомірного посягання на їх права, інтелектуальну власність, інформацію, що може мати місце у процесі їх діяльності. Положення ст.55 Конституції України надають право будь-якими, не забороненими законом засобами захищати свої права і свободи від порушень і протиправних посягань [39]. Під засобами, серед інших, можна розуміти і правові засоби (норми та положення Конституції та законів України, нормативно-правових актів органів влади, нормативних документів суб'єктів господарювання та інших організацій, рішення та ухвали судів, положення судових органів, Міністерства юстиції України, положення договорів, угод, укладених суб'єктами підприємництва, рішення, приписи, накази органів нагляду та контролю). А права можуть поширюватись і на інформаційну сферу. Зокрема право на інформацію, передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів [20]. Крім того, Конституцією

України гарантується право судового захисту щодо спростування недостовірної інформації, право вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням та поширенням недостовірної інформації. Основний закон забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків визначених законом(ст. 32). Конкретизуючи зміст конфіденційної інформації про особу слід зазначити, що до такої інформації належать, зокрема, дані про національність особи, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адресу, дату і місце народження [20]. Тобто Конституція України встановлює загальні умови поведінки суб'єктів, і громадян в інформаційному просторі.

Важливим моментом для забезпечення правової поведінки в інформаційному просторі і правомірних інформаційних відносин є регулювання доступу до інформації. Ці питання регулюються положеннями Закону України « Про інформацію» (Рис. 5.1).

Рис. 5.1 Режим доступу до інформації (Закон України «Про інформацію», ст. ст. 20, 21).

Будь-яка інформація є відкритою крім тієї, що віднесена законом до такої, що має обмежений доступ. Важливо знати, що обмеженню підлягає інформація, а не документ в якому вона міститься. Якщо документ містить таку інформацію, то він підлягає ознайомленню в частині, що не містить інформації з обмеженим доступом [40].

Конфіденційною є інформація про фізичну особу, доступ до якої обмежений фізичною чи юридичною особою, крім суб'єктів владних повноважень. Така інформація може поширюватись зазначеними особами за їхнім бажанням (згодою) у визначеному ними порядку відповідно до передбачених ними умов, інших випадках визначених законом. До суб'єктів владних повноважень законодавець відносить – органи державної влади, місцевого самоврядування, інших суб'єктів, що здійснюють владні управлінські функції відповідно до законодавства, в т.ч. і делеговані повноваження.

Важливим є з'ясування особи яка має право обмежувати доступ та надавати інформації категорію конфіденційної. Очевидно, що це може бути сам власник такої інформації, або особа яка отримує право розпоряджатись даною інформацією. У останньому випадку законодавець визначає перелік розпорядників інформації, види інформації, якими вони можуть розпоряджатись, їх обов'язки та функції (Закон України «Про доступ до публічної інформації» ст. ст. 13-18).

Таємною є інформація, доступ до якої обмежується відповідно до вимог ст.6 Закону України «Про доступ до публічної інформації» і розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить відомості, що складають державну, професійну, банківську, комерційну та інші передбачені законом види таємниць.

До службової інформації належить така, що міститься в документах суб'єктів владних повноважень, а також зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Доступ до таємної інформації визначається відповідно до чинного законодавства установами, органами, які володіють такою інформацією. Доступ до службової інформації визначається відповідно до Закону України «Про доступ до публічної інформації» в порядку передбаченому внутрішніми документами суб'єкта владних повноважень.

Відносини у сфері доступу до публічної інформації регулюються Законом України «Про доступ до публічної інформації». Зокрема, закон дає визначення поняття «публічна інформація» згідно з яким це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні таких суб'єктів, інших розпорядників, крім випадків встановлених законом.

Відповідно до зазначеного вище закону, доступ до публічної інформації здійснюється шляхом її оприлюднення у встановленому порядку та шляхом подання запитів до розпорядників інформації. Інформація надається безкоштовно.

Суб'єктами відносин у сфері доступу до публічної інформації є запитувачі інформації, розпорядники інформації, їх структурні підрозділи або відповідальні особи з питань виконання запитів.

Окремо регулюється система відносин щодо доступу до інформації про особу. Тут маємо брати за основу положення Закону України «Про захист персональних даних», Закону України «Про доступ до публічної інформації», Закону України «Про інформацію». Зокрема передбачається, що збирання, зберігання, використання та поширення інформації про особу не можливе без згоди саме особи, крім випадків передбачених законом. Обсяг такої інформації має бути максимально обмеженим і використовуватись лише з метою та у спосіб, визначений законом.

Суб'єктами відносин у сфері доступу до інформації про особу виступають самі особи, володільці та розпорядники баз персональних даних, треті особи (особи яким володільцями чи розпорядниками баз персональних даних здійснюється передача персональних даних відповідно до закону), уповноважений державний орган з питань захисту персональних даних, інші державні органи, органи місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних.

Про збір даних про осіб, включення інформації про них в базу персональних даних особи мають повідомлятись про їх права володільцем, чи розпорядником бази даних протягом 10 днів з дня формування даних. Разом з тим, коли персональні дані збираються з загальнодоступних джерел таке повідомлення не здійснюється[41].

Поширення персональних даних здійснюється лише за згодою особи. Без згоди - у випадках визначених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини. Порядок доступу до персональних даних та відносини суб'єктів з цих питань регулюються положеннями ст.ст. 16-19 Закону України «Про захист персональних даних».

Питання правового регулювання доступу до персональних даних нормами міжнародного права, забезпечуються положеннями Конвенції Ради Європи «Про захист фізичних осіб при автоматизованій обробці персональних даних» від 28.01.1981р. зі змінами внесеними у 1999р., додаткового протоколу до Конвенції «Про захист фізичних осіб при автоматизованій обробці персональних даних щодо органів нагляду і трансграничних потоків даних» від 08.11.2001 року., Директивою Ради Європейського Союзу «Про захист фізичних осіб при автоматизованій обробці персональних даних і про вільний обіг таких даних» (1995р.), а також Директивою «Про обробку персональних даних і захист прав фізичних осіб у телекомунікаційному секторі» (1997р.). Основними принципами захисту персональних даних викладених у зазначених правових актах є: збір і обробка персональних даних мають здійснюватись коректно і законно; використання персональних даних повинно бути адекватним визначеній меті, та обмежуватись за термінами; персональні дані повинні бути точними, оброблюватись лише з дозволу суб'єктів цих даних, бути доступними для них; персональні дані повинні бути надійно захищені [42].

Важливе значення, з точки зору інформаційної безпеки, має правове регулювання відносин у сфері захисту інформації з обмеженим доступом. Для

підприємницької діяльності важливими питаннями є захист комерційної та банківської таємниці, а також комерційної інформації.

Правову основу комерційної таємниці складають положення Господарського кодексу України, Цивільного кодексу України, Кримінального кодексу України, Кодексу України про адміністративні правопорушення, Законів України «Про захист від недобросовісної конкуренції», «Про інформацію», інших правових актів. Зокрема, сутність комерційної таємниці як виду інформації з обмеженим доступом подається у Цивільному кодексі України. Так, комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи певній формі та сукупності її складових є невід'ємною та не є легкодоступною для осіб, які звичайно мають справу з видом інформації до якого вона належить і у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. За змістом комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не не можуть бути віднесені до комерційної таємниці [43]. Перелік відомостей, які можуть становити комерційну таємницю подається у Постанові Кабінету Міністрів України №611 від 09.08.93р.

Відповідно до положень Господарського кодексу України склад і обсяг відомостей, що становлять комерційну таємницю, спосіб їх захисту визначається суб'єктом господарювання [44].

Таким чином, законодавець не дає конкретного змісту комерційної таємниці, подаючи лише вказівки про що мають бути відомості, які становлять таку таємницю. Слід також звернути увагу на те, що такий вид таємниці як комерційна стосується лише суб'єктів господарювання: юридичних осіб та фізичних осіб зареєстрованих як суб'єкти підприємницької діяльності. Право власності на такий вид інформації вони отримують через створення її власними силами та засобами або іншими особами на договірних засадах з суб'єктами

господарювання за їх кошти і на їх користь, придбанням такої інформації у інших осіб. Створення інформації, що становить комерційну таємницю іншими особами на користь суб'єктів господарювання стосується зазвичай продуктів інтелектуальної власності. Комерційною таємницею у таких випадках захищаються інформаційні характеристики зазначених продуктів. Право власності включає право володіння, право використання і право розпорядження чи поширення. Враховуючи, що суб'єкти господарювання є власниками своєї комерційної таємниці, вони ж самі визначають умови та способи їх захисту, доступу до неї, в т. ч. і у будь-яких взаємовідносинах з іншими суб'єктами. Згідно з положеннями Цивільного кодексу України (ст. 506) право розкриття комерційної таємниці належить особі, яка володіє майновими правами інтелектуальної власності на комерційну таємницю. Тобто, підстави, умови, способи захисту відомостей, що становлять комерційну таємницю у різних суб'єктів господарювання можуть бути різними, організуються кожним із них, виходячи з особливостей їх діяльності, інформаційних потреб та можливостей. Інформаційні відносини суб'єктів господарювання щодо комерційної таємниці, як правило, будуються на договірних засадах, з врахуванням нормативних документів суб'єктів у сфері їх інформаційної безпеки.

Окремо регулюється порядок захисту комерційної таємниці суб'єктів господарювання у їх конкурентних відносинах. Так, відповідно до гл. 4 Закону України «Про захист від недобросовісної конкуренції» неправомірним визнається збирання протиправним способом відомостей, що становлять комерційну таємницю за умов коли це завдало чи могло завдати шкоди суб'єкту господарювання. Крім того, неправомірним також визнається впровадження у виробництво або врахування під час планування чи здійснення господарської діяльності без дозволу уповноваженої на те особи (неправомірне використання) відомостей, що становлять комерційну таємницю. Неправомірним вважається розголошення чи схилення до розголошення комерційної таємниці [45]. Такі дії є протирічать нормам чинного

законодавства і переслідуються у кримінальному, адміністративному чи цивільному (відшкодування шкоди) порядку.

Певну специфіку мають інформаційні відносини предметом яких є банківська таємниця. Згідно ст. 60 Закону України «Про банки і банківську діяльність» банківською таємницею є інформація щодо діяльності та фінансового стану клієнтів банку, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третіми особами при наданні послуг банку [46]. Тобто, банківська таємниця виникає тоді коли суб'єкти господарювання (підприємництва) стають клієнтами банків. Останні вважаються такими у разі отримання послуг банків. Враховуючи ж, що вказані суб'єкти здійснюючи свою фінансово-господарську діяльність обов'язково вдаються до послуг банків, виникнення в них банківської таємниці є закономірним фактом. В той же час слід зазначити, що статус банківської таємниці діє навіть тоді, коли суб'єкт (клієнт) припиняє відносини з банком. Інформація, що надана банку залишається в банку і закон не передбачає, що втрата відносин клієнта з банком припиняє статус банківської таємниці.

Зміст банківської таємниці конкретизовано у зазначеному законі і він є остаточним аж до поки в закон в установленому порядку не буде внесено відповідних змін. Зокрема вказується, що до складу банківської таємниці віднесено:

- відомості про банківські рахунки клієнтів, в т. ч. кореспондентські рахунки банків у НБУ;
- операції, які були проведені на користь чи за дорученням клієнтів, здійснені ними угоди;
- фінансово-економічний стан клієнтів;
- відомості про системи охорони банку і клієнтів;
- інформація про організаційно-правову структуру юридичної особи клієнтів, їх керівників, напрями діяльності;

- відомості стосовно комерційної діяльності клієнтів чи їх комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;
- інформація щодо звітності по окремому банку за винятком тієї, що підлягає опублікуванню (ст. 70) Закону України «Про банки і банківську діяльність»;
- коди, що використовуються банками для захисту інформації.

Тут слід додати, що у зв'язку з появою законодавства про захист персональних даних, НБУ вніс певні доповнення до змісту банківської таємниці. Відповідно до постанови Правління НБУ від 11.07.2012р. №292 банківською таємницею є відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, що стали відомі банку під час обслуговування фізичної особи та взаємовідносин з нею та взаємовідносин з нею чи третіми особами при наданні послуг банку [40].

Тобто, за своєю суттю і змістом банківська таємниця є єдиною для всіх банків і їх клієнтів, на відміну від комерційної таємниці.

Необхідно звернути увагу на те, що перераховані відомості не стають автоматично банківською таємницею з встановленням стосунків з банками. Інформація має стати відомою банку тільки в результаті обслуговування клієнта, що має підтверджуватись відповідною угодою про надання (отримання) банківських послуг. Крім того, фактом, що підтверджує отримання банком відповідної інформації про клієнта мають бути певні документи, які вимагаються банками від їх клієнтів для надання їм тих чи інших послуг. Скажімо, інформація про систему охорони клієнта не є фінансовою інформацією, не стосується послуг банку і тому не може бути відома останньому, а звідси і не може бути банківською таємницею. Тобто, факт надання інформації має бути пов'язано з наданням клієнту послуг банку і засвідчено документально.

Необхідність дотримання такої процедури обумовлюється тим, що інформація, яка становить банківську таємницю залишаючись власністю

клієнта захищається банком. Законодавець поклав на банк відповідні обов'язки щодо організації захисту банківської таємниці, зокрема визначив заходи захисту і встановив порядок доступу до неї. У даному випадку порядок доступу до відомостей, що становлять банківську таємницю є єдиним і не залежить від волі чи бажання власника таємниці або банку.

Зокрема, ст. 62 Закону України «Про банки і банківську діяльність» визначає порядок розкриття банківської таємниці.

Банківська таємниця розкривається:

- на письмовий запит або з письмового дозволу власника даної інформації;
- за рішенням суду;
- органам прокуратури, Служби безпеки України, Міністерства внутрішніх справ України, Антимонопольного комітету України – на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу;
- центральному органу виконавчої влади, що реалізує державну податкову політику: на його письмову вимогу щодо наявності банківських рахунків; за рішенням суду щодо відомостей, зазначених у деклараціях про майно, доходи, витрати і зобов'язання фінансового характеру, у зв'язку з проведенням перевірки їх достовірності;
- центральному органу влади, що реалізує державну політику у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом на його запит щодо фінансових операцій, пов'язаних з фінансовими операціями, що стали об'єктом фінансового моніторингу (аналізу) згідно із законодавством щодо запобігання та протидії легалізації (відмиванню) доходів одержаних злочинним шляхом або фінансового тероризму, а також учасників зазначених операцій;
- органам державної виконавчої служби на їх письмову вимогу з питань виконання рішень судів та рішень, що підлягають примусовому

виконанню відповідно до Закону України «Про виконавче провадження» стосовно стану рахунків конкретної юридичної особи або фізичної особи;

- Національній комісії з цінних паперів і фондового ринку у випадках самостійного подання банком інформації про банк як емітент та адміністративних даних відповідно до законодавства про цінні папери і фондовий ринок.

Порядок надання банками інформації, що становить банківську таємницю визначений у Законі України «Про банки і банківську діяльність» і конкретизовано Правилами зберігання, захисту використання та розкриття банківської таємниці, затвердженими постановою Правління НБУ №267 від 14.07.2006р.

Таким чином, доступ до банківської таємниці суворо регламентовано чинним законодавством дотримання якого законодавець поклав на банки та інших суб'єктів предметом відносин яких є саме інформація, що становить банківську таємницю.

Узагальнюючи викладене необхідно вказати, що основними особливостями банківської таємниці як інформації з обмеженим доступом є наступні: зміст банківської таємниці визначено законом, законодавець встановив вичерпний перелік відомостей, які становлять банківську таємницю, зміст банківської таємниці для всіх суб'єктів, які мають до неї відношення є одним і тим же; банківська таємниця не є різновидом інших таємниць, а становить самостійний вид таємної інформації; інформація, що становить банківську таємницю торкається насамперед клієнтів банків, причому режимом таємності охоплюються відомості, які банки отримують від своїх клієнтів офіційно, в процесі безпосереднього здійснення своєї діяльності. Слід також зазначити, що інформацію про клієнта банк може отримати як безпосередньо від нього, так і інших (третіх) осіб, з якими банк вступає у взаємовідносини, при наданні банківських послуг. Інформація, яка становить банківську таємницю може міститись в документах, що характеризують взаємовідносин банку і клієнта,

документах, що характеризують самого клієнта і його діяльність, а також документах банку, що характеризують самого клієнта і його діяльність.

За посягання на банківську та комерційну таємницю законодавство України передбачає дисциплінарну, кримінальну, адміністративну та цивільну відповідальність.

Тут слід виділити дві основні групи суб'єктів посягань на таку інформацію. Особи, що незаконно заволоділи інформацією банку та особи, що правомірно отримали таку інформацію, але порушили зобов'язання щодо збереження її в таємниці (працівники, контрагенти, партнери, клієнти, державні службовці).

Кримінальна відповідальність передбачена за умисні дії, які спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності.

Крім того, кримінальна відповідальність наступає також за умисне розголошення комерційної або банківської таємниці, без згоди її власника, особою, якій ця таємниця відома, у зв'язку з професійною або службовою діяльністю якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності.

Адміністративна відповідальність може наступати у разі отримання, використання, розголошення комерційної таємниці, з метою заподіяння шкоди діловій репутації або майну конкурента.

Цивільний кодекс України відносить інформацію до об'єктів цивільних прав і визначає, що суб'єкт відносин у сфері інформації може вимагати усунення порушень його права та відшкодування майнової і моральної шкоди, завданої такими правопорушеннями.

Враховуючи особливий статус та значний обсяг електронної інформації в діяльності суб'єктів підприємництва законодавець передбачив відповідні правові умови відносин у сфері такої інформації. Основним правовим

документом тут є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Згідно закону основним об'єктом захисту виступають: інформація, що використовується в інформаційно-телекомунікаційних системах та програмне забезпечення, яке використовується для обробки інформації суб'єктами відносин є: власники інформації, власники систем, користувачі, уповноважений орган виконавчої влади з питань організації спецзв'язку та захисту інформації. Взаємовідносини суб'єктів здійснюється на договірних засадах. Порядок доступу до інформації, що оброблюється в системі, перелік користувачів та їх повноваження визначає власник інформації. У випадках коли в системах оброблюється інформація з обмеженим доступом, доступ до неї визначається законодавством. Положеннями закону врегульовано відносини поміж власниками інформації і власниками інформаційно-телекомунікаційних систем, між власниками різних систем, власниками систем і користувачами. Організація захисту інформації, що оброблюється у системах покладається на власників систем. За порушення порядку і правил захисту інформації, що оброблюється в інформаційно-телекомунікаційних системах може наступати адміністративна та кримінальна відповідальність.

Документообіг в електронному інформаційному просторі на сьогоднішній час є одним із елементів документування підприємницької діяльності. Безумовно, що він має бути в правовому плані врегульованим і захищеним. Це питання регулюється двома законодавчими актами: Закони України «Про електронні документи та електронний документообіг» і «Про електронний цифровий підпис», а також Положеннями «Про технічний захист інформації в Україні» і «Про порядок здійснення криптографічного захисту інформації в Україні» [48, 49, 50, 51]. Зазначені правові норми визначають організаційно-правові засади електронного документообігу, використання електронних документів, правовий статус електронного підпису та регулювання відносин, що виникають при його використанні. Зокрема, в законодавчих актах надається поняття електронного документу та наголошується на його юридичному статусі

(документ не може бути заперечений через те, що він має електронну форму). Крім того, регулюються питання обігу документів, які містять інформацію з обмеженим доступом та їх особливого захисту в електронних мережах і носіях. Також встановлюється, що електронний підпис є обов'язковим реквізитом електронного документу: за своїм правовим статусом прирівнюється до власноручного підпису (печатки) за умов передбачених Законом України «Про електронний цифровий підпис».

Вказані вище Положення визначають порядок технічного захисту інформації та виконання криптографічного захисту інформації з обмеженим доступом.

Організовуючи забезпечення інформаційної безпеки суб'єктів підприємництва у стосунках з представниками засобів масової інформації необхідно досить грамотно орієнтуватись у законодавстві та правових актах, що регулюють діяльність суб'єктів масової інформації. Зокрема доцільним буде ознайомлення з положеннями наступних правових актів: Законів України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про інформацію», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення і радіомовлення», «Про інформаційні агентства», «Про авторське право і суміжні права», «Про державну підтримку засобів масової інформації та соціальний захист журналістів», «Про захист суспільної моралі». Крім того, не зайвим буде ознайомитись з Кодексом професійної етики українського журналіста.

Враховуючи, що діяльність з забезпечення інформаційної безпеки суб'єктів підприємництва зазвичай передбачає взаємовідносини з правоохоронними та судовими органами, органами контролю та нагляду, які керуються спеціальними законодавчими актами, що регулюють їх діяльність, доцільним також буде ознайомлення з правами таких органів в інформаційній сфері. Насамперед положеннями Законів України «Про прокуратуру», «Про міліцію», «Про службу безпеки України», «Про оперативно розшукову

діяльність», «Про організаційні основи боротьби з організованою злочинністю», «Про судоустрій та статус судів», «Про адвокатуру та адвокатську діяльність», «Про державну контрольно-ревізійну службу в Україні», «Про Національний банк України», «Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживання ними», а також Податкового кодексу України та іншими положеннями правових актів, що регулюють діяльність зазначених органів.

Питання правового регулювання інформаційної безпеки суб'єктів підприємництва не буде повним без нормативно-правових документів самих суб'єктів. Саме такі нормативно-правові документи, базуючись на положеннях законодавчих та підзаконних актів утворюють правові підстави та регулюють діяльність суб'єктів щодо встановлення відповідного інформаційного режиму їх інформаційних відносин з іншими суб'єктами, контрагентами, клієнтами, кредиторами і мають певне значення для взаємостосунків з державними органами. Якраз в таких документах обґрунтовується поведінка суб'єктів підприємництва в їх інформаційному просторі за різних умов. На жаль на сьогодні, як і взагалі у сфері інформаційної безпеки суб'єктів підприємництва, так і в питаннях правового її регулювання нормативно-правовими документами самих суб'єктів стійкої позиції немає. Беручи до уваги мету, завдання та зміст інформаційної безпеки суб'єктів підприємництва, структуру процесу її організації та напрацьований досвід, можна рекомендувати наступний перелік таких нормативно-правових документів: Положення про комерційну таємницю та правила її зберігання на підприємстві (у банку); Положення про конфіденційну інформацію підприємства (банку); Інструкція про порядок підготовки, обліку, зберігання та знищення документів, справ, видань і матеріалів, що містять комерційну таємницю та конфіденційну інформацію підприємства (банку); Положення про захист електронної інформації та електронних документів на підприємстві (у банках питання захисту електронної інформації здійснюється відповідно до нормативно-правових документів НБУ); Інструкція про порядок виконання документів, що надходять до підприємства

(банку) від правоохоронних органів, судів та інших державних установ; Положення про архів і архівну діяльність підприємства (банку); Інструкція про проведення службових розслідувань на підприємстві (у банку); Положення про інформаційно-аналітичну роботу на підприємстві (у банку); Інструкція з службового діловодства; Інструкція з спеціального діловодства; Правила використання, поширення та зберігання інформації підприємства (банку) у процесі його діяльності; Методики розробки інформаційних документів підприємства (банку) та надання інформаційних послуг; Пам'ятки працівникам підприємства, банку по збереженню інформації з обмеженим доступом; інші документи [52, 53, 54]. Незважаючи на значний перелік документів, всі вони утворюють правове поле суб'єкта підприємництва у сфері забезпечення його інформаційної безпеки, обґрунтовують поведінку суб'єкта у інформаційному середовищі.

6. Захист інформації в діяльності суб'єктів підприємництва

У вирішенні проблем інформаційної безпеки суб'єктів підприємництва важливе місце займає захист їх інформації. Це питання пов'язане не лише з недопущенням втрати чи знищення інформації або ж її модифікації. Тут важливим є встановлення безпечного режиму її функціонування у процесі діяльності суб'єктів підприємництва, регламентованого доступу до неї. Суттєве значення має налагодження безпечних стосунків з т. з. захисту інформації суб'єктів підприємництва з їх партнерами, контрагентами, клієнтами. Крім того, важливим є захист інформації у процесі офісної роботи особливо цінних виробничих і комерційних інформаційних ресурсів при їх формуванні, обробці, зберіганні і використанні. В останньому аспекті значне місце у захисті інформації займає правильна організація роботи персоналу з інформацією суб'єктів підприємництва і її носіями. Багато фахівців з інформаційної безпеки вважають, що при грамотній організації роботи з персоналом захист інформації забезпечується не менше ніж на 80% [38]. В той же час, захист інформації є складовим елементом інформаційної безпеки суб'єктів підприємництва, ефективне забезпечення якого формує відповідний рівень самої безпеки.

6.1. Інформація з обмеженим доступом в підприємницькій діяльності

Як уже було попередньо розглянуто, в діяльності суб'єктів підприємництва використовується зазвичай два види інформації: відкрита і таємна. Остання – це насамперед банківська і комерційна таємниця, а також конфіденційна інформація. Тому важливим моментом у захисті інформації буде виступати порядок виділення такої інформації як окремого об'єкту захисту. Відповідно до Закону України «Про інформацію» під інформацією розуміються документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому

природньому середовищі. Цивільний Кодекс України уточнює, що події та явища про які іде мова у визначенні змісту зазначеного поняття повинні обов'язково мати місце (зараз чи в минулому) у суспільстві… і т. д. Водночас дещо відмінене визначення поняття «інформація» дає Закон України «Про захист економічної конкуренції» згідно якого інформація - це відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості [55]. Тобто, можна бачити, що зазначені правові норми вказують, що інформацією є документовані чи оголошені відомості, які можуть міститись на різноманітних носіях. Таким чином, захисту мають підлягати відомості, які є у розпорядженні суб'єкта підприємництва і які відтворюють (характеризують) події та явища (діяльність), що відбуваються у нього.

Розглядаючи питання обмеження доступу як способу захисту інформації, слід звернути особливу увагу на те, як законодавець регулює право власника інформації на її захист. Як уже зазначалось, відповідно до вітчизняного законодавства громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаної за власні кошти, або таку, що є предметом їх ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної та встановлюють до неї систему (способи) захисту. Тобто, право встановлювати відповідний режим доступу до інформації мають особи (юридичні та фізичні), які володіють інформацією. За таких умов суб'єкти підприємництва мають право обмежувати доступ до власної інформації, в тому числі і щодо якої вони стали володільцями в результаті її придбання або, яка не є їх

власністю, але є предметом їх інтересу (будь-які відомості отримані суб'єктом підприємництва в результаті проведення заходів інформаційного забезпечення його діяльності).

Безумовно, що головну увагу суб'єкти підприємництва приділяють інформації з обмеженим доступом, тому саме ця інформація в їх діяльності є головним об'єктом захисту.

Найбільш важливе місце в системі захисту інформації займає таємна інформація, а саме банківська та комерційна таємниця. Як було зазначено в розділі 5, законодавець встановив вичерпний зміст та перелік відомостей, що становлять банківську таємницю.

Встановивши такий перелік законодавець разом з тим поклав на банки певні обов'язки щодо організації її захисту. Так, відповідно до ст. 61 Закону України «Про банки і банківську діяльність» банки зобов'язані:

- обмежувати коло осіб, що мають доступ до інформації, яка становить банківську таємницю;
- організовувати спеціальне діловодство з документами, що містять банківську таємницю;
- застосовувати технічні засоби для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;
- застосовувати застереження щодо збереження банківської таємниці та відповідальність за її розголошення у договорах і угодах між банком і клієнтом.

Крім того, керівники та службовці банків зобов'язані не розголошувати та не використовувати з вигодою для себе чи третіх осіб конфіденційну інформацію, яка стала їм відома при виконанні службових обов'язків. Це ж стосується і приватних осіб, які при виконанні своїх функцій або наданні послуг банку отримали доступ до конфіденційної інформації.

Забезпечуючи захист банківської таємниці законодавець встановив і особливий порядок розкриття відомостей, які становлять таку таємницю (про що вже йшла мова у розділі 5.)

Крім того, банк має право надавати інформацію, що становить банківську таємницю, іншим банкам та Національному банку України в обсягах необхідних при наданні кредитів, банківських гарантій; особі (в тому числі яка уповноважена діяти від імені держави), на користь якої відчужуються активи та зобов'язання банку, при виконанні заходів, передбачених програмою фінансового оздоровлення банку, або під час здійснення процедури ліквідації.

Законодавець не поширює обмеження щодо розкриття банківської таємниці на службовців Національного банку України чи уповноважених ними осіб, які здійснюють функції банківського нагляду або валютного контролю. Разом з тим, Національний банк України має право розкривати інформацію, що містить банківську таємницю банків Міністерству фінансів України у разі, коли держава бере участь у капіталізації цих банків.

Розкриття інформації, яка становить банківську таємницю здійснюється виключно за письмовими запитами. Щодо державних органів законодавець встановив, що такий запит має бути оформлено у вигляді письмової вимоги:

- має бути викладена на бланку державного органу встановленої форми;
- бути підписаним керівником державного органу (чи його заступником) та скріплена гербовою печаткою;
- має містити передбачені Законом України «Про банки і банківську діяльність» підстави для отримання інформації;
- має містити посилання на норми закону, відповідно до яких державний орган має право на отримання такої інформації.

Виїмка документів, які містять інформацію, що становить банківську таємницю, проводиться лише за вмотивованою постановою судді в порядку передбаченому Кримінально-процесуальним кодексом України. У цьому випадку банк зобов'язаний виготовити копії документів, які підлягають виїмці. Зазначені копії разом з другим примірником протоколу виїмки залишаються в банку.

Відповідно до вимог Національного банку України банки зобов'язані за погодженням з клієнтом відображати в договорах, що укладаються між ними, застереження щодо збереження банківської таємниці та відповідальності за її незаконне розголошення або використання.

Суб'єкти, які мають доступ до банківської таємниці, в тому числі і банки в своїх нормативних документах повинні встановити особливий порядок реєстрації, використання, зберігання та доступу до документів (в тому чисті і електронних), що містять банківську таємницю.

Характеризуючи інформацію з обмеженим доступом слід звернути увагу на те, що суб'єкти підприємництва як юридичні особи, які здійснюють господарську діяльність виробляють свою власну інформацію, що може бути для них досить важливою та цінною. При розробці нових технологій виробництва, нової продукції, плануванні розвитку, створюються насичені різноманітними відомостями інформаційні об'єкти, які вимагають надійного захисту. Тому суб'єкти підприємництва мають захищати такі об'єкти шляхом надання їм категорії комерційної таємниці.

Тут слід пам'ятати, що відповідно до цивільного законодавства основними ознаками комерційної таємниці є: комерційна цінність інформації, інформація має бути невідомою третім особам і до неї немає вільного доступу, володілець інформації має вживати відповідних заходів для її охорони і таємності, інформація не може бути об'єктом інших таємниць.

Враховуючи, що суб'єкти підприємництва, як власники інформації самостійно визначають зміст своїх таємниць, значення набуває процес формування переліку відомостей, що становлять комерційну таємницю. З одного боку зазначений перелік повинен надійно захищати цінну для суб'єктів інформацію, а з іншого не обмежувати їх інформаційну діяльність на ринку. Вітчизняний досвід діяльності суб'єктів підприємництва має певні приклади організації роботи по визначенню відомостей, що становлять комерційну таємницю, узагальнення якої дало можливість сформувати наступний варіант формування переліку відомостей, що становлять

комерційну таємницю підприємництва, фірми, банку.

Відповідним наказом керівника суб'єкта підприємництва визначається комісія на яку покладається завдання складання переліку відомостей, що становлять комерційну таємницю. Разом з тим, зазначеним наказом керівники всіх підрозділів і установ суб'єкта підприємництва зобов'язуються виокремити відомості по своїх напрямках роботи, які з їх погляду вимагають обмеження доступу до них шляхом надання їм категорії комерційної таємниці. Пропозиції підрозділів надходять до зазначеної вище комісії, яка їх обробляє, перевіряє щодо відповідності вимогам чинного законодавства, формує і узгоджує в підрозділах остаточний проект переліку таких відомостей. Зазначений перелік надається керівнику суб'єкта підприємництва, який відповідним наказом вводить його в дію. Одночасно в наказі визначаються особи, яким інформація, що складає комерційну таємницю може розкриватись в повному обсязі. Крім того, цим же наказом визначаються завдання щодо заходів захисту комерційної таємниці.

Конфіденційна інформація суб'єктів підприємництва як вид інформації з обмеженим доступом може мати подвійний характер. З одного боку це інформація власниками якої є суб'єкти підприємництва і яка з тих чи інших причин не отримала категорії таємної та інформація про персонал яка зберігається в особових справах та документах про оплату праці. Якщо перелік відомостей, що становить конфіденційну інформацію суб'єктів підприємництва визначається в тому ж порядку, що і для комерційної таємниці, то зміст конфіденційної інформації про працівників подається у Законі України «Про інформацію» та забезпечується відповідно до Закону України «Про захист персональних даних». Суб'єкти підприємництва зобов'язані забезпечити конфіденційність таких даних, зібраних на своїх працівників при прийомі та у ході їх роботи.

Одним із заходів захисту інформації з обмеженим доступом, яку мають передбачити суб'єкти підприємництва є встановлення дисциплінарної відповідальності їх працівників за порушення правил роботи з такою

інформацією. Тут слід зазначити, що притягнення до дисциплінарної відповідальності працівників може відбуватись: а) якщо ними порушено вимоги Посадової інструкції, якою передбачено обов'язок працівника зберігати, не розголошувати, не використовувати на власний розсуд і т. і. певні відомості; б) якщо в нормативних документах, що регулюють відповідні технології виробництва і якими має керуватись працівник, вказано правила поводження з інформацією, а він їх порушує; в) якщо подібні правила передбачено в умовах трудового договору. Так, при укладанні трудового договору згідно ст. 21 Кодексу законів про працю України працівник зобов'язується виконувати умови внутрішнього трудового розпорядку, однією з вимог якого може бути зберігання в таємниці певної інформації. Крім того, може бути передбачено також укладання окремої угоди про конфіденційність. Разом з тим, необхідно зауважити, що притягнення працівників до відповідальності за посягання на інформацію чи порушення правил поводження з нею має здійснюватись за певним порядком. Як правило, прийняттю рішення про притягнення працівника до відповідальності має передувати проведення службового розслідування, метою якого є встановлення обставин, умов і причин виявлення фактів посягання на інформацію суб'єкта підприємництва, встановлення осіб безпосередньо причетних до цього, з вини або за сприяння яких мали місце такі факти, вироблення пропозицій і рекомендацій щодо усунення причин і недоліків у роботі установ суб'єкта підприємництва та пропозицій по відшкодуванню понесених збитків, а також притягнення до відповідальності осіб, які спричинили або сприяли витоку (втраті, знищенню, зміні) інформації.

Службові розслідування проводяться у разі виявлення фактів несанкціонованого витоку інформації з обмеженим доступом суб'єкта підприємництва внаслідок чого йому заподіяно матеріальної шкоди або це вплинуло на погіршення його іміджу.

Рішення про проведення службового розслідування приймається

керівником установи суб’єкта підприємництва.

Найчастіше службові розслідування проводяться фахівцями служби безпеки, а при відсутності таких фахівців спеціально призначеними керівником установи особами. Коли для проведення службового розслідування необхідно залучити фахівців інших підрозділів можуть створюватися відповідні комісії.

До участі у проведенні службового розслідування не повинні залучатись посадові особи, якщо мають місце обставини, які можуть викликати їх особисту зацікавленість у результатах розслідування.

При проведенні службових розслідувань особи, які залучені до цього, мають право:

- отримувати від працівників установ суб’єкта підприємництва усні та письмові пояснення щодо факту, який розслідується, а також консультації фахівців суб’єктів з питань службового розслідування;
- вивчати відповідні документи як у паперовому, так і в електронному вигляді, знімати з них копії та отримувати необхідні пояснення по них. У випадках коли документи містять інформацію з обмеженим доступом, справи, що ведуться у зв’язку з службовим розслідуванням, повинні мати гриф не нижче, ніж на документах, з яких отримана інформація;
- збирати з дотриманням вимог законодавства інформацію, необхідну для встановлення об’єктивної суті подій, фактів, випадків, осіб, причетних до них, робити відповідні запити до підрозділів і установ суб’єктів підприємництва

В окремих випадках фахівці або голова комісії можуть отримувати роз’яснення у посадових осіб та керівництва установ суб’єктів.

З дозволу керівника установи фахівцями (комісіями), які проводять службове розслідування, можуть подаватись запити до інших установ, організацій та правоохоронних органів.

Особи, які проводять службове розслідування несуть персональну відповідальність згідно з чинним законодавством за повноту та об'єктивність висновків, зроблених ними за результатами розслідування, розголошення інформації, отриманої у ході розслідування.

Фахівці (члени комісії), які проводять службове розслідування, забезпечуються необхідними для роботи документами, програмно-апаратним, технічними засобами, автотранспортом та іншим обладнанням і технікою.

Працівники суб'єктів підприємництва зобов'язані надавати їм допомогу у встановленні причин та умов виникнення фактів, за якими проводиться службове розслідування, давати пояснення, інформацію та консультації стосовно питань розслідувань.

За результатами службового розслідування складається акт або доповідна записка, де зазначається:

- суть та обставини, що характеризують факти, випадки, за якими проводиться розслідування, учасники та їх дії, у тому числі такі, що суперечать встановленим правилам, посадовим обов'язкам, нормативно-правовим документам, які діють в установах суб'єктів підприємництва умови, що сприяли скоєнню порушень або іншим діям;
- характеристика шкоди, заподіяної суб'єктам підприємництва, прогноз її впливу на їх подальшу діяльність;
- причини, що призвели до таких фактів та особи, з вини яких допущено ці факти;
- заходи щодо відшкодування заподіяної шкоди, захисту честі та гідності посадових осіб, пропозиції щодо усунення причин та умов, що сприяли виникненню фактів, за якими проводиться службове розслідування, покарання винних, рекомендації з профілактики та недопущення подібних випадків.

Посадова особа, яка призначила службове розслідування у 10-денний термін розглядає акт або доповідну записку та приймає відповідне рішення. У разі необхідності така посадова особа може заслухати особу, яка

проводила службову розслідування, або членів комісії, а також осіб, з вини яких допущено те чи інше порушення.

Матеріали службового розслідування є підставою для прийняття керівником установи рішення про притягнення винних осіб до дисциплінарної або іншої відповідальності згідно чинного законодавства.

В певних випадках за рішенням керівника може бути ініційовано подання матеріалів до правоохоронних органів, суду, Антимонопольного комітету України тощо.

6.2. Система захисту інформації суб'єктів підприємництва

З інформаційної точки зору суб'єкт підприємництва являє собою комплекс компонентів, пов'язаних між собою єдиною метою, структурними відносинами, технологіями інформаційного обміну. Зазначені компоненти в процесі функціонування суб'єкта можуть змінюватись, на них можуть здійснювати вплив різного роду внутрішні та зовнішні чинники, які складно прогнозувати та оцінювати. Всі компоненти можна сформувати у чотири групи: персонал, технічні засоби інформатизації, програмне забезпечення, документи і вважати як об'єкти захисту інформації. Зазначені групи у своєму функціонуванні зазнають впливу різного роду специфічних факторів і взаємодіючи між собою впливають один на одного, формуючи відповідний стан інформаційної безпеки суб'єкта підприємництва. Як показує практика, робота з кожною з цих груп щодо забезпечення інформаційної безпеки чи зокрема захисту інформації призводить до покращення якостей безпеки по одних параметрах і погіршення по інших, що вимагає комплексного підходу до забезпечення інформаційної безпеки.

Висока інформатизація та автоматизація виробничого процесу суб'єктів підприємництва не виключає звичайних взаємовідносин їх персоналу з контрагентами та клієнтами, а значні обсяги електронних документів аж ніяк не призводять до зменшення документообігу паперових

носіїв інформації. Тобто забезпечення інформаційної безпеки і такої її складової як захист інформації неможливо здійснити лише організаційними чи технічними заходами, або скажімо програмними чи криптографічними. Дії по забезпеченню інформаційної безпеки повинні являти собою регулярний процес, що здійснюється на всіх напрямках діяльності суб'єкта підприємництва на основі комплексного застосування всіх заходів і засобів безпеки. При цьому засоби, заходи та методи безпеки найбільш раціональним способом об'єднуються в єдиний цілісний механізм не тільки для захисту від зловмисників, але і від некомпетентних, недобросовісних працівників та різних непередбачуваних ситуацій. Тобто, забезпечення інформаційної безпеки як має носити системний та комплексний характер. Системність заходів інформаційної безпеки суб'єктів підприємництва має передбачати наступне:

- високий ступінь захищеності їх інформації як головну характеристику її якісного стану;
- заходами безпеки охоплюються всі інформаційні ресурси суб'єктів підприємництва;
- діяльність по забезпеченню інформаційної безпеки є безперервною і плановою, на основі єдиної концепції безпеки;
- забезпечення інформаційної безпеки здійснюється у тісній єдності з поточною діяльністю суб'єктів підприємництва.

Комплексний характер системи забезпечує оптимізацію заходів та засобів, що використовуються нею задля створення необхідного балансу вимог і можливостей інформаційної безпеки. Комплексний підхід обумовлюється ще і тим, що загрози інформації суб'єктів підприємництва носять різноманітний характер, перекриття яких вимагає застосування багатьох, різних за призначенням заходів і засобів. Крім того, значний спектр різного роду операцій, велика регіональна розпорошеність установ, специфічність поведінки персоналу, контрагентів, суб'єктів підприємництва та клієнтів створюють суттєві особливості їх діяльності і вимагають адекватної реакції

систем безпеки. Водночас адекватність реакції передбачає узгоджені дії всіх сил та засобів безпеки, що можливо лише при системному підході. Більш того, забезпечення безпеки в сучасних умовах має здійснюватись як на технологічному, так і на логічному рівнях, що має забезпечувати врахування всіх факторів і особливостей, які впливають на безпеку суб'єктів підприємництва, а також всіх компонентів інформаційної роботи: збору, обробки, зберігання, передавання, використання інформації. За таких умов системність та комплексність інформаційної безпеки, в тому числі і у сфері захисту інформації є обов'язковою умовою її високої ефективності.

Система захисту інформації суб'єкта підприємництва — це організована сукупність об'єктів і суб'єктів захисту інформації, заходів, методів, засобів та технологій, що використовуються для захисту його інформаційних ресурсів. Основна мета створення системи захисту інформації - забезпечення надійного зберігання і ефективного використання інформації в діяльності суб'єктів підприємництва.

Враховуючи складність структури системи захисту інформації та необхідність її функціонування в умовах невизначеності, побудова такої системи має базуватись на відповідних принципах.

Принцип повноти інформації, що захищається обумовлює необхідність захисту не тільки інформації з обмеженим доступом, а і іншої інформації, втрата якої може нанести шкоди суб'єкту підприємництва. Реалізація даного принципу дозволяє забезпечувати захист всіх об'єктів інтелектуальної власності суб'єкта підприємництва.

Відповідно до принципу обґрунтованості захисту інформації визначається доцільність надання відповідного грифу певним відомостям, виявляються економічні та інші наслідки, що можуть наступати від застосування заходів захисту інформації. Це в свою чергу дозволить більш раціонально та продуктивно здійснювати витрати на захист інформації.

Принципи повної участі та персональної відповідальності передбачають поширення обов'язку захищати інформацію на всіх осіб, що працюють з

інформаційними продуктами (програмами, документами, характеристиками і т. і.) суб'єкта підприємництва , а також вимагають відповідальності кожного із його працівників чи інших осіб за порушення заходів захисту інформації.

Принцип превентивності передбачає плановість заходів захисту інформації, застосування їх з метою виявлення, перетинання та локалізації загроз інформації суб'єкта підприємництва.

Важливе значення у захисті інформації має політика інформаційної безпеки суб'єкта підприємництва. Політика інформаційної безпеки — це прийнята у суб'єкта підприємництва сукупність норм, правил, рекомендацій згідно яких будується система його інформаційної безпеки та управління нею. Вона реалізується за допомогою організаційних заходів і програмно-технічних засобів, які визначають архітектуру системи захисту та за допомогою засобів управління механізмами захисту. Для кожного суб'єкта підприємництва політика безпеки є індивідуальною і залежить від особливостей технологій його виробничої та комерційної діяльності, його відносин та умов функціонування на ринку.

Відповідно до прийнятої політики інформаційної безпеки проводяться організаційні заходи по створенню системи захисту інформації. В даний час суб'єктами підприємництва напрацьовано відповідний алгоритм роботи по організації системи захисту інформації, який включає наступні дії:

- визначення вразливості інформації суб'єкта підприємництва (виявлення в інформаційній системі суб'єкта місць, використання зловмисниками яких може нанести шкоди інформаційним ресурсам і в цілому суб'єкту підприємництва);
- визначення мети, завдань та об'єктів захисту інформації;
- вибір форм, способів та засобів захисту інформації;
- формування елементів системи захисту інформації, її сил та засобів;
- створення нормативної бази суб'єкта з питань захисту інформації;

- планування функціонування системи, використання нею сил та засобів захисту інформації у відповідності до особливостей діяльності суб'єкта підприємництва;
- забезпечення взаємодії всіх елементів системи між собою та з іншими компонентами, які згідно політики інформаційної безпеки можуть бути задіяні для захисту інформації;
- забезпечення функціонування системи (матеріальне, фінансове, наукове та ін.);
- контроль стану захищеності інформації, надійності функціонування системи та ефективності заходів, що вживаються нею.

Вразливість інформації є одним із головних показників стану її захищеності. Тому визначення ступеня вразливості інформації у ході організації її захисту має досить суттєве значення. Зміст роботи по визначенню вразливості інформації показано на рис.6.1.

Результати, отримані в ході визначення вразливості інформації, використовуються для встановлення складу інформації, яка підлягає безпосередньому захисту, тобто об'єктів захисту. Загальний підхід тут полягає у тому, що захисту підлягає вся інформація з обмеженим доступом і найбільш важлива частина відкритої інформації. При цьому інформація з обмеженим доступом повинна захищатись від втрати і несанкціонованого витоку, а відкрита – тільки від втрати.

За деякою практикою суб'єкти підприємництва не передбачають захисту відкритої інформації. Але ж відкритість інформації не лишає її цінності, а цінна інформація безумовно має захищатись, насамперед від втрати її. Захист такої інформації здійснюється шляхом реєстрації її носіїв, обліку, контролю наявності. Разом з тим, захист відкритої інформації не повинен обмежувати її загальнодоступності, але доступ до неї має бути контрольованим, з дотриманням відповідних вимог щодо її збереження. Тобто, відкрита інформація є об'єктом захисту і стосовно неї повинні проводитись певні

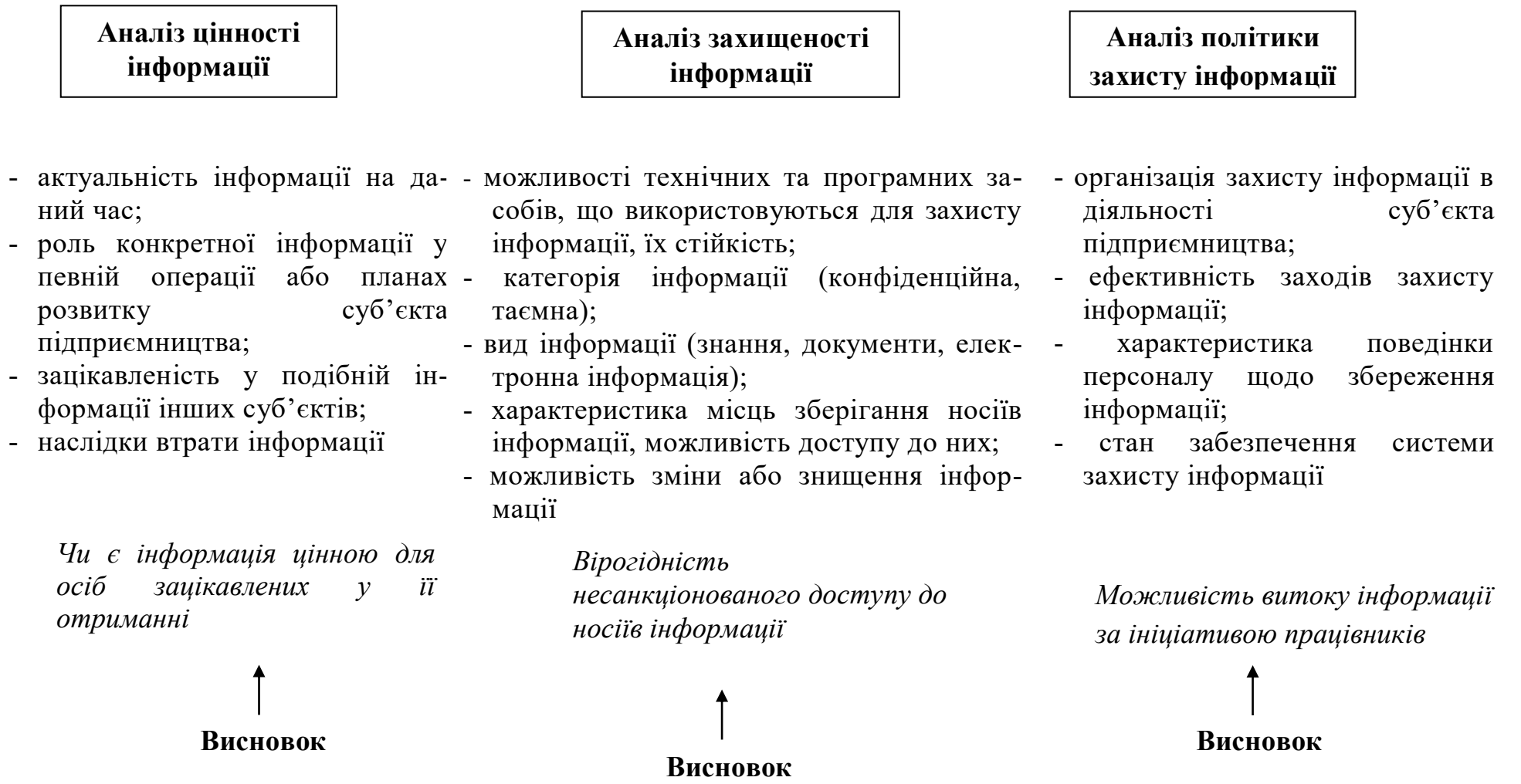


Рис. 6.1. Визначення уразливості інформації з обмеженим доступом в діяльності суб'єкта підприємництва

заходи в системі захисту інформації. Загальною ж основою для вибору об'єкту захисту є цінність інформації

Критеріями цінності можуть бути: необхідність інформації для правового забезпечення діяльності суб'єкта підприємництва; необхідність інформації для здійснення виробничої діяльності; необхідність інформації для ефективного управління діяльністю суб'єкта підприємництва, об'єктивного прийняття управлінських рішень, організації прибуткової його діяльності; необхідність інформації для формування ресурсної бази суб'єкта підприємництва та забезпечення його безпеки. Разом з тим основним і визначальним критерієм у виборі об'єкта захисту інформації є можливість отримання від використання певної інформації переваг за рахунок її невідомості третім особам. Критерій має дві складові: невідомість інформації для третіх осіб і отримання вигоди в силу цієї невідомості.

Водночас система захисту інформації суб'єкта підприємництва *у* своєму функціонуванні носить конкретний характер і вимагає однозначної конкретизації об'єктів захисту. Інформація, на яку спрямовуються зусилля системи захисту не існує сама по собі, а фіксується (відображається) у відповідних матеріальних об'єктах або пам'яті людей, тобто вона існує на відповідних носіях. Таким чином, обираючи об'єкт захисту ми маємо визначити певний перелік носіїв невідомої третім особам інформації за рахунок якої суб'єкт отримує певні переваги у своїй діяльності. Тобто, це можуть бути відповідні документи, матеріали (в тому числі магнітні, магнітооптичні, оптичні та інші засоби), вироби (засоби відображення, обробки, відновлення, передачі інформації), мережі зв'язку та передачі даних, а також працівники суб'єкта. Захист цих об'єктів має здійснюватись шляхом регулювання доступу до них, встановлення відповідного порядку їх використання (діяльності) та формування умов зберігання. Якраз ці заходи і складають структуру системи захисту інформації.

Зазначені заходи в системі захисту інформації здійснюється за

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

Враховуючи різноманітність загроз інформації суб'єктів підприємництва та необхідність найбільш ефективного її захисту, система має виконувати відповідний комплекс завдань орієнтований на використання всіх можливих засобів. Зміст таких завдань у їх комплексі запропоновано на Рис. 6.2.

Особливим об'єктом захисту інформації в діяльності суб'єктів підприємництва є персонал, в пам'яті якого зосереджено величезні масиви інформації, в тому числі і такої, що є крайнє цінною для суб'єктів.

У цьому сенсі працівники суб'єктів підприємництва як носії інформації характеризуються з точки зору її захисту позитивними та негативними рисами. Позитивним є те, що без згоди суб'єктів із пам'яті працівників ніяка інформація ні за яких умов не може бути вилучена, працівники можуть об'єктивно оцінювати важливість інформації, якою володіють і відповідно до цього ставитись до неї, а також ранжувати споживачів їхньої інформації, знаючи кому і яку інформацію можна довірити.

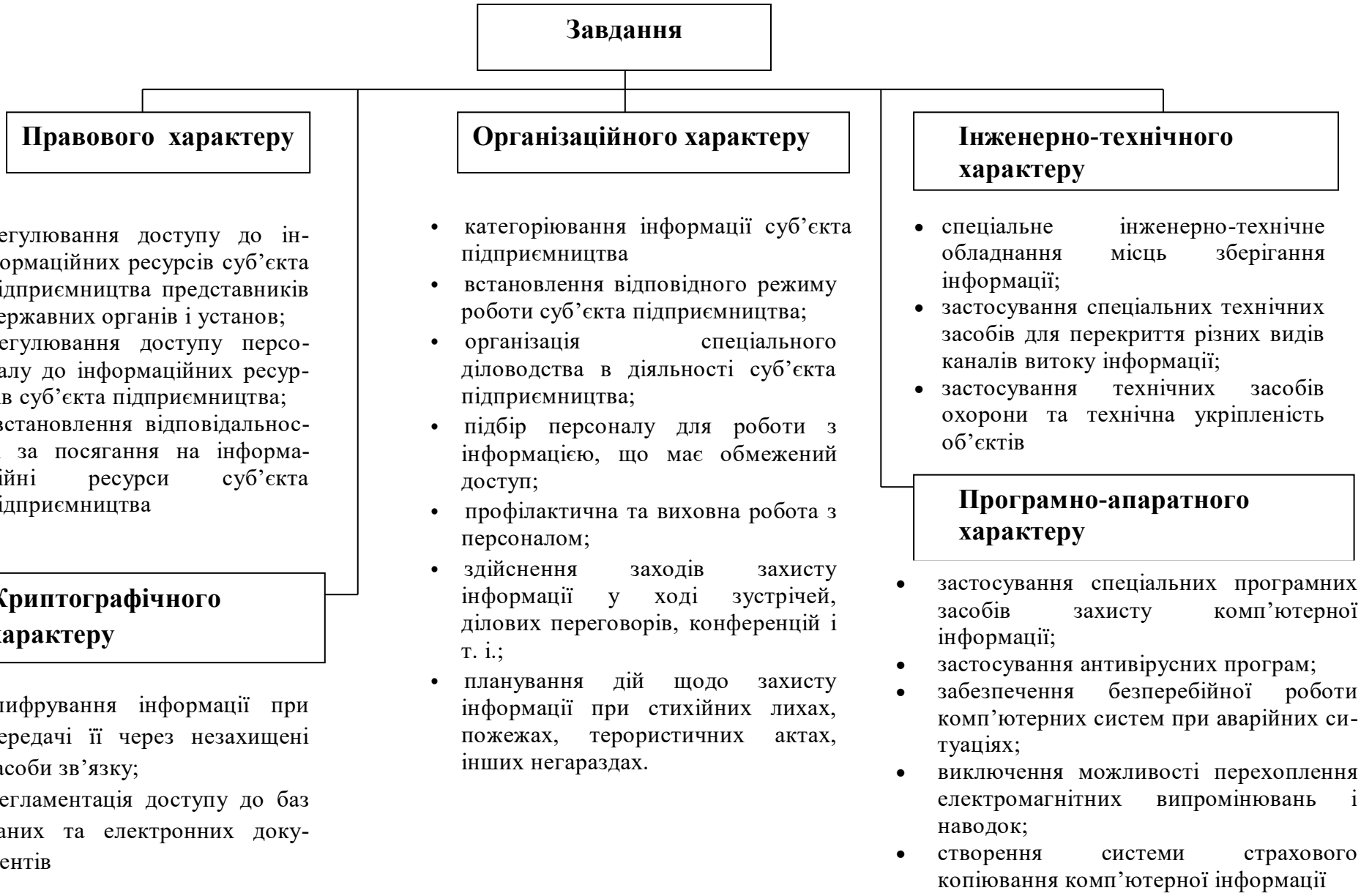


Рис. 6.2. Зміст завдань системи захисту інформації

Негативним є те, що працівники можуть помилятись в щирості таких споживачів, бути не повністю компетентним у важливості інформації, якою володіють, їх дії багато в чому залежать від емоційного стану, характеру, власних потреб.

За таких умов система захисту інформації щодо об'єкту захисту такого як працівники має вживати заходи регламентування роботи працівників з інформацією, встановлювати відповідні обмеження та заборони, а також певним чином мотивувати поведінку працівників до дотримання встановленого режиму захисту інформації.

Регламентування роботи працівників з інформацією здійснюється шляхом:

- визначення осіб, яким надано право доступу до інформації повному обсязі;
- визначення осіб, яким надано право доступу до інформації суб'єкта підприємництва в частині, що їх стосується;
- встановлення порядку доступу до інформації суб'єкта підприємництва та повноважень осіб щодо її використання;
- визначення порядку та правил використання носіїв інформації в процесі діяльності суб'єкта підприємництва;
- визначення порядку та правил зберігання інформації, вироблення, обліку та пересилання електронних та паперових документів.

Заборони та обмеження досягаються виключенням фізичної та іншої можливості доступу до інформації, яка згідно повноважень працівника йому не повинна доводитись. Крім того, обмеження доступу здійснюється і шляхом виконання певних завдань чи робіт по окремих частках групою працівників, кожен з якої не обізнаний із змістом інформації, яка повністю характеризує завдання (обсяг роботи).

Мотивації у забезпеченні захисту інформації, якою володіють праців-

ники формуються через зацікавленість працівників у виконанні ними заходів захисту. Основними методами тут виступають: формування у працівників фірмового патріотизму; матеріальна та кар'єрна вигода дотримання заходів захисту; відповідне відношенні колективу до осіб, що порушують встановлені правила захисту інформації; зручність виконання зазначених заходів і т. і.

Важливе значення мають заходи протидії попадання працівників під вплив осіб, зацікавлених в отриманні інформації суб'єктів підприємництва (конкурентів, промислових шпигунів і т. д.). Як правило, підрозділи безпеки суб'єктів підприємництва розробляють відповідні методики роботи з персоналом щодо протидії витоку інформації, якою володіють працівники. Зазвичай до змісту таких методик включаються наступні питання:

- визначення готовності кандидатів на роботу та працівників до зрадництва, легкої наживи, аморальної поведінки;
- формування сприятливих умов роботи кожному із працівників;
- формування умов та можливостей максимального заробітку та кар'єри;
- вжиття заходів гарантованого захисту інформаційних об'єктів та регламентування доступу до джерел інформації;
- встановлення відповідальності за посягання на інформацію суб'єктів підприємництва;
- пропаганда захисту таємниць суб'єктів підприємництва як однієї із умов ефективного їх розвитку та забезпечення добробуту працівників, вжиття заходів з профілактики недобросовісної їх поведінки;
- контроль роботи, поведінки та зв'язків працівників, обізнаних з таємницями суб'єктів підприємництва;
- встановлення в діяльності суб'єктів підприємництва суворого пропускного режиму;
- контроль наявності документів, стану документообігу, в тому

числі і в комп'ютерних мережах, переговорів через засоби зв'язку;

- аналіз можливих способів посягання на інформацію суб'єктів підприємництва та методів протидії їм з практики роботи інших суб'єктів.

З питань захисту інформації працівники суб'єктів підприємництва зобов'язані:

- зберігати в таємниці всі службові відомості, з якими вони ознайомлені у зв'язку зі своєю роботою на посаді;
- виконувати встановлений порядок і правила роботи з документами та інформацією, які мають таємний або конфіденційний характер;
- знати кому із працівників і в якому обсязі дозволено працювати з відомостями обмеженого доступу;
- на вимогу працівників підрозділу безпеки надавати документи, матеріали, електронні носії інформації для перевірки;
- не користуватись на робочому місці власними засобами зберігання та передачі інформації, фото- та відеоапаратурою;
- дотримуватись встановлених правил передачі (пересилання, обробки) інформації з службових документів, ведення службових переговорів, в тому числі і по засобах зв'язку;
- негайно доповідати безпосередньому керівнику про втрату документів службового призначення, особливо тих, що мають гриф таємності;
- своєчасно інформувати підрозділи безпеки про спроби сторонніх осіб отримати інформацію таємного чи конфіденційного характеру.

Захист інтересів суб'єктів підприємництва у взаємовідносинах з персоналом, допущеним до їх таємниць здійснюється шляхом правового закріплення таких взаємовідносин у відповідних документах (Рис. 6.3).

При звільненні працівників з роботи захист інформації здійснюється шляхом виконання таких заходів: отримання від працівників, які звільняються всіх матеріалів конфіденційного та таємного характеру, що

обліковуються за ними з оформленням відповідного акту; передача працівниками, що звільняються, перепусток, печаток, штампів, ключів, сейфів тощо уповноваженим від суб'єкта підприємництва особам; проведення бесіди з працівниками, які звільняються з роботи, про необхідність збереження в таємниці всіх відомостей таємного та конфіденційного характеру, які були їм відомі під час роботи, підписання зобов'язань про нерозголошення ними цих відомостей; попередження працівників про відповідальність за розголошення чи використання таємних або конфіденційних відомостей, що належать суб'єкту підприємництва. Підписані працівниками зобов'язання зберігаються в їх особових справах протягом всього терміну зберігання справ.

Практика забезпечення безпеки діяльності суб'єктів підприємництва знає приклади коли витік цінної для них інформації здійснювався мимовільно, без злого наміру, в силу недоопрацювання певних питань чи не врахування особливостей ситуації, яка склалась навколо них. Система захисту інформації у зв'язку з цим має поширювати свій вплив і на такі випадки, зокрема щодо пропагандистських, рекламних заходів, публікації звітів, проспектів емісії акцій, оголошень та інших заходів, які проводяться суб'єктами підприємництва, оприлюдненням певної інформації в інформаційному середовищі. Тут інформація має надаватись у так званому диверсифікованому вигляді. Диверсифікація в даному випадку передбачає надання інформації по різних інформаційних каналах, через різних суб'єктів, окремими частками, з перервою у часі.

За певних умов може бути доцільним надання неповної інформації або ж у формі коротких заяв, повідомлень, прес-релізів, без будь-яких коментарів. В окремих випадках може бути необхідним згадати давно забуте слово цензура, особливо для інформації, яка активно поширюється суб'єктом підприємництва в інформаційне середовище. У даному разі заходи цензури будуть передбачати:

Зобов’язання про нерозголошення інформації з обмеженим доступом

Правовий документ, в якому працівник добровільно письмово дає згоду на обмеження його прав щодо використання інформації суб’єкта підприємництва з обмеженим доступом.

Одночасно працівник попереджується про відповідальність за розголошення такої інформації

Трудовий договір (контракт)

↓

Наявність у договорі:

- зобов’язань працівника не розголошувати відомості, які становлять таємну або конфіденційну інформацію;
- зобов’язань працівника дотримуватись правил захисту інформації з обмеженим доступом визначених суб’єктом підприємництва
- зобов'язань працівника повідомляти безпосереднього керівника і службу безпеки суб’єкта підприємництва про втрату носіїв інформації з обмеженим доступом;
- видів відповідальності працівника за недотримання ним правил захисту інформації

Наказ про призначення на посаду

↓

- визначається ступінь допуску до відомостей, які становлять таємну та конфіденційну інформацію;
- визначаються обов’язки працівника та заходи, які повинні ним вживатись для захисту інформації

Посадова інструкція

- обов’язок працівника дотримувати у таємниці відомості, які йому стали відомі у зв’язку з його роботою у суб’єкта підприємництва
- відповідальність працівника за порушення правил зберігання інформації суб’єкта підприємництва

Рис. 6.3. Заходи захисту інтересів суб’єктів підприємництва у взаємовідносинах з персоналом, допущеним до роботи з їх інформацією, яка має обмежений доступ.

- аналіз інформації стосовно належності її до такої, що має обмежений доступ;
- перевірку об’єктивності інформації та відповідності її чинному законодавству;
- порівняння змісту інформації, що надається для оприлюднення із змістом попередньо оприлюдненої на предмет суперечності одна одній чи виявлення в сукупності повідомлень ознак конфіденційності;
- аналіз інформації з точки зору її сприйняття інформаційним середовищем;
- узагальнення всієї інформації, що надана в інформаційне середовище та виявлення критичної межі її змісту для врахування у подальшій роботі.

Чинне законодавство передбачає право доступу до інформації суб’єктів підприємництва представникам державних органів. Тут інформація подається за рішенням керівника установи суб’єкта підприємництва в межах повноважень, якими наділений зазначений представник та в порядку, який встановлений суб’єктом.

Представники інших суб’єктів підприємництва, установ та організацій отримують доступ до інформації в межах і в порядку передбаченому відповідними договірними документами. У разі виникнення екстремальних ситуацій доступ до інформації суб’єктів підприємництва представникам правоохоронних органів, органів МНС, іншим особам надається за рішенням керівників установи суб’єкта в межах питань, які стосуються вирішення екстремальних ситуацій.

Однією з особливостей сьогодення є поширене використання різноманітних електронних засобів для отримання інформації з акустичного каналу. За таких умов система захисту інформації суб’єктів підприємництва має передбачати нормативне регулювання питань, пов’язаних з правилами користування технічними засобами накопичення, обробки, зберігання та передачі інформації. Крім того, доцільним є

включити в перелік заходів захисту інформації періодичне проведення атестації окремих приміщень установ суб'єктів підприємництва на предмет наявності в них пристроїв електронної розвідки. До заходів протидії витоку інформації через спеціальні електронні пристрої слід включити спеціальне інженерно-технічне обладнання приміщення де зберігається, оброблюється інформація з обмеженим доступом та обговорюються важливі для суб'єкта підприємництва питання. Сюди ж слід додати і використання спеціальних технічних засобів виявлення пристроїв електронної розвідки та періодичний огляд засобів і мереж зв'язку, місць їх розташування. Звичайно, що система захисту інформації повинна забезпечувати технічний захист інформації, яка оприлюднюється у ході переговорів, нарад та інших видів конфіденційного спілкування.

У захисті інформації суб'єктів підприємництва важливе місце відводиться організації спеціального діловодства. Діловодство розуміється як система заходів по документаційному забезпеченню діяльності суб'єкта підприємництва. Основним правилом в організації діловодства і захисту інформаційних ресурсів є забезпечення розмежування потоків відкритої інформації і інформації з обмеженим доступом. За таких умов в діяльності суб'єктів підприємництва має бути організовано службове діловодство (забезпечення документообігу відкритої інформації) і спеціальне діловодство, яке забезпечує документообіг інформаційних матеріалів таємного та конфіденційного характеру. Водночас у ході руху документів конфіденційного та таємного характеру збільшується кількість осіб, обізнаних з цінною інформацією, а з тим і розширюються потенційні можливості втрати конфіденційної та таємної інформації, збільшується ризик розголошення її персоналом, витоку через технічні засоби, зникнення документів. У такому випадку документообіг, як процес руху документованої інформації з обмеженим доступом, також стає об'єктом захисту. Головним у конфіденційному документообігу стає формування спеціальної технології руху документів, яка б забезпечувала необхідну

безпеку інформації на будь-якому із етапів її обігу. Тому захищений документообіг має являти собою контролюючий рух документів конфіденційного та таємного характеру по регламентованих пунктах приймання, обробки, розгляду, виконання, використання, зберігання в жорстких умовах організаційного і технологічного забезпечення безпеки як носіїв інформації, так і її самої. У такому разі в доповнення до правил службового документообігу конфіденційний документообіг додатково включає наступні заходи:

- обмеження доступу персоналу до документів справ і баз даних діловою, службовою та виробничою необхідністю;
- персональна відповідальність посадових осіб за надання дозволу на доступ працівників суб'єктів підприємництва до відомостей і документів конфіденційного і таємного характеру;
- жорстка регламентація порядку роботи з документами, справами, базами даних для всього персоналу.

Документообіг, як головна складова діловодства, базується на відповідній систематизації документів якою є номенклатура справ. Згідно з номенклатурою справ всі документи групуються у відповідні групи (справи) і обліковуються та зберігаються по таких групах (справах). Номенклатура справ є єдиною для установи суб'єкта підприємництва. Документообіг здійснюється у відповідності з номенклатурою справ та поділяється на вхідний, вихідний та внутрішній документопотоки. Вхідний документопотік спеціального діловодства включає: приймання, облік і первинну обробку пакетів, конвертів та незаконвертованих документів, що надійшли до установи суб'єкта підприємництва; облік документів і формування довідково-інформаційного банку даних по документах; попередній розгляд і розподіл документів; розгляд документів керівниками і надання їх на ознайомлення з документами виконавців, використання чи виконання.

Вихідний та внутрішній документопотоки включають: вироблення

документів (визначення грифу таємності та облік носія майбутнього документу, розробка документу, облік підготовленого документу та його виготовлення; контроль процесу вироблення документів); обробка виданих документів: експедиційна обробка і відправлення їх адресатам, передавання внутрішніх документів відповідним підрозділами суб'єкта підприємництва; систематизація вироблених документів відповідно до номенклатури справ, оформлення їх по справах; підготовка і направлення справ до архіву суб'єкта підприємництва відповідно з встановленим порядком архівації документів. Всі документи, справи і носії інформації повинні мати інвентарний номер.

Спеціальне діловодство є централізованим і забезпечується відповідним підрозділом. Основною особливістю документообігу в спеціальному діловодстві є багатоступеневий облік всіх процедур і операцій, що проводяться з документами. Зміст зазначених процедур і операцій конфіденційного документообігу розкрито в Додатках 1-2.

Важливе місце в організації захисту інформації в діяльності суб'єктів підприємництва є визначення режиму функціонування інформації. Режим, як правило,обирається у залежності від категорії інформації, її цінності для діяльності суб'єкта та зацікавленості в ній інших осіб. Тут можна пропонувати три режими: повністю закритий режим функціонування інформації, частково закритий режим та періодично закритий режим. У першому випадку доступ до інформації надається виключно обмеженому колу осіб і практично ніколи така інформація не розкривається у зв'язку з втратою цінності та її категорії. Документи, в яких міститься подібна інформація з втратою їх значення, як правило, знищується. Частково закритий режим функціонування інформації встановлюється шляхом надання доступу до окремих відомостей певному колу осіб при неможливості їх спілкування між собою з метою узагальнення отриманих відомостей. Періодично закритий режим інформації встановлюється для інформації, яка характеризує нові розробки, види продукції, тривалі

відносини або види діяльності, що пов’язані з розвитком бізнесу (проникнення в нові регіон, сегменти ринку, сфери діяльності і т. і.).

В умовах режимного функціонування можуть застосовуватись різні способи захисту інформації, які поділяються на активні, пов’язані з протидією загрозам та пасивні – спрямовані на захист від загроз. Активними можна вважати періодичну атестацію приміщень, в яких зосереджена цінна для суб’єктів підприємництва інформація або проводиться робота з нею, а також періодичне обстеження засобів обробки і передачі інформації. Сюди ж доцільно віднести періодичні перевірки наявності документів та вимірювання електромагнітних випромінювань і наводок. Обов’язковим має бути встановлення контролю персоналу, допущеного до роботи з інформацією обмеженого доступу суб’єктів підприємництва.

У окремих випадках, з метою протидії посяганням на інформацію суб’єктів підприємництва, останні можуть вдаватись до дезінформації осіб, які генерують такі загрози щодо місць знаходження інформації, її важливості, провокувати їх на дії через які вони будуть компрометувати себе.

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

Важливу роль у забезпеченні ефективного функціонування системи захисту інформації в діяльності суб’єктів підприємництва відіграє правильне управління такою системою, яка має здійснюватись централізовано на рівні головної установи певного суб’єкта. Насамперед воно передбачає вироблення правил, норм, стандартів захисту інформації, їх деталізації, по силах і засобах, залучених до захисту інформації. З метою забезпечення цілеспрямованого і організованого впливу на

функціонування системи має здійснюватись конкретизація та періодичне уточнення завдань всім підрозділам, установам з питань захисту інформації. Конкретизація завдань має випливати із аналізу ситуації, що складається в той чи інший час. Важливим в управлінні є здійснення контролю в системі захисту інформації, який передбачає проведення різного роду перевірок, періодичне отримання звітів про результати виконання заходів захисту, аналіз показників функціонування системи та оцінку ефективності її в цілому.

6.3. Особливості захисту інформації в комерційній діяльності суб'єктів підприємництва та їх ділових взаємовідносинах

Про необхідність захисту інформації, особливо цінної, для суб'єктів підприємництва безумовно знають всі, більш того, більшість суб'єктів вживають відповідних заходів її захисту. Разом з тим, всі погоджуються, що система отримання чужої інформації, несанкціонованого доступу до неї сьогодні також досить розвинена, у певних випадках навіть більш розвинена ніж система її захисту. В той же час, мабуть не всім відомо, що переважна більшість втраченої чи несанкціоновано розкритої інформації належить до тої, яка використовується в комунікаційній діяльності та діловому спілкуванні. Інформацію, яка зберігається на паперових, електронних чи інших носіях, навіть ту, що являє собою суму знань працівників значно легше захистити, якщо вона знаходиться без руху. Існує достатня кількість методик, засобів, організаційних заходів щодо захисту інформації, яка зберігається в установах суб'єктів підприємництва. Як правило, надійність зберігання інформації, яка знаходиться у статиці є досить високою. Але ж інформація має використовуватись, перетворюватись у певні технології, методики, формуватись у певні характеристики, за допомогою інформації здійснюються необхідні обґрунтування, переконання, приймаються необхідні рішення. За таких

умов захист інформації повинен мати суттєві особливості.

Насамперед слід подбати про захист інформації, яка використовується в комерційній діяльності, причому захист має бути спрямовано з одного боку на недопущення несанкціонованого доступу до інформації та протиправного її використання, а з іншого на можливість відшкодування шкоди, завданої неконтрольованим витоком інформації. У першому випадку (недопущення несанкціонованого доступу та використання інформації) основним правилом має бути:

- оптимізація інформації, яка використовується при проведенні відповідних комерційних операцій. Оптимізація передбачає використання відомостей в обсягах, що забезпечують виконання комерційних завдань без втрати вигоди, але не допускають можливості використання відомостей на шкоду суб'єкту підприємництва. Зазвичай ніхто на це не звертає уваги і працівники суб'єктів підприємництва навіть не знають про необхідність такого елементу захисту інформації, а якщо і знають, то не володіють методиками такої оптимізації. Відсутність системного підходу до захисту інформації і інформаційної безпеки взагалі робить технології комерційної діяльності досить уразливими з точки зору швидкого оволодіння ними конкурентами та втрати їх переваг у конкурентній боротьбі;

- обмеження кола осіб, які отримують цінну для суб'єкта підприємництва інформацію для її використання у конкретних операціях. Це можуть бути лише ті особи, які безпосередньо спілкуються з контрагентами, клієнтами, партнерами та опікуються взаємовідносинами з ними. Причому з метою виключення адаптації працівників до умов проведення операції і можливості формування у них спокуси до скоєння порушення через глибоку обізнаність у відповідній інформації періодично може проводитись їх ротація щодо клієнтів, контрагентів, видів продукції та умов проведення операцій;

- диференціація інформації серед працівників, які задіяні у

проведенні операцій. Зазвичай до проведення комерційної операції залучається декілька працівників (менеджери з продажу, технологи, бухгалтери, маркетологи та ін..), кожен з них отримує інформацію в межах необхідних йому для виконання покладених на нього обов'язків в тій чи іншій операції. Така ситуація унеможливить змову з клієнтами, контрагентами, партнерами та зробить інформацію, якою володіє кожен з працівників менш привабливою для осіб, що зацікавлені у отриманні повної інформації;

- прийняття сторонами комерційних операцій на себе зобов'язань щодо дотримання в таємниці і нерозголошення відомостей, які визначені певною стороною як конфіденційні чи таємні або сторони самі дійшли згоди про конфіденційність якоїсь інформації у їх взаємовідносинах. Такі зобов'язання обов'язково мають бути легітимізовані положеннями відповідних договорів;

- грамотне формування звітів про результати комерційної діяльності з врахуванням вимог законодавства та необхідності забезпечити прибуткову діяльність суб'єктів підприємництва. Будь-яка лишня інформація у таких звітах, або недостовірність може спровокувати додаткові перевірки з боку фіскальних та правоохоронних органів, а за ними певні санкції до суб'єктів підприємництва;

- оптимізація рекламної інформації. Остання має характеризувати суто продукцію, з неї неможливо зробити висновок про технологію виробництва продукції;

- перевірка надійності партнерів та контрагентів з т. з. їх інтересу до інформації з обмеженим доступом суб'єкта підприємництва.

Разом з тим, такі рекомендації носять загальний характер, у кожному окремому випадку вони можуть доповнюватись додатковими заходами та видозмінюватись. В той же час, як показує практика підприємницької діяльності, необхідність вжиття заходів захисту інформації під час комерційної діяльності є досить актуальною і ні за яких умов не може бути

ігнорованою.

У другому випадку – відшкодування шкоди, завданої суб'єктам підприємництва в результаті несанкціонованого доступу до його інформації, насамперед вимагається оцінка вартості такої шкоди. Тому, суб'єкти повинні мати методики оцінки вартості своїх інтелектуальних продуктів. А враховуючи, що відповідно до цивільного законодавства комерційна таємниця є інтелектуальним продуктом і належить відповідному суб'єкту як власнику, вона може захищатися в т. ч. і засобами інтелектуального права. Крім того, однією з ознак комерційної таємниці є її комерційна цінність. Інформація, яка не має такої цінності не може бути комерційною таємницею. У свою чергу, комерційна цінність інформації визначається: вартістю шкоди завданої втратою такої інформації, вартістю вигоди від використання даної інформації, вартістю інформації як товару. Методики визначення комерційної цінності інформації і розрахунки вартості конкретних відомостей будуть підставою для обґрунтування вимог суб'єктів підприємництва у судах по відшкодуванню шкоди нанесеної несанкціонованим доступом до зазначених відомостей. Крім того, суб'єкти підприємництва мають напрацювати механізм захисту своїх прав щодо відшкодування шкоди у випадках несанкціонованого доступу до їх інформації та посягань на неї. Такі питання будуть вимагати від них не лише відповідних заходів і певної системи їх застосування, а і правової та інформаційної культури.

В окремих випадках комерційна діяльність суб'єктів підприємництва може бути заснована на придбанні (продажу) продуктів інтелектуальної власності, які можуть мати конфіденційні інформаційні характеристики. За таких умов договори комерційних угод будуть носити конфіденційний характер, а супроводження виконання таких договорів мають здійснювати особи допущені до даного виду інформації. З боку контрагентів повноваження таких осіб має бути підтверджено відповідними документами. При цьому в розділі договорів де вказується

вартість продуктів чи в цілому угоди, окремо можуть вказуватись вартісні характеристики інформації про такі продукти.

Крім того, важливе значення буде мати юридичне закріплення права власності на продукти (об'єкти) інтелектуальної власності, порядок та умови її передачі до нового власника по угоді продажу, придбання.

Зазвичай, суб'єкти підприємництва розробляють відповідні алгоритми здійснення взаємовідносин з придбання (реалізації) продуктів інтелектуальної власності, що мають конфіденційний характер. Будь яке відхилення від такого алгоритму буде вважатись ознакою, яка вказує на порушення умов конфіденційності. Сукупність таких ознак дає підстави для проведення заходів по виявленню дій контрагентів, спрямованих на шкоду суб'єкту підприємництва, отримання інформації для обґрунтування його вимог до контрагентів.

Деякі із суб'єктів підприємництва, особливо із категорії великого бізнесу у своїй комерційній діяльності з метою захисту інформації вдаються до заходів промислової контррозвідки. Остання розуміється ними як комплекс заходів, що виконується з метою протидії актам промислового шпигунства та захисту власних джерел інформації. Основні дії промислової контррозвідки такі суб'єкти зосереджують на прогнозуванні шпигунської діяльності щодо них, виявлені заходів та осіб, що займаються такою діяльністю безпосередньо у структурах суб'єктів підприємництва, вжитті заходів щодо захисту своїх джерел інформації. Для виконання заходів промислової контррозвідки суб'єкти підприємництва залучають необхідних їм фахівців, як правило, з структур правоохоронних органів та взаємодіють з державними органами, сферою діяльності яких є захист вітчизняних об'єктів інтелектуальної власності.

У процесі підприємницької діяльності значну роль відіграють ділові стосунки партнерів, контрагентів, інших осіб, які можуть проводитись у формі зустрічей, переговорів, нарад. Безумовно, що у ході ділового спілкування може використовуватися інформація конфіденційного чи

навіть таємного характеру, тому необхідність захисту такого спілкування є очевидною. Порядок проведення спілкування у ході якого санкціоновано розкривається інформація з обмеженим доступом має регламентуватись відповідними нормативними актами в яких насамперед передбачаються заходи захисту вказаної інформації. Основною загрозою такій інформації є розголошення тих відомостей, які не обумовлені необхідністю спілкування. Причинами такого розголошення можуть бути недостатні знання учасниками спілкування складу інформації, що дозволена до розкриття, способів її захисту, умисне невиконання вимог щодо захисту інформації, провокації співрозмовників спрямовані на стимулювання розголошення необхідних їм відомостей. Розкриття у ході ділового спілкування конфіденційної інформації має бути виправдане комерційною необхідністю та доцільністю для конкретних умов і характеру питань по яких проходить спілкування. Основні етапи проведення ділових зустрічей, переговорів, нарад по яких розкривається інформація обмеженого доступу вказані на Рис. 6.4

Підготовка до проведення спілкування	Процес спілкування і його документування	Аналіз підсумків спілкування

Рис. 6.4. Етапи проведення конфіденційного спілкування

Дозвіл на проведення конфіденційного спілкування та обсяг конфіденційних відомостей, які можуть бути розкриті у процесі спілкування надає виключно керівник установи суб'єкта підприємництва. Зокрема, керівник визначає дату і місце проведення зустрічі (наради, перемовин), її тему, склад учасників, зміст інформації конфіденційного характеру, яка може бути розкрита у ході спілкування, завдання щодо забезпечення конфіденційності зустрічі (наради, перемовин), заходи з документування процесу спілкування, осіб, відповідальних за проведення таких зустрічей (нарад, перемовин).

У ході підготовки конфіденційних зустрічей (нарад, перемовин) готується перелік конфіденційних даних, які можуть бути розкриті у ході зустрічі та необхідні інформаційні матеріали, проекти рішень, список учасників по кожному з питань порядку денного. Проекти договорів, контрактів, угод передбачені для видачі учасникам спілкування не повинні містити конфіденційних відомостей. Такі відомості можуть вноситись у зазначені документи за результатами спілкування. Доцільно уникати, щоб у документованих та інших матеріалах, що плануються для видачі учасникам спілкування мали місце відомості конфіденційного характеру. Останні можуть повідомлятись усно і подаватись у документах, що складаються за результатами спілкування.

На конфіденційні зустрічі (наради, перемовини) запрошуються лише ті особи без яких такі заходи провести неможливо, незалежно від того чи є ці учасники працівниками суб'єкта підприємництва чи це сторонні особи.

Особливі вимоги існують до приміщень, де проводяться конфіденційні зустрічі (наради, перемовини). Перш за все такі приміщення мають бути у власності або принаймні у розпорядженні установи суб'єкта підприємництва. Напередодні проведення зустрічей (нарад, перемовин) має бути обстежено приміщення на предмет відсутності засобів несанкціонованого отримання інформації. Вікна мають бути закриті, в т. ч. і світло непроникаючими шторами, а двері мати звукоізоляцію. У даному приміщенні не повинно бути стаціонарних телефонів, комп'ютерів, телевізорів, радіо, інших засобів та обладнання, що безпосередньо не використовується у ході спілкування. Допуск до приміщення учасників спілкування здійснюється відповідно затвердженого списку у строго визначений час. Не допускається чекання учасниками інших питань поряд з приміщенням де проходить спілкування. Перед початком спілкування головуючий (представник

приймаючої сторони) нагадує присутнім про необхідність збереження у таємниці змісту спілкування та уточнює, які безпосередньо відомості можуть бути цінними для учасників зустрічі (наради, перемовини). Учасники не мають права:

- приносити до приміщення в якому проводиться зустріч (нарада, перемовини) фото-, відео-, аудіоапаратуру, комп'ютери, радіоприймачі, мобільні телефони, інші засоби і користуватись ними;
- робити виписки з документів, які використовуються у ході спілкування, незалежно від того чи мають вони гриф конфіденційності чи ні;
- обговорювати питання, що винесені для конфіденційного спілкування поза межами спеціально визначеного місця;
- надавати інформацію про тему, зміст та рішення зустрічі (наради, перемовин) іншим особам;

Всі учасники при висловлюванні своїх думок не мають права розкривати конфіденційні відомості поза межі, які визначено під час підготовки зустрічі (наради, перемовин). Процес спілкування може документуватись одним із його учасників або секретарем. Документи, складені за результатами спілкування, в т. ч. і протоколи зустрічі (наради, перемовин) в яких містяться відомості конфіденційного характеру повинні мати відповідний гриф і обліковуються в установленому порядку.

Певні особливості щодо захисту інформації у конфіденційній діяльності суб'єктів підприємництва існують у взаємовідносинах з відвідувачами їх установ. Під відвідувачами тут можна розуміти: осіб, яким необхідно вирішити певні ділові чи особисті питання з керівництвом або менеджерами установ; осіб, разом з якими, уповноважені особи суб'єкта підприємництва виробляють (обговорюють) певні питання виробничої, комерційної чи іншої діяльності; осіб, які здійснюють контрольні та інші функції державних органів.

Враховуючи різноманітність питань з якими приходять відвідувачі, різноплановість їх повноважень і функцій, а також потенційну наявність загроз інформації суб'єкта підприємництва, яку вони з собою несуть, роботу з відвідувачами доцільно централізувати на рівні установи. Всю роботу з відвідувачами проводить секретар-референт установ, який забезпечує виконання відвідувачами їх завдань в межах установи. З метою оптимізації роботи з відвідувачами та забезпечення ефективного захисту інформації доцільно провести чітку їх класифікацію. Зокрема всіх відвідувачів можна класифікувати наступним чином:

- особи, що не є штатними працівниками установи суб'єкта підприємництва, але які входять до складу дорадчих органів управління, є його акціонерами;
- представники державних органів та установ;
- представники установ та організацій з якими суб'єкт підприємництва підтримує ділові стосунки;
- клієнти, споживачі;
- представники ЗМІ, іноземці, приватні особи

Зазначені особи можуть нести в собі загрози інформації суб'єкта підприємництва як цілеспрямовані, так і побічні, через випадкове ознайомлення з інформацією суб'єкта. Відвідування установ суб'єктів підприємництва має бути підпорядковано певному регламенту, основними положеннями якого мають бути: узгодження можливості і умов прийому відвідувачів керівником та менеджерами установи; ідентифікація і реєстрація відвідувачів; вирішення питань, з якими звертаються відвідувачі секретарем-референтом; організація прийому відвідувачів керівником установи та її менеджерами; організація дій відвідувачів після вирішення їх питань. Заходи захисту інформації суб'єктів підприємництва у роботі з відвідувачами подано у Додатку 5.

Щоденна кількість відвідувачів повинна відповідати можливостям установи (час, навантаження на менеджерів, трудомісткість питань, що

Рис. 6.5. Захист конфіденційних відомостей при участі суб'єкта підприємництва у виставках, ярмарках, рекламі продукції

мають вирішуватись). Складні і довготривалі питання обговорюються у першу чергу. Кожному відвідувачу має бути виділено певний час (проміжок часу) на вирішення їх питань, відвідування керівництва установи чи її менеджерів. Всі особи, що приймають відвідувачів мають бути ознайомлені та знати правила захисту інформації суб'єкта підприємництва у роботі з відвідувачами, порядок вирішення їх питань.

Важливе місце у системі захисту інформації суб'єкта підприємництва повинно бути відведено заходам, які проводяться при участі суб'єктів у виставках, ярмарках та при рекламі продукції. Основні правила, якими тут має керуватись суб'єкт показані на Рис. 6.5.

Таким чином, комерційна діяльність суб'єктів підприємництва та їх ділові стосунки обумовлюють особливі умови функціонування їх інформації. З одного боку інформація забезпечує необхідний рівень довіри до суб'єктів з боку їх партнерів, контрагентів, споживачів, клієнтів, державних органів, а з другого, неконтрольоване і безпідставне її оприлюднення може шкодити діловій репутації, іміджу, економічній діяльності суб'єктів. За таких умов має бути знайдено оптимальний варіант використання інформації та запроваджена адекватна система її захисту, адаптована до динамічних умов комерційної діяльності і ділового життя суб'єктів підприємництва.

7. Інформаційне забезпечення підприємницької діяльності

У сучасному бізнесі інформація стала самим дорогим і ліквідним товаром, який дозволяє отримувати величезні прибутки тим суб'єктам, які вирвались вперед в інформаційних перегонах. Характерною рисою їх діяльності є швидкий розвиток нової парадигми управління — менеджмент, заснований на знаннях. Сьогоднішня ситуація в підприємництві, яка характеризується ускладненням комерційних схем, умов укладання угод, використанням складних комплексних продуктів, посиленням конкуренції суб'єктів ринку вимагає якраз такого підходу до управління сучасним бізнесом. Особливо це стосується таких ринків як енергетичний, фінансових послуг, хімічної продукції та деякі інші. Суб'єкти великого та середнього бізнесу стали потужними структурами, зі складним господарством та розгалуженими управлінськими зв'язками. Фінансові потоки, рух капіталів і товарів, управління ресурсами та персоналом стає все більш складним завданням, що пов'язано із зростанням обсягів звітності і документообігу, збільшенням швидкості інформаційних потоків, які з використанням сучасних інформаційних технологій вимагають самого високого рівня управління підприємницькою діяльністю. Якраз потреба в такому рівні управління і формує головну проблему сьогодення в управлінській діяльності. За сучасних умов органи управління потребують не просто знань, а конкретних і об'єктивних знань. Простого інформування уже недостатньо. Жоден з органів управління сьогодні не в змозі вести самостійно обробку всього масиву інформації, який поступає до нього, вибирати необхідні йому знання. Більш того, органи управління, як правило, не є компетентними в технологіях обробки інформації. До того ж, управлінська діяльність вимагає все більшої децентралізації, залишаючи за центральними органами лише стратегічні рішення. Потоки інформації, які надходять до них мають бути

скороченими і поділеними з врахуванням проміжних ланок, яким має бути делеговано право управління поточною діяльністю суб'єктів підприємництва, а це в свою чергу буде вимагати і розподілу в інформаційному забезпеченні. Для забезпечення стратегічного управління діяльністю суб'єктів підприємництва їх центральні органи мають отримувати інформацію переважно прогностичного характеру, яка дозволяє оцінити варіанти рішень, планів, сценаріїв розвитку, реалізації майбутніх проектів, а також відслідковувати тенденції змін на ринку.

Водночас, проміжні ланки управління мають отримувати інформацію, що характеризує сучасну ситуацію суб'єкта підприємництва, стан його діяльності, в тому числі і по окремих напрямках. Безумовно, що ефективним такий підхід до управління діяльністю будь-якого суб'єкта, може бути лише за умов потужного інформаційного забезпечення. Сучасне підприємство, банк не може не тільки ефективно, а взагалі ніяк розвиватись не здійснюючи інформаційного забезпечення своєї діяльності. Тобто, сучасна ситуація в бізнес-діяльності обумовлює декілька висновків:

- для забезпечення ефективної діяльності і розвитку підприємництва поряд з фінансовими, матеріальними, кадровими конче потрібні ще і інформаційні ресурси;
- формуванням таких ресурсів мають займатись досить компетентні фахівці, професіонали в галузі інформаційних технологій і аналітичної роботи;
- робота, пов'язана з формуванням зазначених ресурсів має складати на підприємстві, у банку окремий вид їх діяльності. Водночас, інформаційний ресурс є важливою компонентою їх економіки, складовою виробничої та комерційної діяльності.

7.1. Інформаційний ресурс **суб'єктів підприємництва** і його характеристики

Даючи характеристику інформаційному ресурсу суб'єктів підприємництва слід зазначити, що він являє собою сукупність інформації, яка знаходиться у власності чи розпорядженні кожного з них і використовується ними для забезпечення їх діяльності.

Структуру інформаційного ресурсу з точки зору його змісту складає правова інформація (нормативно-правові документи суб'єктів підприємництва, інші правові документи та матеріали); комерційна інформація (характеристика ринку та його суб'єктів, умови комерційної діяльності); ділова інформація (ділові зв'язки, партнери, взаємовідносини з ними та інша інформація, яка може бути використана в ділових стосунках); інформація про персонал (відомості, що містяться в особових справах працівників); інформація про ринки (аналітичні характеристики ринків, сфер економіки, в яких працює та планує працювати суб'єкт підприємництва); інформація про сферу діяльності (технології виробництва, методи забезпечення діяльності суб'єкта підприємництва, плани розвитку); інші види інформації (статистична, про клієнтів, наукова, про забезпечення безпеки і т. і.).

Таким чином, інформаційні ресурси, як сукупність інформації мають певні особливості щодо їх існування. На відміну від інших видів ресурсів, які існують в певній матеріальній формі, інформаційні ресурси представлені трьома категоріями: документами на паперових і електронних носіях, зразками продукції та інтелектом (знаннями) працівників суб'єктів підприємництва.

Важливою особливістю інформаційних ресурсів є їх багатофункціональність, вони можуть нести освітню, аналітичну, комерційну, інформуючу, маскуючу функції та функцію впливу. Така багатофункціональність інформаційних ресурсів обумовлює

різнонаправлене їх використання. Зокрема, інформаційні ресурси суб'єктів підприємництва можуть використовуватись для:

- формування знань працівників суб'єкта підприємництва, необхідних для забезпечення своєї професійної діяльності;
- створення нормативно-правових документів суб'єктів підприємництва, що регулюють окремі види їх діяльності та поведінку на ринку;
- формування управлінських та виробничих рішень;
- розробки нових продуктів та послуг;
- формування іміджу суб'єктів підприємництва на ринку, забезпечення інформаційного впливу в їх інформаційному середовищі;
- проведення наукових та інших досліджень, необхідних для забезпечення діяльності суб'єктів підприємництва;
- забезпечення безпеки діяльності суб'єктів підприємництва, ефективного проведення фінансових, комерційних, господарських та інших операцій;
- проведення інформаційно-аналітичних досліджень клієнтів, партнерів, контрагентів;
- формування перспектив розвитку суб'єктів підприємництва

Враховуючи важливість інформаційного ресурсу та особливу роль, яку він виконує в діяльності суб'єктів підприємництва постає питання про умови та зміст роботи по його формуванню. Як говорилось вище, інформаційний ресурс є результатом роботи підприємства, банку по інформаційному забезпеченню їх діяльності. Тобто, формування інформаційного ресурсу має здійснюватись шляхом проведення роботи по його інформаційному забезпеченню. В свою чергу структуру інформаційного забезпечення складають такі види інформаційної діяльності як маркетингові дослідження, інформаційно-аналітична робота і комерційна розвідка.

Організовуючи інформаційне забезпечення діяльності суб'єктів

підприємництва та формування їх інформаційного ресурсу не можна не враховувати властивості інформації, які роблять її особливим видом бізнес-ресурсу. Інформація виступає як форма існування знань, за допомогою неї подаються кількісні та якісні характеристики об'єктів, подій, процесів, вона є змістом різного роду документів, ідей, інтелектуальних продуктів. Інформація є відповідним видом впливу (реклама, пропаганда, управлінські та виробничі рішення, імідж). Крім того, інформація може виступати формою комерції як товар, а також одним із видів інтелектуальної зброї. Таким чином, різноманітність властивостей інформації вимагає від суб'єктів підприємництва вести інформаційну роботу в різних сферах інформаційного середовища, з різними категоріями суб'єктів. Разом з тим, інформація в інформаційному середовищі знаходиться в диверсифікованому вигляді. Окремі інформаційні характеристики знаходяться у різних носіїв, надавались в середовище через різні канали, протягом тривалого часу, знаходяться у різноманітному вигляді (відкриті повідомлення, чутки, дезінформація, витік відомостей обмеженого доступу і т. і.). Досліджуючи характер існування інформації в інформаційному середовищі науковці та фахівці-аналітики приходять до висновку про наявність тенденції до збільшення відкритої інформації в характеристиках певних об'єктів, подій, процесів. Якщо раніше із відкритих джерел можна було отримати до 80 % необхідної інформації, то на даний час обсяг цінної інформації яка отримується із відкритих джерел зріс до 95 % [56]. Причинами виникнення зазначеної тенденції є стрімко зростаюча кількість користувачів мережі Інтернет і можливості оперативно подати в ній будь-яку інформацію; розвиток комп'ютерних засобів обробки та аналізу інформації; необхідність підвищення відкритості бізнес-діяльності для досягнення успіху в конкурентному змаганні.

Крім того, сьогодні досить помітна ще одна тенденція - швидке оновлення інформації в інформаційному середовищі, що унеможливлює

організацію інформаційної роботи суб'єкта лише в одній якійсь формі: маркетингових досліджень, інформаційно-аналітичної роботи чи комерційної розвідки.

За таких умов організація інформаційного забезпечення діяльності суб'єктів підприємництва має носити комплексний характер і здійснюватись у різних сферах інформаційного середовища. Крім того, інформаційне забезпечення має відповідати наступним вимогам:

- законності — здійснюватись в межах чинного законодавства;
- безперервності — інформаційні ресурси для забезпечення їх високої якості мають постійно оновлюватись;
- активності — сили, задіяні в інформаційному забезпеченні повинні постійно прагнути до отримання інформації;
- високої технічної оснащеності — інформаційна робота повинна спиратись на сучасні комп'ютерні засоби та технології збору і обробки інформації;
- компетентності — особи, які виконують завдання інформаційного забезпечення мають бути професіоналами у своїй галузі, здатними на високому професійному рівні виконувати свої обов'язки.

Водночас організація інформаційного забезпечення, незважаючи на єдину мету здійснюється окремо по кожному з видів забезпечення: маркетингових досліджень, інформаційно-аналітичної роботи і комерційної розвідки. Враховуючи, що організація маркетингових досліджень не є предметом безпеки, основну увагу тут буде приділено інформаційно-аналітичній роботі та комерційній розвідці.

У зв'язку з цим необхідно звернути увагу на особливості вітчизняного досвіду інформаційного забезпечення підприємницької діяльності. Ситуація має суттєві відмінності залежно від категорії суб'єктів бізнесу. Так, у великому бізнесі його власники зазвичай приймають стратегічні рішення орієнтуючись на загальнополітичну та загальноекономічну ситуацію в країні, використовуючи інформацію про розстановку бізнес-суб'єктів на ринку, їх

інформаційний ресурс складається із власного досвіду та власного бажання, результатів оцінки ситуації, зв'язків у певних колах, а також інформації, що є доступною для них у державних структурах. Безпосередня робота з інформаційного забезпечення починається на етапі реалізації прийнятого рішення, коли зусилля суб'єктів підприємництва спрямовуються на отримання інформації, необхідної для вибору варіанту виконання рішення та способів конкретних дій. Зазвичай інформаційний ресурс, яким користуються власники великого бізнесу є недоступним для їх суб'єктів підприємництва, що нерідко обумовлює конфлікти між власниками і керівниками суб'єктів або ж формує досить агресивну поведінку вказаних суб'єктів на ринку.

Середній бізнес, як правило, попередньо потребує інформації для вироблення подібних рішень і рідко коли останні приймаються без суттєвого інформаційного забезпечення. Реалізація прийнятих рішень базується на тих же інформаційних ресурсах, що використовуються при прийнятті рішень і додатковій інформації, яка конкретизує варіанти і способи дій суб'єктів підприємництва.

Малий бізнес у інформаційному плані забезпечує свою діяльність і розвиток використовуючи власний досвід і поточну інформацію, яка зазвичай і складає його інформаційний ресурс.

Важливу роль інформаційний ресурс займає у виробленні інформаційних продуктів. Сучасні суб'єкти підприємництва здійснюють свою діяльність не лише на економічних ринках, а і ще в інформаційному середовищі. Тому інформаційні продукти, то не тільки товар, а під ними можна розуміти різного роду інформаційні та інтелектуальні матеріали, що супроводжують та забезпечують економічну діяльність суб'єктів підприємництва. Тобто, інформаційні продукти притаманні практично всім суб'єктам, які здійснюють свою діяльність на будь-якому ринку. Інформаційними продуктами можуть виступати технології виробництва, комерційної діяльності та взаємовідносин, результати маркетингових,

соціологічних та інших досліджень, пропозиції, проекти, аналітичні матеріали. Більш того, інформаційні продукти як інформаційні характеристики суб'єктів підприємництва чи їх діяльності можуть носити віртуальний характер, поширюючись у інформаційному просторі досить динамічно. Аналізуючи роль інформаційних ресурсів в діяльності суб'єктів підприємництва можна говорити, що рівень їх досконалості суттєво впливає на ефективність бізнесу суб'єктів, оскільки інформаційні ресурси:

- забезпечують об'єктивне бачення менеджментом суб'єкта підприємництва процесів, які відбуваються на ринку і у взаємовідносинах з іншими суб'єктами та організаціями, дають можливість приймати ефективні рішення;
- сприяють розробці більш якісних проектів та програм діяльності суб'єктів підприємництва, конкретно адаптованих до особливостей ситуації чи регіону, формуванню ефективних взаємовідносин та поведінки на ринку, який має динамічний розвиток;
- утворюють передумови для підтримання необхідного рівня конкурентоспроможності суб'єктів підприємництва на ринку, результативної протидії актам недобросовісної конкуренції;
- забезпечують пізнавальні потреби споживачів, клієнтів, контрагентів, партнерів у необхідних їм послугах, товарах, роботах чи взаємовідносинах;
- формують необхідні бази даних, як інформаційний капітал суб'єктів підприємництва, здатний забезпечувати їх глобальні та локальні перспективи розвитку.

За своїм призначенням інформаційний ресурс суб'єктів підприємництва може мати наступну структуру: пізнавальний, виробничий, організаційний, спеціальний, допоміжний. Пізнавальну частину ресурсу складає інформація, яка характеризує суб'єкт підприємництва як комерційну організацію. Дає уявлення про можливості та результати (показники) його діяльності, продукцію, послуги, роботи; інформацію для внутрішнього

користування про технології, проекти, партнерів, клієнтів, контрагентів, особливості поведінки на ринку, взаємовідносини з іншими суб'єктами; інформацію про персонал, перспективні розробки, шляхи розвитку, характеристики окремих суб'єктів, подій; ситуації.

Інформація щодо виробництва включає дані про технології, які використовуються у ході вироблення товарів, характеризують правила, умови, порядок надання послуг, виконання робіт, підходи до формування їх вартості, фінансову діяльність суб'єкта підприємництва, іншу виробничу інформацію призначену для внутрішнього використання.

Організаційна інформація характеризує нормативно-правову складову діяльності суб'єкта підприємництва, зміст договорів, протоколів перемовин, рішень щодо організації діяльності суб'єкта, взаємовідносин з іншими суб'єктами, сюди ж слід віднести інформацію про управління його діяльністю.

Спеціальна інформація складає дані про безпеку суб'єкта підприємництва, його конфіденційні звязки, відомості з досьє осіб щодо яких має зацікавленість суб'єкт підприємництва, зміст картотек, інтегрованих баз даних.

Допоміжна інформація – матеріали, що будь-яким чином характеризують сферу діяльності та взаємовідносин суб'єкта підприємництва, яка отримується з локального та глобального інформаційного середовища.

Важливе місце у структурі інформаційного ресурсу займає т. з. ділова інформація на яку зазвичай виникає найбільший попит у провідних менеджерів суб'єктів підприємництва. До такої інформації може бути віднесено макроекономічні показники сфери (галузі) діяльності, ринку; фінансові та біржові відомості; комерційна інформація про власну діяльність та діяльність інших суб'єктів, які утворюють чи можуть утворювати конкуренцію суб'єкту підприємництва; статистичні дані всіх рівнів; інформація про ділові зв'язки.

Слід звернути увагу і на те, що інформаційний ресурс є джерелом інформації не лише безпосередньо для самих суб'єктів підприємництва, а і для зовнішніх користувачів. Насамперед, це можуть бути кредитори, інвестори, партнери, державні органи інші суб'єкти. Тобто, інформаційний ресурс є досить структурованим за різним призначенням і доступом до інформації. Утворення такого ресурсу вимагає значної роботи. І тому не дивно, що значна частина суб'єктів підприємництва формуванню якісного, структурованого за різними ознаками інформаційного ресурсу не придає суттєвої уваги, залишаючись у сучасному інформаційному просторі недостатньо інформаційно озброєними.

7.2. Інформаційно-аналітична робота в діяльності суб'єктів підприємництва

Інформаційно-аналітична робота (ІАР) розуміється як діяльність пов'язана зі збором і обробкою відкритої інформації, формуванням відповідних інформаційних документів та наданням їх керівництву суб'єкта підприємництва. Тобто ІАР — це насамперед діяльність в середовищі відкритої інформації, причому діяльність пов'язана зі збором інформації, її обробкою та формуванням відповідних інформаційних документів. Кінцевим етапом ІАР є інформування керівництва суб'єктів підприємництва. Структуру ІАР подано на Рис. 7.1.

Основним в організації ІАР є визначення сфер інформаційної уваги, об'єктів і джерел інформації, так як це дозволяє більш конкретизувати і спрямувати дану роботу, концентрувати зусилля суб'єктів підприємництва на найбільш важливих її напрямках. Справа в тому, що інформаційне середовище підприємницької діяльності є досить глобальним, неоднорідним, обсяги інформації в ньому є такими, що не дають можливості без ефективної організаційної роботи здійснювати інформаційне забезпечення суб'єктів підприємництва. За таких умов зазначені суб'єкти змушені сегментувати

сфери інформаційного середовища в яких у наступному будуть виконувати необхідну їм інформаційну діяльність.

Таким чином, сфера інформаційної уваги суб'єкта підприємництва являє собою сегмент інформаційного середовища, в якому він забезпечує стратегічні, тактичні та оперативні інформаційні інтереси і завдання. Враховуючи специфіку діяльності суб'єктів підприємництва та структуру їх інформаційного середовища, сфера інформаційної уваги може включати: сферу інтересів, яка може бути представлена інформацією про об'єкти, регіони, галузі економіки, до яких прагне проникнути суб'єкт у майбутньому, події, які характеризують відповідні ринки; сферу впливу, яка характеризується інформацією про події, об'єкти, що можуть здійснювати вплив на поточну діяльність суб'єкта; сферу безпосередньої діяльності — інформацію про об'єкти та події, які характеризують або впливають на проведення тієї чи іншої операції, що здійснюється суб'єктом на даний час.
Як правило, суб'єкти підприємництва забезпечують роботу у всіх сферах інформаційної уваги і використовують інформацію: сфери інтересів — як стратегічну для прийняття рішень щодо довгострокових угод, договорів, планування перспектив розвитку; сфери впливу — як тактичну для прийняття рішень щодо співробітництва з партнерами, інвестування (вкладання) коштів в нові проекти, протидії недобросовісній конкуренції, визначення поведінки на ринку в той чи інший проміжок часу; сфери безпосередньої інформаційної діяльності — як оперативну для прийняття рішень щодо безпосереднього здійснення конкретної операції, укладання конкретної угоди.

Основними факторами, які безпосередньо обумовлюють визначення сфер інформаційної уваги можуть бути: сфери і галузі економіки, бізнесу, в яких здійснює свою діяльність суб'єкт підприємництва, плани його розвитку; стан конкуренції на ринку, агресивність конкурентної боротьби, наявність, види, небезпечність загроз діяльності суб'єкта та особливості поточної діяльності; необхідність формування (підтримання) позитивного іміджу

Рис. 7.1. Структура інформаційно-аналітичної роботи суб’єкта підприємництва

суб'єкта в його інформаційному середовищі; інтереси суб'єкта та особливості його поведінки на ринку.

Звичайно, що інформація у сферах інформаційної уваги суб'єктів підприємництва, як і взагалі в інформаційному їх середовищі існує не взагалі, а зосереджена в певних місцях, які прийнято називати об'єктами інформації. У даному випадку під об'єктом інформації доцільно розуміти установу, організацію, виробництво, захід, в яких зосереджена необхідна суб'єктам підприємництва інформація. Тобто об'єктами інформації для кожного суб'єкта підприємництва можна вважати інших суб'єктів, установи засобів масової інформації, установи, організації клієнтів, контрагентів, партнерів, громадські та політичні організації, органи влади та їх установи, науково-дослідні установи, правоохоронні органи і судові установи, детективні та охоронні агентства і організації, рекламні агентства, з'їзди, конференції, виставки, презентації і т. і.

Зосереджена на вказаних об'єктах інформація знаходиться на відповідних носіях, якими в свою чергу можуть бути працівники зазначених вище установ і організацій, а також самого суб'єкта підприємництва, продукція засобів масової інформації, документи, рекламні продукти, аудіо- та відео матеріали, комп'ютерна техніка і електронні носії інформації, продукція, виставкові експозиції, наукові навчальні чи інші видання та ін.

Таким чином, організовуючи ІАР суб'єкти підприємництва мають визначатись не тільки із сферами інформаційної уваги, а і з об'єктами інформації, та її джерелами, які з об'єктів та джерел мають представляти для них найбільший інтерес. Водночас, важливим залишається завдання отримання інформації. Як правило, служби безпеки суб'єктів підприємництва для отримання інформації з відкритих джерел формують так звані інформаційні канали, по яких інформація і потрапляє до суб'єктів. Під інформаційним каналом зазвичай розуміють сукупність джерел інформації, засобів та методів їх подання до споживачів

інформаційних продуктів. Перелік та характеристика інформаційних каналів представлені на Рис. 7.2.

Рис. 7.2. Інформаційні канали ІАР суб'єктів підприємництва

Враховуючи відкритий характер інформації, яка, як було вже вказано вище, використовується в ІАР, інформаційні канали носять також легальний характер і формуються на добровільних взаємовідносинах суб'єктів підприємництва з постачальниками інформації. Серед найбільш поширених на даний час каналів отримання інформації, які використовуються суб'єктами підприємництва можна вказати наступні:

- укладання договорів на інформаційне співробітництво із спеціалізованими підприємствами, в основі діяльності яких знаходиться надання інформаційних послуг;
- підписка на періодичні видання друкованих засобів інформації та організація прийому радіо- та телепередач спеціальним підрозділом суб'єкта підприємництва;
- робота з персоналом суб'єктів підприємництва, організація

періодичного проведення соціально-психологічних досліджень в установах суб'єктів;

- створення (участь) громадських організацій і отримання інформації через громадську діяльність останніх;
- взаємообмін інформацією з іншими суб'єктами та установами, правоохоронними та іншими органами;
- замовлення інформаційних продуктів через науково-дослідні установи, інформаційні та рекламні агентства;
- робота на ринку праці, формування «Кадрового резерву»;
- формування інституту аналітиків в установах суб'єктів підприємництва;
- отримання інформації та експертних висновків по запитах суб'єктів від державних та інших установ і організацій;
- збір чуток.

Використовуючи наявні інформаційні канали суб'єкти підприємництва зосереджують увагу переважно на двох формах збору інформації: інформаційному аудиті і інформаційному моніторингу.

Інформаційний аудит — це інформаційне обстеження сфери інформаційної уваги чи певних об'єктів з метою отримання, вивчення і оцінки необхідної суб'єкту підприємництва інформації. Основними технологіями інформаційного аудиту є: пошук та вивчення інформації про конкретну подію, факт, особу безпосередньо на самому об'єкті; пошук та вивчення інформації про конкретний об'єкт через його зв'язки (ділові, комерційні, організаційні та ін.); пошук та вивчення інформації про конкретний об'єкт шляхом спеціального обстеження його інформаційного середовища. Зміст операцій по кожній з технологій подано в Додатку 6.

Інформаційний моніторинг — це контроль надходження інформації в інформаційне середовище суб'єкта підприємництва з метою виявлення важливої та цінної інформації і її використання для забезпечення його діяльності.

Технологіями, які використовуються в ході інформаційного моніторингу є: контроль інформації, яка надходить в інформаційне середовище суб'єкта підприємництва за визначеними ознаками та індикаторами; контроль інформації, яка надходить в інформаційне середовище суб'єкта по визначених джерелах; суцільний контроль інформації, яка з'являється в інформаційному середовищі суб'єкта. Зміст операцій по кожній із технологій подається в Додатку 7.

Основним методом збору інформації в діяльності суб'єктів підприємництва є: систематизація інформації, яка надходить до суб'єктів підприємництва від їх клієнтів, споживачів, контрагентів, інших суб'єктів. Ретельне вивчення інформації отриманої від зазначених джерел про їх стан та діяльність, зв'язки, історію, є досить важливим моментом у зборі інформації та формуванні інформаційного ресурсу.

Надання інформаційних запитів до відповідних установ і організацій та отримання відповіді на них є також важливим методом збору інформації, саме таким способом збирається найбільш достовірна та цінна інформація. Інформаційна взаємодія суб'єкта підприємництва з різними суб'єктами як державними, так і недержавними також дає досить позитивні результати у зборі необхідної інформації.

Робота з рекламними та пропагандистськими матеріалами, різного роду оголошеннями, також вважається одним із методів збору інформації. По рекламному оголошенню наприклад можна оцінити фінансове становище суб'єкта, кількість офісів і адресу їх розташування. Регіон розташування впливає на орендну плату. Якщо скажімо офісів два і більше, розташовані вони в різних районах міста, то можна думати, що суб'єкт розвивається досить успішно і його фінансове становище може бути стабільним. Про фінансові можливості суб'єкта може говорити і кількість телефонів в офісі суб'єкта, чим їх більше тим пристойним може бути його фінансовий стан.

Періодичне опитування, що проводиться суб'єктами підприємництва

у їх сегменті ринку є також суттєвим моментом методики збору інформації. Ну і звичайно це постійна робота з друкованими засобами інформації. Відкрита преса традиційно є найбільш ємним і популярним інформаційним каналом. Головне, це системний підхід до аналізу матеріалів преси, що на жаль не досить полюбляють робити служби безпеки вітчизняних суб'єктів підприємництва. Водночас іноземні фахівці вказують, що якраз системний аналіз матеріалів преси дозволяє отримати практично всі необхідні їм відомості. Преса дає уявлення про ситуацію не просто в цифрах і фактах, а на зрозумілій читачу мові, хай навіть на рівні чуток, пліток чи певного відчуття, що дозволяє зв'язати всі ці складові в цілісну картину, яка характеризує події, тенденції, поведінку ринку чи окремих його суб'єктів. Матеріали засобів масової інформації дозволяють зіставити, уточнити і доповнити новими відомостями інформацію, отриману з інших джерел, формувати нові напрямки для поточної роботи по збору інформації.

Інформація, яка зібрана суб'єктом підприємництва в процесі формування інформаційного ресурсу являє собою відомості, що потребують подальшої обробки. Структура процесу аналітичної обробки інформації і вказана на Рис. 7.3.

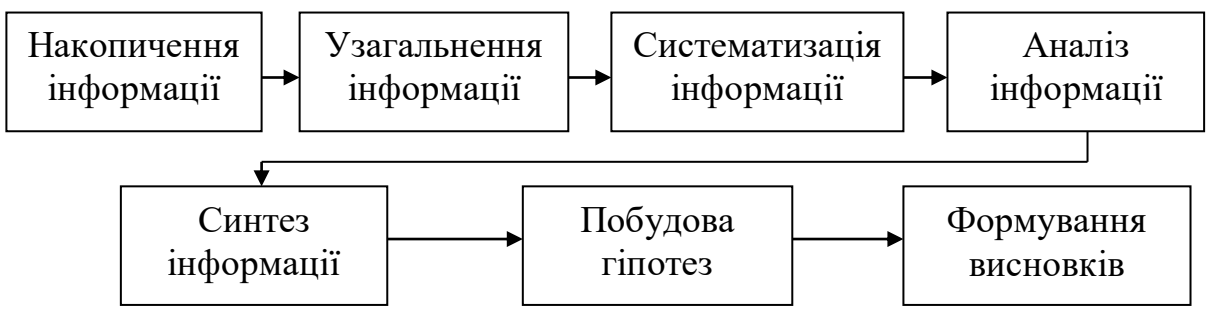


Рис. 7.3. Структура та алгоритм процесу аналітичної обробки інформації.

У ході накопичення інформації здійснюється формування обсягів інформації, достатніх для проведення аналітичної оцінки подій чи певних

об’єктів. Обсяги інформації формуються з різних джерел незалежно від часу її виявлення та достовірності.

При узагальненні інформації на основі однорідних ознак, загальних характеристик, властивостей здійснюється поєднання фактів, подій, повідомлень, формування загального поняття чи загальних положень.

Класифікація подій, фактів, об’єктів, узагальнених понять і положень, виявлення закономірності у їх виникненні, розвитку та функціонуванні — проводиться у ході систематизації інформації.

У ході аналізу інформації здійснюється вивчення подій, фактів по окремих елементах, виявляються зв’язки між ними. Водночас синтез інформації передбачає вивчення тих же подій, фактів, об’єктів у їх взаємозв’язку, взаємовідносинах між собою та іншими явищами, умовами, об’єктами.

При побудові гіпотез здійснюється формування припущень щодо причин, умов та розвитку подій, фактів, об’єктів, залежно від ситуації, що складається на ринку та можливих рішень, що їх може прийняти керівництво суб’єкта підприємництва.

На основі сформованих гіпотез здійснюється вироблення кінцевого підсумку обробки інформації у вигляді одного або декількох можливих варіантів, що характеризують стан ситуації (об’єкта) та перспективи її (його) розвитку.

У ході обробки інформації, яка характеризує об’єкт, що певним чином може загрожувати суб’єкту підприємництва, існує певний алгоритм аналітичної оцінки такого об’єкта. Спочатку визначається існуючий (економічний, юридичний, соціальний) стан об’єкта, закономірності і тенденції його розвитку. У наступному здійснюється вивчення його можливостей, потенціалу, реальність та напрямки загроз, які можуть надходити від нього, і далі прогнозуються наміри об’єкта, вірогідність негативних його дій стосовно суб’єкта підприємництва, в тому числі за терміном, місцем і обсягом, наслідки, які можуть настати для субєкта в

результаті реалізації зазначених загроз.

Сформовані висновки та пропозиції надаються керівництву та іншим особам у вигляді інформаційних документів. На даний час за досвідом підприємницької діяльності серед інформаційних документів існують:

- інформаційні повідомлення — надання інформації, особливо важливого значення у вигляді усного чи письмового викладення;
- інформаційні доповіді — комплексне і всебічне викладення проблеми з використанням всієї наявної по ній інформації;
- інформаційні довідки — опис окремих характеристик конкретних подій або об’єктів;
- інформаційні огляди — опис основних інформаційних повідомлень за визначений період у формі резюме з класифікацією по рубриках;
- інформаційні зведення — опис загальної картини існуючих подій;
- інформаційні прогнози — короткий огляд подій, фактів, викладення висновків за їх наслідками і можливому розвитку ситуації з відповідним обґрунтуванням.

Аналітичні та інші матеріали, документи, що складають інформаційний ресурс зберігаються у справах поточного та архівного зберігання. Окремі матеріали та документи зберігаються у вигляді досьє. Досьє являє собою всебічну характеристику певних об’єктів з детальним їх описом та підтверджуючими матеріалами. Як правило, досьє створюються щодо найбільш важливих об’єктів (фізичні та юридичні особи), які можуть становити загрозу суб’єкту підприємництва або створити йому суттєву конкуренцію.

На всі об’єкти, до яких суб’єкт підприємництва має (чи мав в минулому) певний інтерес складається картотека, в якій містяться загальні їх характеристики, як правило, статистичні дані.

Зазвичай суб’єкти підприємництва створюють електронні бази даних куди надається інформація про різні сфери їх діяльності та інтересів,

клієнтів, партнерів, кредиторів, контрагентів, а також персонал. Звичайно, що і електронні бази даних, і досьє та картотеки, а також поточні та архівні справи відповідним чином захищаються від несанкціонованого доступу до них.

Стратегія управління діяльністю суб'єкта підприємництва повинна завжди інтегрувати у собі нову інформацію про поточну ситуацію, тільки за таких умов ми можемо не допускати упущеної вигоди. Разом з тим, досвід показує, що інформація і розуміння суті справи не є синонімами. Щоб інформація була корисною ми маємо правильно визначати суть проблеми, яку прагнемо вирішити. Виходити слід з того, що інформація про необхідний нам об'єкт, подію, ситуацію може мати різну конструкцію, яка вибудовується кожним хто так чи інакше має справу з даним об'єктом (подією, ситуацією) чи інформацію про нього. Тому за всіх умов, здійснюючи інформаційне супроводження підприємницької діяльності ми маємо досить грамотно підійти до визначення того, яка саме інформація нам потрібна. Такий підхід сформує наше відношення до необхідної нам інформації чи її джерел, а з цим і зумовить нашу увагу до неї. Тоді, оволодівши увагою до необхідної нам інформації ми не пропустимо її з поміж великої кількості відомостей або так званого інформаційного шуму яким багате будь-яке інформаційне середовище. При такому підході робота по збору необхідних для інформаційного забезпечення діяльності суб'єктів підприємництва відомостей стає більш ефективною, значно скорочується час та знижується ризик «потонути» у великій кількості може бути важливої, але не цінної інформації. Тобто, потреба у інформації визначається метою, на досягнення якої спрямовує свої зусилля суб'єкт підприємництва на кожному із етапів своєї діяльності. Причому ця мета може носити як стратегічний характер (визначення напряму, сфери, результату діяльності), так і тактичний (вибір шляхів, супутників, обсягів ресурсів) та оперативний (вибір, розробка способів діяльності) характер.

Визначаючи важливість інформації, необхідної для прийняття стратегічних рішень, іноземні фахівці стверджують, що такі рішення прямо впливають на долю підприємств, їх розвиток і життєздатність. Оточення підприємств постійно змінюється, швидкість таких змін збільшується. Від того кількість стратегічних рішень також зростає, їх наслідки все складніше прогнозувати, а ціна помилок постійно стає все більш масштабною [57]. Звідси стратегічні потреби в інформації включають в себе будь-які відомості, які здатні забезпечити довгостроковий вплив на діяльність суб'єктів підприємництва. Це можуть бути відомості про сферу діяльності, ступінь її розвитку, технології, що використовуються у даній сфері, коньюктуру ринку, можливості та перспективи її зміни. Враховуючи, що новий суб'єкт підприємництва рідко може бути єдиним у даній сфері діяльності чи на певному ринку, безумовно на нього будуть впливати (безпосередньо чи опосередковано) конкуренти, в результаті чого це може відбиватись на досягненні його стратегічної мети. У цьому випадку інформація про конкурентів, їх можливості, здатність змінити ситуацію у галузі та на ринку, осіб, що лобіюють інтереси конкурентів також буде належати до стратегічної. З метою забезпечення стратегічного планування необхідною буде інформація про можливість змін у правовому полі, здатних впливати на формування чи зміну стратегічної мети суб'єктів підприємництва. Доречними будуть і відомості про можливості сировинної бази, транспортної інфраструктури регіону, фінансову ємність ринку. Враховуючи особливості вітчизняних реалій до стратегічної слід віднести інформацію про внутрішньополітичну ситуацію в країні та можливості її кардинальних змін.

Структура інформації, необхідної для прийняття стратегічних рішень, зазвичай включає в себе: *інформацію про розвиток галузі*, в якій здійснює діяльність суб'єкт підприємництва в конкретному регіоні чи в країні в цілому, позицію керівництва регіону (країни) щодо подальшого розвитку галузі, роль і місце в ньому суб'єктів підприємництва, соціальну оцінку рівня та перспектив розвитку галузі, можливості державної підтримки галузі.

Важливою буде інформація про продукцію, яка культивується у галузі (товари, послуги, роботи), попит на неї з боку населення, місцевих громад, наявність державних замовлень на даний час чи на майбутнє. Слід також звернути увагу на тенденції, які панують у галузі, динаміку та причини їх змін. *Технологічна інформація*_– насамперед інформація про джерела та обсяги сировини, її можливу вартість та способи доставки до суб'єктів виробництва, наявність суб'єктів, здатних виступати партнерами у виробленні допоміжних матеріалів, без яких досягнення стратегічної мети буде неможливим чи значно ускладненим. Крім того, технологічна інформація має містити відомості про існуючі технології виробництва, ступінь їх досконалості та відповідності сучасним умовам, можливість опанування ними у визначенні терміни. *Комерційну інформацію* складають відомості про коньюктуру ринку, його основних суб'єктів, взаємовідносини та рівень монополізації ринку, особливості реалізації продукції та умови формування прибутку. *Соціально-кадрова інформація* має містити відомості про соціальну ситуацію, основні соціальні групи, впливові громадські об'єднання, наявність кваліфікованих фахівців для роботи у структурах суб'єкта підприємництва, характеристики криміногенної ситуації. Звичайно, що у залежності від специфіки діяльності суб'єктів підприємництва структура стратегічної інформації може бути доповнена іншими відомостями або дещо змінена.

Доцільність такого структурування стратегічної інформації пояснюється необхідністю поглянути за межі звичайної сфери діяльності суб'єктів підприємництва, тобто туди де знаходяться найбільш сприятливі або найбільш небезпечні фактори, які можуть впливати на формування стратегічного рішення. Чим більш віддалена за часом стратегічна мета суб'єкта підприємництва тим більш широкою має бути точка зору осіб, що приймають стратегічні рішення.

Тактика діяльності суб'єктів підприємництва визначає характер їх поведінки на ринку: що, з ким, як? Відповіді на такі питання формуються за

допомогою т. з. тактичної інформації. Остання має забезпечити два види потреб: вибір найбільш оптимального варіанту виконання визначених для досягнення стратегічної мети завдань і контроль умов в яких здійснюється виконання таких завдань.

У першому випадку необхідно виробити варіанти дій, які можливі за даних умов (що, в якому обсязі і коли виконати, де і за яку ціну придбати сировину, кого, на який термін і для виконання яких робіт залучити для виробництва продукції, від кого і яку отримати підтримку (згоду), через кого і кому забезпечити реалізацію продукції). Для вибору та оптимізації варіантів потрібно буде отримати інформацію, яка необхідним обсягом характеризує кожну із складових обраних варіантів. На базі такої інформації і буде прийматись остаточне рішення.

У другому випадку необхідно мати постійну інформацію про поведінку суб'єктів ринку (в першу чергу потенційних і реальних конкурентів), контрагентів, партнерів, позицію місцевих чи центральних органів влади щодо розвитку галузі, ролі суб'єктів підприємництва (в т.ч. і конкретних) у ньому, зміни (можливі зміни) політичної та правової ситуації, коньюктури ринку. Тобто, у інформаційній роботі на тактичному рівні мають бути присутні як інформаційний аудит (для першого випадку), так і інформаційний моніторинг (для другого випадку). Суб'єкти підприємництва мають бути готові до інформаційного супроводження своєї діяльності саме за такими формами інформаційної роботи. З точки зору забезпечення перспектив діяльності та враховуючи обмежені проміжки часу виконання кожного із таких завдань важливе місце будуть займати прогнози розвитку ринкової ситуації та поведінки окремих суб'єктів ринку.

Головним тут буде розуміння взаємозв'язків і тенденцій, що існують як у галузі в цілому, так і в конкретному регіоні чи на ринку. Тут у нагоді може стати досвід суб'єктів підприємництва, напрацьований ними попередньо. За таких умов інформаційне супроводження їх діяльності буде базуватись не

лише на отриманні нової інформації, а і на узагальненні тих даних, що були отримані у минулому, аналізі нової інформації у сукупності таких даних.

Оперативний рівень інформаційного забезпечення діяльності суб'єктів підприємництва передбачає зосередження зусиль на виявленні загроз конкретним операціям, які проводять суб'єкти в даний час. Інформаційні потреби тут зазвичай полягають у отриманні інформаційних характеристик щодо потенційних чи реальних клієнтів, контрагентів, партнерів для забезпечення найбільш оптимального їх вибору і мінімізації загроз співпраці з ними; інформаційних ознак, що можуть вказувати на загрозливі зміни ринкової ситуації чи взаємовідносин на ринку, поведінки клієнтів, контрагентів, партнерів; інформації про загострення політичної чи соціальної ситуації, виникнення різного роду конфліктів у оточенні суб'єктів підприємництва, екологічні та техногенні загрози. Зазвичай інформація збирається з оточення суб'єктів підприємництва (клієнти, контрагенти, підрядники, система торгівлі, партнери, кредитори, інвестори і т. і.), які, як показує практика, є потенційним джерелом досить небезпечних загроз для суб'єктів підприємництва. В той же час, слід пам'ятати, що інформація може бути цінною лише тоді коли вона може бути використана в діяльності суб'єктів підприємництва. Особливо це стосується оперативного рівня, де діяльність суб'єктів є досить динамічною і інформація може швидко старіти.

На основі отриманої інформації фахівці радять формувати наступні бази даних: конкуренція (вся інформація по наявних і потенційних конкурентах), ринки (будь-яка ринкова інформація), технології (виробництво, реалізація, використання продукції), законодавство (правові норми, які забезпечують регулювання діяльності суб'єктів підприємництва, формують умови їх контролю), ресурси (інформація про джерела, умови поставки та якість всіх видів ресурсів), загальні тенденції (політична, економічна, соціальна та інша інформація) [57].

Важливим моментом у інформаційному забезпеченні діяльності суб'єктів підприємництва є збір інформації і аналітична робота з нею. Тут

слід мати на увазі те, що будь яка інформація, яка характеризує певний об'єкт, ситуацію чи подію як би вона не була утаємничена, може бути доступною. Як показує практика, у всі види діяльності залучено досить багато фізичних чи юридичних осіб, самі ситуації та події відбуваються та утворюються також не без їх участі, щодо об'єктів, ситуацій, подій, висловлюються різного роду оцінки, думки, точки зору. Тобто, все, що відбувається у суспільному житті не залишається поза участю або хоча б увагою значної кількості громадян, засобів інформації, державних установ, що робить неможливим збереження у абсолютній таємниці будь-якої інформації, особливо коли до неї проявляється активна зацікавленість. Як правило, інформація про певні ситуації, події, поведінку суб'єктів з'являється в інформаційному просторі у вигляді чуток, що є ознакою витоку інформації і можливості її отримання. Крім того, підприємницька діяльність багата великою кількістю контактів: перемовини, обмін, поставки, купівля-продаж, розрахунки, інвестиції та кредити, прийом на роботу працівників та інших стосунків. Всі такі контакти залишають інформаційні сліди у вигляді актів, угод, контрактів, рекламної продукції, фінансових документів, які зазвичай не носять конфіденційного характеру. Враховуючи наявність значного обсягу інформації, яка перебуває у інформаційному просторі суб'єктів підприємництва та постійну її зміну, питання інформаційного забезпечення суб'єктів буде полягати у досить досконалій організації збору інформації і її ефективній обробці. Тут можна скористатись хоча і давньою, але від того не менш дієвою методикою 4к+1, яка включає 4 обов'язкові і один випадковий канал інформації [22, 57]. Перший канал має умовну назву *текст.* З цього каналу збирається спеціальна інформація необхідна для організації виробничого процесу. Це можливість отримання інформації з спеціалізованих по сферах діяльності періодичних видань, публікацій у різних загальних чи наукових виданнях, збірниках праць, банків (баз) даних, оглядів, звітів і т. і.. По даному каналу може бути отримано до 30-40% необхідної інформації.

Другий канал – *фірма* – являє собою знання всіх працівників суб'єкта підприємництва, які у ході виконання своїх обов'язків підтримують контакти з клієнтами, контрагентами, представниками державних установ, іншими особами і отримують від них відповідну інформацію. Пам'ятаючи про такий канал, доцільно, щоб підрозділ безпеки суб'єкта підприємництва ознайомив працівників з необхідними правилами ділового спілкування, елементами психотехнічної комунікації з тим, що їх взаємовідносини з особами, які співпрацюють з суб'єктами бізнесу були більш продуктивними з т. з. отримання інформації. Фахівці вказують, що з цього каналу може бути отримано до 60% інформації про конкурентів, ринок, ресурси, 15% - про технології, 15% - про документи, 10% - про тенденції та напрямки розвитку галузі чи окремих її суб'єктів.

Наступний канал має назву *консультант*. Інформація з такого каналу може отримуватись через експертів, з матеріалів їх роботи, від суб'єктів, які досліджують ринок або окремі його сегменти, осіб, що виконують аналітичну або дослідницьку роботу на ринку. Сюди ж можна віднести інформацію, яка подається у ході конференцій, семінарів, на виставках. Суб'єкти підприємництва можуть організовувати власні інформаційно-аналітичні лабораторії, замовляти аналітичні чи інші матеріали у спеціалізованих підприємств, або наймати на умовах аутсортингу певних фахівців-консультантів. З такого каналу може бути отримано – 10-15% інформації, але така інформація буде найбільш об'єктивною.

Четвертий канал – *бесіда*. Інформація отримується з різного роду зустрічей, перемовин, візитів, брифінгів, просто розмов, тобто будь-якого спілкування, в т. ч. і засобами зв'язку (електронного звязку). Головне правильно побудувати розмову, зацікавити співрозмовника у наданні інформації, пояснень, аргументів, обґрунтувань, доказів. Ємність такого каналу – 5-6% необхідної інформації. Слід пам'ятати, що крім безпосереднього отримання інформації тут формується відповідний

контакт, який може бути використаний у майбутньому.

Випадковий канал – *джокер*, може виникати тоді, коли за певних обставин випаде можливість скористатись чужою бесідою, базікою-сусідом у дорозі, втраченими (забутими) документами і т. і. Користь від такого каналу може складати від 0 до 100%.

Як можна бачити, мова у інформаційному забезпеченні підприємницької діяльності іде про інформацію відкритого доступу. Разом з тим, така інформація може бути приватною і вона, зазвичай, контролюється її власниками. Тобто, відкритість інформації не означає можливість вільного доступу до неї. Фахівці, зайняті в інформаційному забезпеченні підприємницької діяльності мають знати про це і обирати найбільш оптимальні шляхи отримання необхідної інформації. Враховуючи, що підрозділи безпеки суб'єктів підприємництва не є суб'єктами оперативно-розшукової роботи і не підпадають під дію законодавства, що регулює діяльність розвідувальних органів, а також відсутність законодавчих актів про детективну діяльність, важливим елементом інформаційного забезпечення підприємницької діяльності є аналітична робота. Аналізуючи точки зору різних фахівців, можна дійти висновку, що аналітична робота в інформаційному забезпеченні суб'єктів підприємництва являє собою формування необхідних даних для забезпечення процесу управління їх господарською, фінансовою, комерційною та іншими видами діяльності шляхом отримання та аналітичної обробки інформації. Об'єктом аналітичної роботи є інформація, що характеризує політичну, соціальну, ринкову ситуацію у сфері діяльності суб'єктів підприємництва. Аналітична робота спрямовує свою дію на формування об'єктивного бачення ситуації, яке дасть можливість керівнику суб'єкта підприємництва приймати ефективні та своєчасні рішення.

Результати аналітичної роботи мають відповісти на наступні питання:

- як, з точки зору безпеки бізнесу, характеризується ситуація (політична, економічна, соціальна, ринкова);
- які причини викликають зазначену ситуацію, які тенденції панують в ній;
- яким чином можна було б впливати на вказані причини з т. з. їх посилення чи послаблення;
- хто може бути союзником у подальшому розвитку суб'єкта підприємництва, а хто агресивним конкурентом;
- якими є основні фактори, що можуть зумовити позитивний результат управлінського рішення;
- прогноз розвитку ситуації, в т. ч. і в результаті прийняття відповідного рішення;

Змістом аналітичної роботи є приведення розрізнених відомостей в логічно обґрунтовану систему залежності (просторово-часових, причинно-наслідкових та ін.) з метою надання правильної (об'єктивної) оцінки як всій сукупності ситуації, так і кожному з окремих подій та фактів [58]. В той же час основним напрямком аналітичної роботи є прогнозування. Як показує практика, прогнозування більш за все використовується на середньому рівні управління. Для нижчої ланки воно не має суттєвого значення, оскільки вона зайнята оперативними питаннями діяльності суб'єкта підприємництва. Прогнози базуються на виявленні певних закономірностей притаманних об'єкту, діяльності, ситуації; на вивченні планів, намірів, попиту; по аналогії через виявлення подібних ситуацій і дій у минулому; через аналіз існуючих тенденцій. В той же час, прогноз завжди формується з інформації про минулі події, тобто ймовірність розвитку ситуації за прогнозом носить умовний характер. І тут не треба ставати рабом прогнозу. Останній виступає певним фактором, який враховується при прийнятті рішення [59].

7.3. Спеціальні інформаційні операції та комерційна розвідка в підприємницькій діяльності

Важливим завданням інформаційної роботи суб'єктів підприємництва в сучасних умовах є забезпечення впливу на його інформаційне середовище з метою формування позитивного іміджу суб'єктів на ринку, маскування роботи по розробці нових продуктів та дезінформації конкурентів чи кримінальних елементів у разі реального існування загроз від них. Забезпечення інформаційного впливу здійснюється шляхом проведення спеціальних інформаційних операцій.

Під спеціальними інформаційними операціями, розуміється комплекс спеціальних інформаційних заходів, які проводяться суб'єктами підприємництва протягом конкретно визначеного часу в їх інформаційному середовищі з метою формування (підтримання, відновлення) позитивного іміджу, захисту від негативного інформаційного впливу та дезорієнтації конкурентів та кримінальних елементів, які є суб'єктами загроз. Тобто, спеціальні інформаційні операції проводяться для забезпечення вигідного положення суб'єктів підприємництва на ринку, особливо при необхідності вирішення важливих для них завдань; формування сприятливої громадської думки про них, їх керівництво і персонал, укріплення (підвищення, відновлення) авторитету суб'єктів і довіри до них з боку партнерів і клієнтів; стратегічної і тактичної дезінформації конкурентів, опонентів та інших суб'єктів, від яких можуть надходити (надходять) загрози.

Основною відмінною особливістю інформаційних операцій є надання інформації в інформаційне середовище шляхом концентрації різноманітних інформаційних заходів з використанням багатьох інформаційних каналів протягом конкретно визначеного часу.

Видами спеціальних інформаційних операцій є:

- пропаганда — систематичне та активне поширення в інформаційному середовищі інформації про досягнення, переваги, масштаби діяльності

суб'єкта підприємництва, вигідність взаємовідносин з ним по різних напрямах його діяльності з метою впливу на суспільну думку і формування позитивного його іміджу. Особливістю пропаганди є те, що вона стосується не продукції суб'єкта підприємництва, а так званого його бренду, комерційного найменування. Тобто пропагується певна ідеологія поведінки на ринку, з чим якраз і пов'язується високий результат. У пропаганді використовуються пропагандистські та агітаційні матеріали: листівки, буклети, відеоматеріали, публікації ЗМІ і т. і.

Пропаганду не слід плутати з рекламою, остання спрямовується на презентацію певного товару, послуги, роботи і має вплив на індивідуальну поведінку людини. Крім того, реклама обмежується часовими межами, які обумовлюються необхідністю найбільш ефективного просування продукції на ринок. Пропаганда ж не обмежується такими термінами, вона зазвичай супроводжує діяльність суб'єктів підприємництва на всьому протязі їх існування і впливає як на емоції, так і на свідомість людей. Заходи пропаганди заздалегідь плануються і завжди мають цілеспрямований характер. Зачіпаючи духовну сферу обраної аудиторії пропаганда переконує її у правильності сприйняття того чи іншого суб'єкта та відношення до нього. Тобто, у ході пропаганди формується аудиторія позитивно налаштованих до певного суб'єкта підприємництва, громадян, колективів, соціальних груп, які завжди будуть готові підтримати даного суб'єкта. Ефективність пропаганди визначається співвідношенням фактичної кількістю залучених прихильників суб'єкта підприємництва до запланованої. Критеріями пропаганди виступають: актуальність головної тези; сприйняття її аудиторією; складність її спростування або критики. За всіх умов головна теза повинна зачіпати інтереси цільової аудиторії, тобто, вона має формуватись з потреб, очікувань, проблем, які є на даний час актуальними для аудиторії.

Слід звернути увагу на те, що у конкурентній боротьбі використовується і т. з . негативна пропаганда, яка спрямовується на формування негативного сприйняття певного суб'єкта на ринку, неадекватної

поведінки аудиторії щодо нього, його діяльності а то і продукції, яка виробляється ним. Тут, у більшості випадків здійснюється маніпулювання громадською думкою, інформацією та індивідуальною свідомістю громадян. Технології негативної пропаганди спрямовуються на створення образу поганого, шкідливого, неефективного суб'єкта підприємництва, якому не місце на ринку.

Історія підприємництва знає досить багато прийомів пропаганди, які ефективно використовуються різними суб'єктами, особливо з залученням засобів масової інформації. Окремі прийоми пропаганди подані у Додатку 8.

Слід також звернути увагу на особливості сьогоднішньої пропаганди (як позитивної, так і негативної), яка поширена в конкурентній боротьбі суб'єктів підприємництва. Заходи пропаганди все більшою мірою поширюються на соціальну поведінку людей, їх психологію, мотивацію. У пропаганді досить часто використовуються різного роду провокації, соціальні конфлікти, неправдива інформація. Головним стає виживання на ринку, в т. ч. і за рахунок інших суб'єктів;

- контрпропаганда — інформаційна реакція суб'єктів підприємництва на комунікативні дії конкурентів чи інших осіб, якими вони прагнуть забезпечити свій вплив на інформаційне середовище ринку всупереч інтересам зазначених суб'єктів.

Безумовно, що контрпропаганда проводиться з метою зниження ефективності заходів пропаганди, які використовуються конкурентами, особливо у випадках коли від таких заходів страждає імідж суб'єктів підприємництва та падає їх конкурентоздатність. У ході контрпропаганди суб'єкти підприємництва зазвичай дотримуються наступного алгоритму:

- вивчається організація пропаганди конкуруючих суб'єктів, прийоми та методи впливу на аудиторію, зміст заходів пропаганди;
- виявляються канали поширення пропагандистських матеріалів;
- вивчається аудиторія, що є об'єктом пропаганди та виявляється її громадський настрій;

- здійснюється спростування інформації поданої в пропагандистських матеріалах конкурентів;
- нав’язуються власні теми, що характеризують конкурентів для обговорення у інформаційному середовищі;
- надаються різного роду факти та їх оцінки з діяльності конкурентів, які знижують ефект заходів пропаганди;
- для контрпропаганди використовують одночасно різноманітні канали подачі інформації та різні види компрометуючих матеріалів.

Основними принципами контрпропаганди мають бути активність, оперативність, конкурентність, комплексність, гнучкість, врахування особливостей аудиторії.

- дезінформація — поширення в інформаційному середовищі суб’єктів підприємництва викривлених або неправдивих відомостей з метою введення в оману конкурентів, кримінальних елементів, інших осіб і організацій, що загрожують суб'єктам. Поширена інформація має замаскувати істинні наміри діяльності суб’єктів підприємництва. Захист інтересів суб’єктів підприємництва за допомогою актів дезінформації може здійснюватись по різних напрямках, виходячи з особливостей ситуації, в якій в той чи інший період своєї діяльності знаходиться певний суб’єкт. Зокрема такими напрямками можуть бути:

- введення в оману конкурентів стосовно термінів проведення суб’єктами заходів по підвищенню своєї конкурентоспроможності, надання на ринок нових товарів, послуг, проведення реорганізації і т. і.;
- створення ілюзії підготовки до отримання (вкладання) великих інвестицій в певні сфери економіки чи регіони або інвестування конкретних суб’єктів;
- широке висвітлення «проблем» у суб’єктів підприємництва в окремих сферах їх діяльності, критика низької якості продукції, послуг, робіт;

- «витік» спеціально занижених чи завищених економічних чи інших показників діяльності суб'єктів підприємництва, перебільшення чи заниження негативного впливу політичних, соціальних, економічних або інших умов на перспективи розвитку певних напрямів їх діяльності.

Зміст дезінформуючої інформації завжди базується на певній частині правдивих відомостей, дійсних подіях та фактах. Водночас зазначені об'єктивні відомості доповнюються інформацією, яка може не відповідати дійсності, але бути на певний час досить актуальною. Варіанти застосування дезінформації в підприємницькій діяльності показано в Додатку 9.

- чутки — усна інформація з невизначеним ступенем достовірності, що стихійно поширюється в інформаційному середовищі суб'єктів підприємництва з метою захисту їх інтересів на ринку. Чутки є неформальним каналом комунікації, по якому можна отримати до 80 % інформації, яка в окремих випадках не суттєво суперечить об'єктивній ситуації [60]. Оскільки чутками інформація передається значно швидше чим каналами формального спілкування суб'єкти підприємництва можуть формувати необхідні їм чутки для запланованого поширення в інформаційне середовище необхідних їм відомостей. Контролюючи зворотню реакцію на чутки суб'єкти можуть коригувати свою діяльність, плани та поведінку на ринку. А враховуючи, що чутки є більш впливовою інформацією суб'єкти підприємництва можуть використовувати їх для:

- формування і підтримки власного іміджу на ринку;
- прикриття їх проникнення в нові регіони чи сфери економіки, розробки нових продуктів, послуг, робіт;
- уведення в оману суб'єктів загроз;
- захисту від негативного впливу чужих чуток, які ганьблять суб'єктів;
- підготовки середовища ринку до відповідних дій суб'єктів;
- зниження напруженості у виробничих колективах, середовищі клієнтів, контрагентів та акціонерів;

- забезпечення впливу потенційних споживачів, просування на ринок нових продуктів;
- отримання незалежної думки певних груп громадян про діяльність суб’єктів та якість їх послуг, продукції, робіт;
- вивчення настрою в колективах підрозділів та установ субєктів;
- привернення уваги до відповідної події, ситуації на ринку послуг чи взагалі діяльності суб’єктів.

Деякі питання використання чуток надані в Додатках 10, 11, 12.

Особливостями сучасного бізнесу (переважно великого) є комплексне забезпечення його розвитку. Тут мають місце різного роду напрямки впливу на середовище, від політичного і до безпосередньо ринкового. Важливим виступає забезпечення впливу на владні структури, які можуть сприяти або навпаки стримувати розвиток бізнес-діяльності конкретних суб’єктів, а також на суспільство, яке дає відповідну оцінку суб'єктам підприємництва, а з нею і забезпечує попит на їх продукцію. У зв’язку з цим суб’єкти підприємництва нерідко вдаються до залучення певних представників владних кіл та авторитетних суспільних діячів у якості т. з. агентів впливу. Такими агентами можуть виступати посадові особи органів влади або інших державних інституцій, а також особи, що користуються суспільною довірою. Основним змістом у їх діяльності у якості агентів впливу є лобіювання різними способами у владному чи суспільному середовищі інтересів конкретних суб’єктів підприємництва. Користуючись своїми повноваженнями та використовуючи довіру громади такі особи формують у відповідного середовища необхідне суб’єктам підприємництва враження про їх діяльність, забезпечують прийняття позитивних рішень щодо таких суб’єктів, суспільну підтримку їх діяльності.

Формування корпусу агентів впливу та забезпечення їх ефективної діяльності є також одним із видів спеціальних інформаційних операцій. Залучення необхідних осіб до співробітництва у якості агентів впливу може здійснюватись шляхом просування «своїх людей» на відповідні посади у

апаратах влади, сприяння обранню їх до Верховної ради чи місцевих органів самоврядування, підтримки їх у певних взаємовідносинах з керівництвом, колективами, громадою, створення їм позитивного іміджу. Серед завдань, які можуть виконувати агенти впливу є наступні:

- послаблення чи нейтралізація діяльності конкурентів та інших суб'єктів шляхом нормативного обмеження їх можливостей на ринку, додаткового контролю діяльності, формування умов для притягнення до відповідальності за порушення законодавства;
- посилення позицій суб'єктів підприємництва через лобіювання їх участі у виконанні державних програм, надання державних інвестицій, розширення їх співробітництва з іноземними суб'єктами, виділення необхідних ресурсів;
- блокування прийняття нормативних актів, якими стримується чи обмежується діяльність певних суб'єктів підприємництва, робота з засобами масової інформації щодо «правильного» висвітлення діяльності суб'єктів;
- забезпечення політичної, громадської, владної оцінки та підтримки діяльності певних суб'єктів підприємництва.

У значній частині випадків агентами впливу бувають консультанти, радники, особи наближені до відповідних посадовців чи громадських діячів: секретарі, водії, члени сім'ї, близькі друзі. Важливе місце у бізнесі займає об'єктивне розуміння ринкової ситуації, взаємовідносин та поведінки суб'єктів ринку, їх намірів щодо розвитку своєї діяльності. За таких умов доцільним виступає мати за агента впливу достатньо поінформовану людину, в т.ч. і не пов'язану з діяльністю суб'єкта, з яким плануються відповідні взаємовідносини. Така людина може і не мати прямого відношення до вказаного суб'єкта, головне щоб вона знала механізм прийняття рішень. У такому випадку можна більш ефективно побудувати структуру переговорів, врахувати прийоми формування рішень та відповідним чином зацікавити співрозмовників у наданих їм пропозиціях. Крім того, агенти впливу можуть вказати з ким із керівників суб'єкта

підприємництва більш доцільно мати справу, щоб позитивно вирішити певні питання.

На даний час багато розмов точиться навколо розвідувальної діяльності в бізнесі. Можна чути про конкурентну, ділову, економічну, комерційну розвідку, бізнес-розвідку, промислове шпигунство і т. і. Разом з тим, всі ці романтичні та інтригуючи назви по суті своїй розкривають одну і ту ж діяльність — отримання необхідної для діяльності суб'єктів підприємництва інформації з джерел, доступ до яких обмежено. Професіонали знають, що коли ми застосовуємо поняття розвідка, то однозначно розуміємо, що така діяльність не обмежує себе роботою з відкритими джерелами інформації. Тому натяки деяких авторів на те, що шпигунство ґрунтується на незаконних методах добування інформації, а розвідка — на законних, м'яко кажучи є не зовсім об'єктивним розумінням даного питання. Усім давно відомо, що діяльність сил розвідки будь-якого походження спрямовується насамперед на розкриття певних таємниць, стосовно яких їх власники вживають заходів захисту. Порушення таких заходів чи оминання їх може межувати з порушенням певних правових норм. В деяких країнах законодавство щодо захисту інформації є недосконалим (в тому числі і в Україні) і професійні розвідники знаходять шляхи отримання таємної інформації насамперед через прогалини в правових нормах із захисту інформації та прогалини в організації захисту своїх таємниць їх власниками. Основною ж особливістю розвідувальної діяльності є не стільки правомірність її дій щодо проникнення до інформації з обмеженим доступом, а якраз таємний її характер. Саме таємничість форм, методів, взаємовідносин, що встановлюються у ході отримання інформації, невідомість конкретних суб'єктів, задіяних в розвідувальній діяльності, а то і самого факту такої діяльності робить розвідку Розвідкою.

Незважаючи на існуючі умови щодо розвідувальної діяльності у бізнесі, певна частина суб'єктів підприємництва все ж таки вдається до відповідних заходів розвідувального характеру. Інформація ж, яку

отримують суб'єкти підприємництва в результаті дій їх сил розвідки носить здебільшого комерційний характер і використовується насамперед для забезпечення їх комерційної діяльності. Основним змістом цієї інформації є характеристика ділових стосунків конкурентів, інших суб'єктів, перспективи їх поведінки на ринку, наміри в комерційній діяльності. Тому думки автора сходяться на тому, що діям сил розвідки суб'єктів підприємництва, які пов'язані із забезпеченням комерційної їх діяльності (що і є предметом підприємництва) більш притаманна назва комерційної розвідки. А оскільки такі дії мають місце у вітчизняному бізнесі, може бути корисним розгляд деяких аспектів розвідувального забезпечення суб'єктів підприємництва. Тут слід звернути увагу на те, що до професійних дій з розвідки вдаються зазвичай суб'єкти великого бізнесу, оскільки їх можливості дають змогу забезпечити таку діяльність як професійно та матеріально, так певним чином і з правової точки зору.

Враховуючи, що отримання інформації з обмеженим доступом відповідно до чинного законодавства може бути здійснено лише з дозволу її власника, силам розвідки необхідно провести відповідну роботу з ним, розпорядником чи принаймні володільцем такої інформації. В арсеналі розвідки достатньо методів формування позитивних для неї відносин з подібними суб'єктами і як показує практика, доволі часто вдається отримати доступ до інформації, яка цікавить суб'єктів підприємництва.

Слід також звернути увагу і на норми чинного законодавства, які визначають умови доступу до інформації, що є конфіденційною чи таємною. Так, згідно ст. 162 Господарського кодексу України особа, яка самостійно і добросовісно одержала інформацію, що є комерційною таємницею, має право використовувати цю інформацію на свій розсуд. Тлумачення поняття «самостійно» подається українськими словниками як — здійснення своїми силами, з власної ініціативи, без сторонньої допомоги [61]**.** Таке розуміння зазначеного поняття означає, що право збирати інформацію, яка є комерційною таємницею є можливим тільки за умов передбачених ст. 162 Господар-

ського Кодексу України. Наприклад, у разі коли інформація отримана у зв'язку з якимось недоглядом власника інформації. До речі, однією з ознак належності інформації до комерційної таємниці є вжиття щодо неї заходів захисту, одним з яких є запровадження спеціального діловодства. Як показує досвід, сучасні суб'єкти підприємництва, власники інформації з обмеженим доступом проводять заходи спеціального діловодства лише за рідким виключенням. Тому дії комерційної розвідки, щодо отримання інформації з обмеженим доступом у таких суб'єктів будуть правомірними, оскільки їх інформація не набула ознак таємності. Але за всіх умов подібні дії є досить ризиковими і вимагають серйозного професіоналізму та глибоких правових знань.

В той же час, розглядаючи перспективи вітчизняного підприємництва та враховуючи іноземний досвід слід зазначити, що комерційна розвідка поширена у багатьох компаніях світу.

За оцінками західних експертів витрати на комерційну розвідку становлять у середньому 1,5% обороту торгових концернів і транснаціональних корпорацій. Частка компаній у світі, які використовують можливості комерційної розвідки складають: Японія – 99,99%, США – 82%, Великобританія – 75%, Німеччина – до 68%, Франція – до 52%, Іспанія – 35%, Росія – 7-9%, Україна – до 5% [62].

Як бачимо, у нас ринок розвідувальних послуг досить обмежений і значним чином відстає від більшості розвинутих країн. У результаті суб'єкти підприємництва вимушені силами своїх підрозділів безпеки здійснювати розвідувальні заходи, що під силу лише представникам великого бізнесу. Крім того, комерційна розвідка зазвичай діє в інтересах забезпечення безпеки компаній, в той час як питання їх стратегічного розвитку та діяльності залишаються без розвідувального забезпечення.

Основними принципами розвідки в діяльності суб'єктів підприємництва можна вважати: здійснення заходів розвідки в межах чинного законодавства; добування інформації силам розвідки без порушення

прав, свобод, честі і гідності громадян; використання добутої інформації виключно в комерційних інтересах; виконання заходів розвідки на професійних засадах; легендування діяльності сил розвідки суб'єктів підприємництва [63]. Враховуючи особливу специфічність взаємовідносин у сфері комерційної розвідки важливо забезпечити морально-етичні норми таких взаємовідносин. Всі зв'язки, які підтримуються силами розвідки з джерелами інформації мають носити конфіденційний характер, а методи роботи з джерелами повинні обиратись найменш небезпечні. Слід всіляко уникати ситуацій за яких для джерел інформації можуть виникати різного роду небезпеки та загрози. У всіх можливих випадках сили розвідки мають дбати про здорові зв'язки з джерелами інформації, надавати при необхідності їм допомогу. У розвідувальній діяльності не слід користуватись послугами кримінальних елементів, суб'єктів з негативною репутацією, вдаватись до крадіжок документів, інших носіїв інформації якщо це може зашкодити джерелам інформації. За всіх умов сили розвідки мають бути обов'язковими до своїх джерел інформації, виявляти до них повагу, вживати заходів захисту зв'язків з ними. Ні в якому разі не слід застосовувати силу, залякування, будь-які аморальні дії до джерел інформації.

Середовище комерційної розвідки можуть складати посередники, клієнти, конкуренти, контрагенти, кредитори та інвестори, громадські та політичні об'єднання. Ключовим моментом у комерційній розвідці є інформаційно-пошукова робота, яка може розумітись як комплекс соціальних заходів, спрямованих на виявлення місць зосередження необхідної інформації та її джерел, формування умов та забезпечення процесу отримання інформації. В умовах відсутності правового регулювання здійснення комерційної розвідки основними її способами можуть бути: вивчення наявної інформації, опитування, спостереження, огляд, отримання довідок, використання спеціальних програм пошуку необхідної інформації в глобальному інформаційному середовищі, співпраця з фахівцями, експертами, консультантами, фото- відео зйомка, вивідування інформації,

оманливі перемовини з працівниками об’єктів інформації і т. і. Пошук необхідної інформації здійснюється у просторі та часі шляхом виявлення її демаскуючих ознак та їх ідентифікації з еталонною структурою, змістом, поведінкою об’єкта, джерела, знаннями про них. Разом з тим, необхідно акцентувати, що комерційна розвідка на відміну від інформаційно-аналітичної роботи здійснює свою діяльність не в інформаційному, а в комунікаційному середовищі. Тому її кінцевим результатом є не власне інформація, а зміни в компанії, які проходять під впливом такої інформації. З врахуванням такої інформації сили безпеки розробляють моделі загроз розвитку компанії, сценарії можливих криз, визначають ознаки їх наближення. Підготовка до таких загроз та криз і буде змістом тих змін, які відбуваються у суб’єктів підприємництва за результатами діяльності сил комерційної розвідки [64]. Тобто, комерційна розвідка в діяльності суб’єктів підприємництва являє собою певну систему збору, обробки, аналізу, зберігання та використання інформації, класифікації ознак загроз та криз, які можуть зачіпати діяльність суб’єктів і негативно впливати на їх розвиток, систематизацію таких ознак і розробка на їх основі прогнозів можливого розвитку ситуацій в яких суб’єкти здійснюють свою діяльність або подій, що відбуваються за їх участю.

Актуальність комерційної розвідки в сьогоднішніх умовах обумовлюється насамперед тим, що при наявності великого обсягу інформації, необхідної для прийняття управлінських рішень керівники суб’єктів підприємництва користуються даними і оцінками наданими їм їх менеджерами. В той же час, менеджери, будучи працівниками функціональних підрозділів, як правило, проінформовані одностороннє і зазвичай не мислять категоріями загальних інтересів компанії (фірми, підприємства, банку). Звідси кожен з таких менеджерів прагне підкреслити їх точку зору як найбільш об’єктивну і не помічати деталі, які з їх погляду не варті уваги, оскільки не торкаються функцій їх підрозділів. За таких умов керівники суб’єктів підприємництва попадають у інформаційну залежність

від своїх менеджерів і не маючи об’єктивних критеріїв оцінки цінності наданої їм інформації, приймають не зовсім ефективні рішення. Таким недоліком не страждає комерційна розвідка, оскільки є нейтральною до всіх підрозділів, напрямків діяльності суб’єктів підприємництва та позицій менеджерів.

Враховуючи зазначене, комерційна розвідка має долучатись до вирішення наступних завдань діяльності суб’єктів підприємництва:

- пошук шляхів розвитку суб’єктів здатних забезпечити їм суттєві переваги на ринку;
- розробка принципово нових підходів до ведення бізнесу, які можуть забезпечити суб'єктам позитивні перспективи розвитку;
- своєчасне викриття планів конкурентів по досягненню конкурентних переваг, формування небезпечних для суб’єктів поведінки та дій [65].

Важливе місце у ІАР займає інформування керівництва та працівників суб’єктів підприємництва. Як показує досвід така робота організовується в порядку наданому на Рис. 7.4.

Основними вимогами до процедури інформування є: відповідність потребам осіб, яким надається інформація, конкретність, обґрунтованість , достовірність, своєчасність, зручна форма і зрозумілість інформації.

Щоб інформація, яка надається певним особам у ході інформування була переконливою і збуджувала їх до прийняття необхідних рішень, доцільно дотримуватись наступних правил:

- висвітлення в матеріалах інформування небезпек і загроз має бути поєднано з негативними наслідками, які можуть настати для суб’єкта підприємництва у разі їх реалізації;
- надання показників, що характеризують захисні функції суб’єкта як таких, що не можуть гарантувати його захист при реалізації зазначених небезпек і загроз;

- обґрунтування можливих шляхів, термінів та умов реалізації небезпек і загроз щодо діяльності суб'єкта;

- розрахунок обсягів втрат, шкоди, яких може бути завдано суб'єкту від реалізації небезпек і загроз;

- надання інформації про можливі способи, шляхи, заходи, застосування яких буде сприяти мінімізації небезпек і загроз з обґрунтуванням можливого розвитку ситуації;

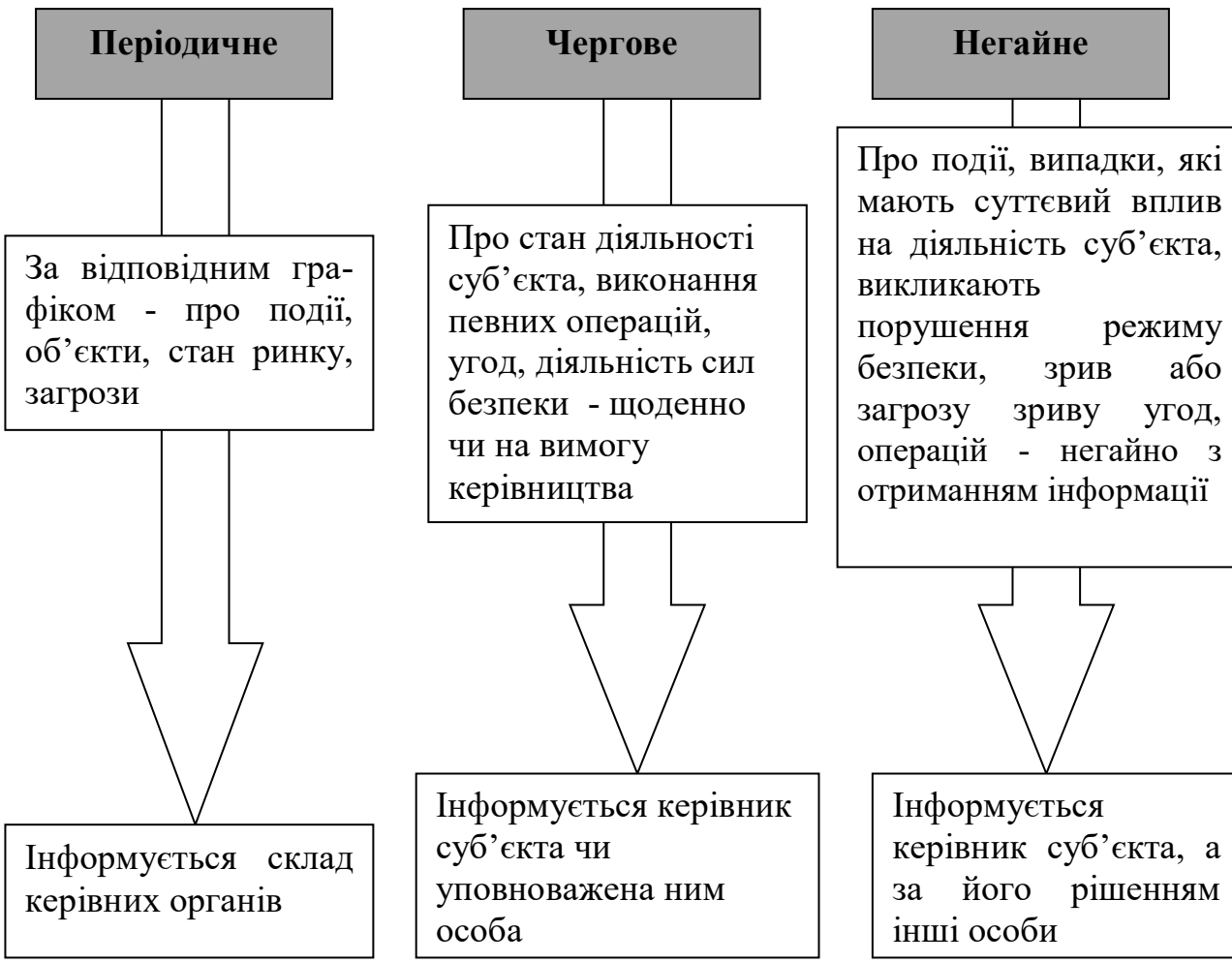


Рис. 7.4. Порядок інформування керівництва та персоналу суб'єкта підприємництва.

- обґрунтування результатів вжиття запропонованих заходів, використання шляхів і способів мінімізації небезпек і загроз.

Таким чином, інформаційне забезпечення діяльності суб’єктів підприємництва є важливою умовою сучасного їх функціонування, суттєвим елементом їх безпеки та головною підставою високого статусу на ринку. Водночас інформаційне забезпечення є досить складним, трудомістким видом діяльності, який вимагає до себе постійної уваги.

8. Протидія інформаційно-психологічному впливу в підприємницькій діяльності

Говорячи сьогодні про використання інформаційних технологій для впливу на масову і індивідуальну свідомість, певну ситуацію чи об'єкт – це «відкривати Америку». У даний час це не новина. Зазначені технології широко використовуються практично у всіх сферах життєдіяльності, в т. ч. і в бізнесі. В той же час, звертає на себе увагу те, що розвиток засобів, методик та технологій інформаційного впливу за своїми темпами значно випереджує розвиток способів та технологій захисту від нього та протидії негативним його наслідкам. Маємо акцентувати, що в основі інформаційного впливу знаходяться технології маніпулювання інформацією та свідомістю мас чи окремих людей (Рис. 8.1).

У технологіях інформаційного впливу широко використовується відомий закон філософії – боротьби протилежностей. Будь-яка подія, діяльність, ситуація,завжди має дві протилежні властивості – позитивну та негативну. Змінюючи акценти з однієї на іншу можна посилювати одну з них: добре, погано; добро, зло. У більшості випадків таким чином можна впливати на емоційне сприйняття людиною (колективом, громадою) відповідної інформації. Тут використовуються кількісні показники, що характеризують протилежні властивості, наприклад витрати і отримані результати. В бізнесі за критерій таких показників можуть братись гроші або рейтинги. Маніпулюючи їх показниками можна формувати відповідне розуміння, оцінку того чи іншого суб'єкта в очах колективу, громади, суспільства в цілому.

Значне місце у технологіях маніпулювання займає обман, неправдива інформація. Остання приносить швидку вигоду, хоча і не тривалу. Тому такі технології передбачають підтримання відповідного стану в колективах, суспільстві подачею обману протягом значного періоду. У свою чергу обман

призводить до формування пасивної поведінки, апатії, застою, невдоволення, руйнування моральних принципів.

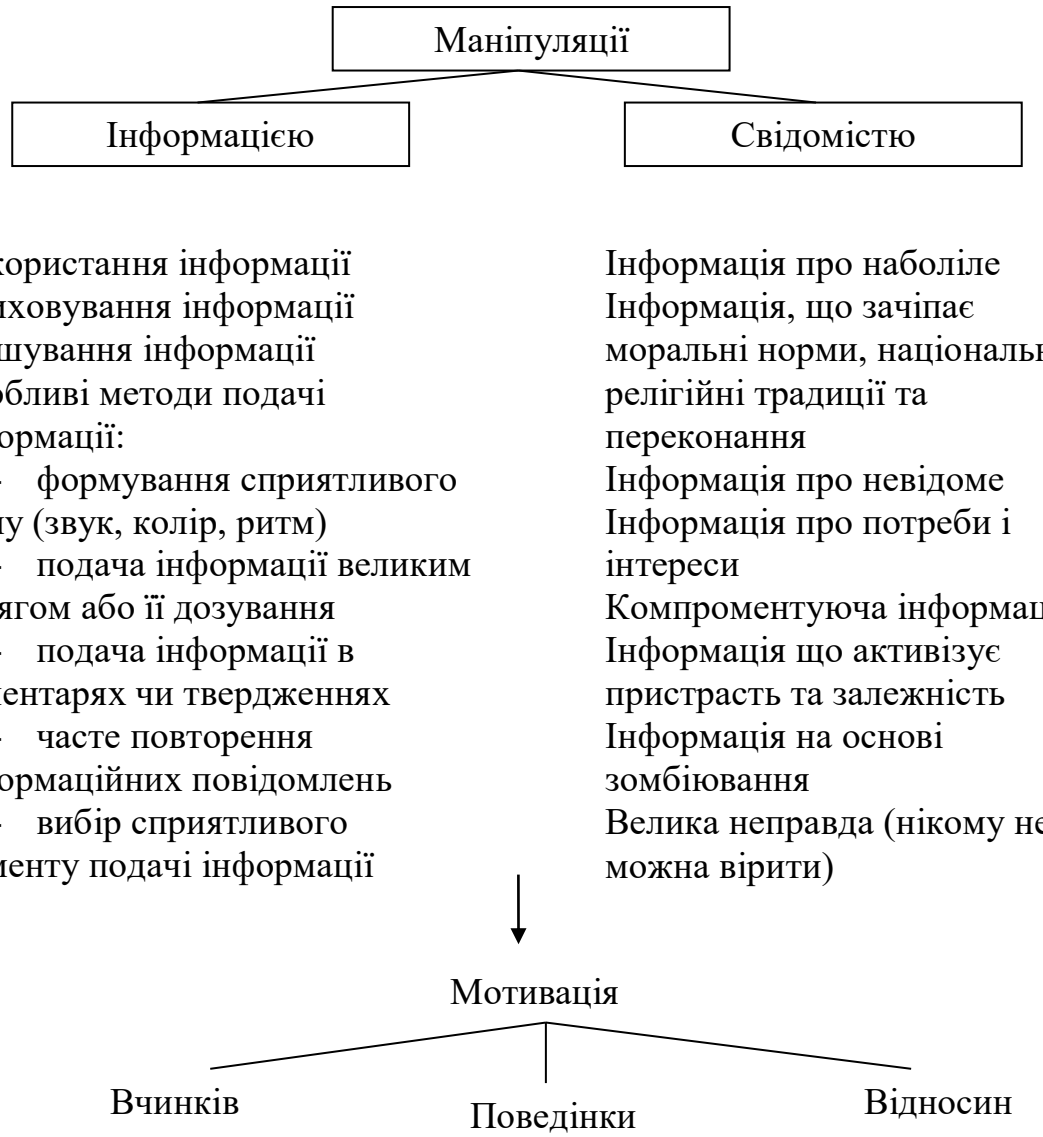


Рис. 8.1. Маніпулювання інформацією та свідомістю у сучасних інформаційних технологіях

Поширення технологій маніпулювання інформацією та свідомістю, яка має місце у суспільстві і бізнес-відносинах може призвести до суспільної та економічної деградації. Принаймні така загроза сучасних умов інформаційного розвитку є реальною.

Враховуючи відносну новизну протидії заходам маніпуляції та інформаційно-психологічного впливу в діяльності суб’єктів підприємництва

можна бачити, що підрозділи безпеки останніх є досить обмеженими і діють не завжди адекватно тим загрозам, які утворюються від такої ситуації в інформаційному просторі. У даному випадку мова іде саме про ситуації коли технології інформаційно-психологічного впливу створюють передумови для збитків та втрат суб'єктів підприємництва. Розглядаючи питання протидії інформаційно-психологічну впливу слід звернути увагу на те, що він є одним із інструментів інформаційного протиборства або вищої його стадії інформаційної війни суб'єктів ринку. У даному випадку заходи інформаційно-психологічного впливу застосовуються з метою нанесення шкоди суб'єкту щодо якого вони застосовуються. Захист суб'єктів підприємництва від інформаційно-психологічного впливу, як правило, здійснюється шляхом мінімізації ризику отримання негативного результату від нього. Водночас, як показує досвід, тільки заходами мінімізації вказаного ризику суттєвої зміни ситуації не досягається. Тут необхідно значним чином активізувати саме протидію інформаційно-психологічному впливу. Важливим моментом у цьому випадку є вибір об'єкту протидії. Насамперед, необхідно захистити власний персонал, в першу чергу шляхом впровадження в роботу з ним заходів, спрямованих на руйнування тих інформаційно-психологічних конструкцій, які з'являються у персоналу під чужим впливом. Разом з тим, об'єктом тут мають виступати інформаційне середовище, через яке поширюються заходи інформаційно-психологічного впливу та сам суб'єкт, який є зацікавленою стороною в поширенні такого впливу, а також суб'єкти через які поширюється такий вплив. Тобто, протидія має проводитись не з метою захисту. Основна мета протидії інформаційно-психологічному впливу — припинення його проведення. Важливим тут буде зрив та нейтралізація заходів інформаційно-психологічного впливу, що проводяться проти певних суб'єктів підприємництва.

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

В повсякденній діяльності людина зазвичай не має часу детально аналізувати складний механізм здійснення інформаційного протиборства. Для прийняття рішень вона використовує значно спрощені моделі, готові погляди, точки зору, якими характеризуються певні події, випадки, суб'єкти діяльності, конкретні особи. Враховуючи таку ситуацію при здійсненні інформаційно-психологічного впливу важливим є формування таких моделей і надання їх в інформаційний простір або до конкретного об'єкта. Такий підхід значним чином спрощує розуміння процесів, що відбуваються для споживачів інформації. Адаптація таких моделей в інформаційному просторі та у свідомості людини практично є програмуванням її психіки. Досвід ведення інформаційних війн наказує, що існує декілька моделей, які в різних комбінаціях застосовуються для забезпечення інформаційно-психологічного впливу на протидіючі сторони. Тобто протидія впливу — це не що інше як такий же самий вплив з метою руйнування методології, задумів, технологій проведення інформаційного протиборства.

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

- мотиваційна (ціннісні орієнтири, переконання);
- сфера потреб та інтересів, бажань, потягів;
- інтелектуально-пізнавальна (знання, пам'ять, мислення);
- емоційно-вольова (емоції, почуття, настрої, вольові процеси);
- комунікативна (характер і особливості спілкування, взаємини з людьми, між особисті сприйняття);

- функціональна (виконання службових і посадових обов'язків, дисциплінованість) [1].

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

У разі, коли об'єктом протидії впливу обирається інформаційне середовище суб'єкти підприємництва готують і проводять за відповідними технологіями (моделями) заходи контрпропаганди, спрямовані на руйнування ефекту, якого очікують особи, що ведуть проти зазначених суб'єктів інформаційну війну. З метою посилення протидії інформаційно-психологічному впливу в інформаційному середовищі можуть формуватись групи підтримки, однодумців, громадські об'єднання з клієнтів, акціонерів, інших осіб за допомогою яких здійснюється поширення сформованих суб'єктами підприємництва моделей протидії в інформаційному середовищі. В окремих випадках можуть проводиться певні акції: мітинги, демонстрації, пікети, громадські вимоги в підтримку вказаних суб'єктів. За таких умов буде здійснюватись не тільки гуртування громадян навколо суб'єктів, а і відповідна трансформація колективної свідомості. Доповненням до цього може бути поширення позитивних для суб'єктів та руйнівних для технологій інформаційно-психологічного впливу чуток та міфів.

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

- виявлення особи, якою ініціюється проведення інформаційно-психологічного впливу на певний суб'єкт підприємництва та осіб через яких здійснюється такий вплив;

- розкриття негативного змісту діяльності зазначених осіб у засобах масової інформації та іншим шляхом в інформаційному середовищі суб'єкта підприємництва;

- звернення до органів влади, правоохоронних органів, Антимонопольного комітету, суду, громадськості з вимогами щодо припинення проведення щодо суб'єкта негативного інформаційно-психологічного впливу;

- залучення до протидії інших суб'єктів (партнерів, клієнтів, акціонерів) та вжиття спільних заходів щодо протидії інформаційно-психологічному впливу;

- формування компрометуючих інформаційних моделей протидії та поширення їх в інформаційному середовищі щодо осіб, якими проводяться дії інформаційно-психологічного впливу на суб'єктів підприємництва.

Звичайно, що виконання такої роботи для підрозділів безпеки суб'єктів підприємництва є новим і в більшості своїй вони не готові до таких дій. Але водночас саме ці підрозділи за своїм функціональним призначенням є найбільш придатними для виконання заходів протидії інформаційно-психологічному впливу. Якраз вони володіють інформацією, необхідною для організації і проведення таких дій, а опанування технологіями протидії забезпечить їм необхідні умови для ефективної їх реалізації у разі інформаційного протиборства чи інформаційної війни на ринку.

9. Управління інформаційними ризиками в діяльності суб'єктів підприємництва

Пошук заходів з попередження шкоди, заподіяної від реалізації інформаційних загроз, може бути забезпечено через систему управління інформаційними ризиками.

Зазначена система управління має забезпечувати не тільки надійний захист інформаційних ресурсів, але й сприяти ідентифікації інформаційних ризиків, виявленню факторів та умов їх появи, забезпечувати їх мінімізацію у процесі діяльності суб'єкта підприємництва

Процес управління інформаційними ризиками передбачає проведення процедур аналізу, оцінки, контролю і мінімізації ризиків.

Аналіз ризиків передбачає їх визначення та оцінювання. Під час визначення ризиків встановлюють, які саме інформаційні ризики можуть існувати чи існують в діяльності суб'єкта підприємництва або в процесі проведення ним конкретної комерційної чи будь-якої іншої операції, яким чином вони можуть вплинути на діяльність чи операцію та яка існує ймовірність настання негативних наслідків від дії ризику.

Оцінювання інформаційного ризику передбачає оцінку обсягу шкоди, яку може зазнати суб'єкт унаслідок впливу зазначеного ризику.

Контроль інформаційних ризиків передбачає проведення заходів щодо з'ясування умов, за яких такі ризики можуть бути мінімальними, суттєвими або значними.

Мінімізація інформаційних ризиків передбачає вжиття заходів, спрямованих на зниження ймовірності негативного впливу ризиків, їх уникнення або зменшення їх обсягу. Одним з напрямів мінімізації інформаційних ризиків у разі, коли неможливо їх уникнути, може бути розподіл їх вартості в часі, щоб зменшити одночасний тиск ризику у певні миті діяльності суб'єкта чи здійснення ним певної операції.

Найпоширенішим варіантом мінімізації інформаційних ризиків є передача їх іншому суб'єкту, передусім за рахунок страхування ризиків.

Враховуючи багатовекторність використання інформації в діяльності суб'єктів підприємництва та можливість формування різноманітних для нього загроз управління інформаційними ризиками суб'єктів має передбачати:

- управління системою захисту інформації;
- управління процесом інформаційного забезпечення підприємницької діяльності суб'єкта;
- управління заходами з протидії інформаційному впливу;
- створення самої системи управління.

Ураховуючи те, що в ході діяльності суб'єктів підприємництва зосереджуються доволі значні обсяги інформації в т. ч. і з обмеженим доступом (банківська, комерційну таємниці, конфіденційна інформація) та те, що зазначені суб'єкти мають самостійно вживати заходів захисту своїх інтересів на одне із перших місць випливають питання аналізу, контролю та мінімізації втрати інформації. Головним в аналізі ризиків втрати інформації є виявлення способів несанкціонованого доступу до інформації суб'єктів підприємництва та її найбільш уразливих носіїв. Під час проведення такого аналізу слід виходити з того, що інформація може бути зосереджена переважно в двох групах її носіїв: комп'ютерній інформаційній мережі та в працівників суб'єктів підприємництва. Звідси несанкціонований доступ до інформації може бути здійснено, з одного боку, за допомогою технічних і програмних засобів, а з другого — за допомогою засобів інтелектуального та психологічного характеру. Ураховуючи, що поведінка людей, працівників, є доволі непередбачуваною, а телекомунікаційні системі суб'єктів підприємництва в умовах значного розвитку штучного інтелекту є уразливими, можна говорити, що ризики втратити суб'єктами їх інформації зосереджені головним чином на таких її носіях, як персонал і телекомунікаційні системи.

Оцінювання ризиків втрати інформації передбачає оцінку вартості інформаційних ресурсів, щодо яких існує ризик втрати, та оцінку власне самого ризику як імовірності реалізації певної загрози, у даному разі пов'язаної з втратою інформації. Вартість інформації оцінюється через її комерційну цінність, яка, своєю чергою, визначається через розміри збитків (шкоди), які можуть настати у зв'язку з її втратою, обсягом (перспективами) вигоди, яку може отримати суб'єкт підприємництва, використовуючи наявну в нього інформацію, а також витрати, пов'язані з виробленням, отриманням і захистом такої інформації. Щодо банківської таємниці, то її цінність може бути визначена через обсяги залучених коштів від клієнтів банку, інформацію про комерційну та фінансову діяльність яких він зберігає.

На оцінювання власне ризику як імовірності реалізації певної загрози щодо відповідної інформації впливає кілька різноманітних показників. Головними серед них є привабливість інформації для суб'єктів загроз, її цінність, актуальність, доступність, рівень захисту. Через ці показники визначається рівень критичності інформації. Скажімо, для інформації про фінансову діяльність суб'єктів підприємництва рівень критичності може бути доволі високий, незважаючи на вжиття ними заходів її захисту. Це насамперед пов'язане з тим, що доступ до такої інформації має значна кількість осіб (працівники фінансових підрозділів суб'єктів, керівники установ, працівники банків, податкових органів, антимонопольного комітету, КРУ, представники інших державних установ, працівники телекомунікаційних систем, служби безпеки суб'єктів підприємництва), а в проведенні платежів задіяно дуже багато технічних засобів та інформаційних мереж, за допомогою яких така інформація передається. Ризик доступу до зазначеної інформації буде тим вище, чим активніше здійснюють свої фінансові операції суб'єкти підприємництва (проведення платежів, отримання кредитів, операції з цінними паперами, валютою, пластиковими платіжними засобами). Крім того, береться до уваги ділова активність суб'єктів підприємництва, їх роль і місце на ринку, конкурентна поведінка. У цьому разі інформація про фінансовий

стан та діяльність суб'єктів підприємництва буде доволі привабливою для їх конкурентів і останні намагатимуться її отримати.

Якщо суб'єкт підприємництва обслуговується лише в одному банку, то ризик посягань на його інформацію буде дещо нижчим порівняно з тим, коли свої фінансові операції він проводить в різних банківських установах. Виходячи з цього, ймовірність реалізації загроз, як, власне, ризик втрати інформації може бути високою (коли показники діяльності суб'єктів підприємництва, особливо фінансової та комерційної набувають суттєвої актуальності), середньою (за умов високої актуальності хоча б одного показника) і звичайною (для суб'єктів, які не відрізняються високою активністю на ринку).

Контроль ризиків втрати інформації забезпечується шляхом проведення періодичних перевірок та аналізу стійкості інформаційної системи суб'єктів підприємництва до внутрішніх і зовнішніх загроз, своєчасного виявлення уразливих місць в її захисті. Крім того, на основі постійного моніторингу інформаційного середовища діяльності суб'єктів виявляють ознаки небезпек і загроз їх інформації. Особливу увагу приділяють виявленню осіб (як фізичних, так і юридичних), взаємовідносини суб'єктів підприємництва з якими можуть утворю вати для них певні ризики втрати інформації, а також осіб, діяльність яких може бути спрямована на несанкціоноване оволодіння інформацією, суб'єктів.

Крім того, тут слід звернути увагу і на ризики, що випливають з поведінки персоналу суб'єктів підприємництва як одного із небезпечних джерел витоку інформації. У цьому разі їх персонал можна розглядати як активний елемент інформаційної системи, здатний виступати не тільки творцем і джерелом інформації, а й суб'єктом протиправних дій щодо інформаційних об'єктів. Працівники суб'єктів підприємництва можуть як володіти, так і поширювати інформацію в межах своїх функціональних обов'язків. Крім того, вони здатні її аналізувати, узагальнювати, робити відповідні висновки, а за певних умов — розголошувати, продавати,

незаконно використовувати або незаконно передавати третім особам. На можливість посягань на інформацію суб'єктів підприємництва з боку його працівників вказують результати досліджень іноземних фахівців щодо структури виробничих колективів (Рис. 9.1). Зі 100 % працівників суб'єктів підприємництва 75 % можуть здійснити посягання на інформацію суб'єктів.

Питання мінімізації ризику втрати інформації є доволі серйозним для суб'єктів підприємництва однак чи всі ризики необхідно мінімізувати, і якщо так, то до якого ступеня? З досвіду відомо: як би суб'єкти підприємництва ні намагалися виключити ризик втрати інформації, зробити це майже неможливо. Крім того, їх керівництво повинно бути орієнтоване на певний ризик втрати інформації, щоб виникнення якоїсь непередбаченої ситуації не стало проблемою, яку неможливо вирішити. У цьому разі суб'єкти підприємництва завжди передбачатимуть дії на випадок втрати інформації, розраховувати свої можливості по ліквідації наслідків і бути готовими до неадекватного розвитку ситуації в інформаційних взаємовідносинах із своїми кредиторами, клієнтами, акціонерами, партнерами, контрагентами та іншими особами.

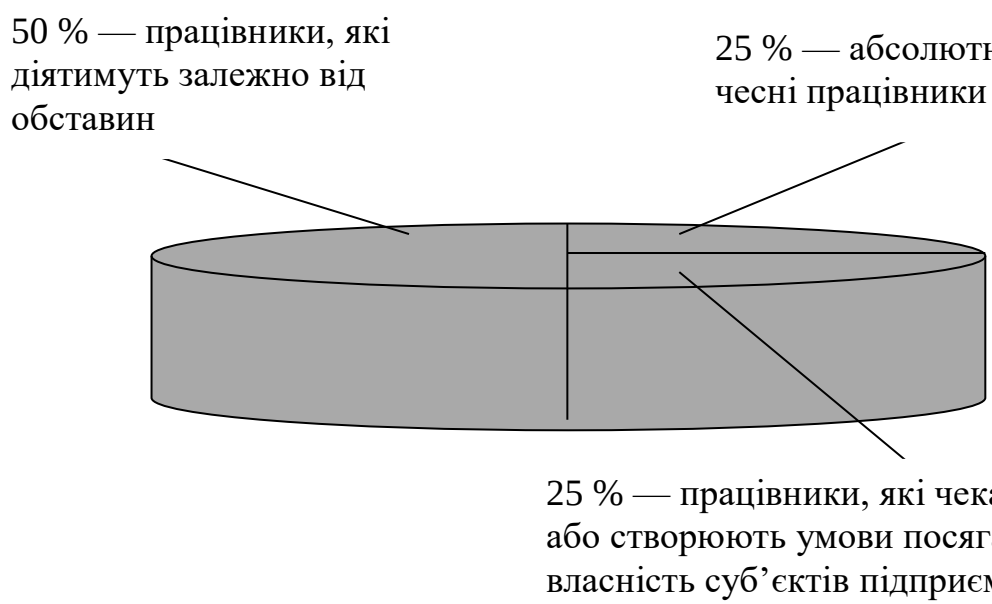


Рис. 9.1. Структура виробничих колективів за критерієм готовності до посягань на інформацію суб'єкта підприємництва

Водночас для зниження (мінімізації) ризику втрати інформації суб'єкти підприємництва мають вживати відповідних заходів, диференціюючи їх відповідно до певних загроз. Серед таких заходів насамперед мають бути:

- формування правових умов захисту інформації безпосередньо в установах суб'єктів підприємництва. Під такими умовами слід розуміти розробку нормативно-правових документів стосовно захисту всіх видів інформації (документованої, електронної, а також інформації, яка існує у вигляді знань працівників суб'єктів). Зазначеними документами мають регулюватись взаємовідносини суб'єктів підприємництва з їх працівниками, клієнтами, партнерами, кредиторами, контрагентами, іншими особами щодо доступу до інформації суб'єктів, прав щодо її отримання та захисту, відповідальності за неправомірну поведінку стосовно інформації, яка має обмежений доступ;
- створення системи захисту інформації, яка функціонує в інформаційній мережі. Зазначена система має передбачати комплекс організаційних, технічних, апаратних, криптографічних заходів і забезпечувати гарантований захист від посягань на електронну інформацію суб'єктів підприємництва.
- забезпечення контролю за носіями інформації, насамперед працівниками суб'єктів підприємництва, стосовно дотримання ними встановленого режиму захисту інформації, своєчасне реагування на всі збої в захисті інформації, що зберігається та функціонує в інформаційних мережах суб'єктів;
- запровадження надійної системи документообігу в установах суб'єктів підприємництва (службового та спеціального діловодства), яка виключала б можливість несанкціонованого доступу до документів, їх втрати, знищення чи модифікації;
- забезпечення надійної охорони установ суб'єктів підприємництва, особливо з погляду виключення можливості

несанкціонованого доступу до їх документів чи електронних носіїв інформації.

Таким чином, управління інформаційними ризиками з позиції мінімізації загроз втрати інформації є доволі трудомістким і багатогранним процесом, який охоплює різні види організаційної, правової, інженерно-технічної, кадрової та безпосередньо інформаційної роботи.

Управління ризиками, що виникають у процесі формування суб'єктами підприємництва інформаційного ресурсу, носить особливий характер. Справа в тім, що тут існує певна проблема, пов'язана з необхідністю суттєвого інформаційного забезпечення діяльності суб'єктів підприємництва відсутністю для цього відповідного правового регулювання. Як уже вказувалось, нині в Україні немає законодавства, яке регулювало б права, умови та порядок доступу суб'єктів підприємництва до джерел інформації, що необхідна їм для забезпечення їх діяльності. Відсутність такого законодавства створює безліч ризиків, які виникають у процесі інформаційного забезпечення насамперед фінансових, комерційних, господарських та інших операцій. Аналіз ризиків, що можуть виникати під час формування інформаційного ресурсу суб'єктів підприємництва за умов відсутності необхідного правового регулювання, показує, що найпоширенішими серед них можуть бути ризик відсутності необхідної суб'єктам підприємництва інформації, ризик отримання та використання неповної, необ'єктивної інформації, ризик дезінформації. Особливу небезпеку створюють ризики, які виникають під час інформаційно-аналітичного дослідження контрагентів, клієнтів, інших осіб, з якими суб'єкти підприємництва встановлюють відповідні відносини.

Ризик відсутності інформації може виникати, коли суб'єктам підприємництва в короткі терміни потрібна буде конкретна інформація, або коли об'єкти й джерела певної інформації невідомі. Особливо такі ситуації можуть бути характерними у комерційній діяльності суб'єктів підприємництва під час проведення фінансових операцій, а також у ході

прийняття управлінських рішень, особливо у процесі фінансового моніторингу сумнівних операцій та ідентифікації осіб, щодо яких є підозра в легалізації (відмиванні) коштів, отриманих незаконним шляхом. Відсутність необхідної інформації призводить до прийняття необ'єктивних рішень і як наслідок неефективних дій на ринку.

Ризик отримання та використання неповної та необ'єктивної інформації існує завжди і саме такою ситуацією, як правило, характеризується функціонуванням сучасного підприємництва. Ситуація невизначеності при прийнятті рішень є характерною для бізнес-діяльності, але тут важливим є те, щоб ризик використання такої інформації не призводив до неефективної діяльності та збитків. Тобто, якщо ризик відсутності інформації є менш імовірним, то ризик отримання та використання неповної чи необ'єктивної інформації практично буде присутнім завжди у діяльності суб'єктів підприємництва. Водночас, і перший, і другий ризики мають бути враховані при здійсненні конкретних дій чи проведенні суб'єктом підприємництва конкретної операції.

Ризик дезінформації може виникати через загострені взаємовідносини з конкурентами чи недобросовісну поведінку клієнтів, контрагентів. Справа в тім, що в перших двох випадках ризики (ризик відсутності інформації та ризик використання неповної чи необ'єктивної інформації) мають об'єктивний характер через те, що одні суб'єкти намагаються захистити свою інформацію, а інші навпаки — отримати її, водночас ризик дезінформації утворюється певними суб'єктами штучно, з метою введення інших в оману. За таких умов ризик дезінформації зазвичай завжди матиме суттєві негативні наслідки для підприємців. Тому, забезпечуючи свою діяльність в інформаційному середовищі та формуючи свої інформаційні ресурси суб'єкти підприємництва, мають звертати особливу увагу на наявність ризику дезінформації.

Слід пам'ятати, що обсяги дезінформації різко зростають у так звані критичні періоди, які характеризуються:

- зростанням напруженості у відносинах із суб’єктами конфлікту;
- відсутністю об’єктивної інформації та невизначеністю ситуації в інформаційному середовищі суб’єктів підприємництва
- необхідністю інформації для прийняття швидких та адекватних рішень сторонами конфлікту.

За таких умовах виникає особлива небезпека дезінформуючого впливу, оскільки дезінформація може будуватись на мінімальних обсягах об’єктивної інформації (Рис. 9.2.)

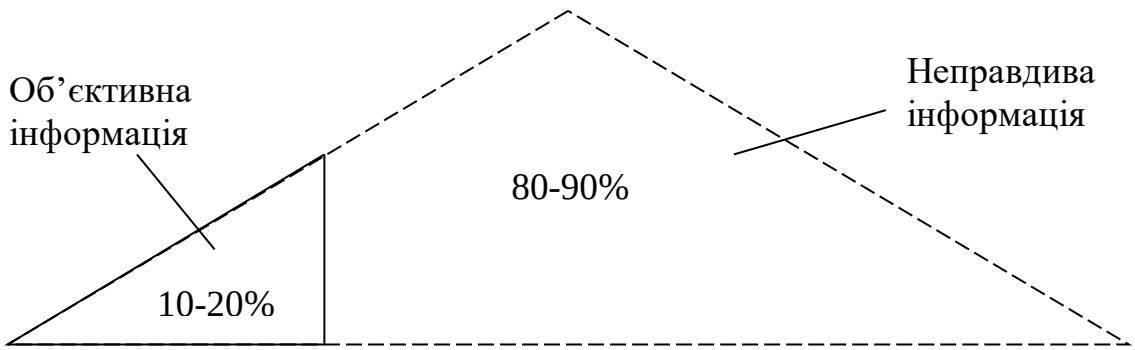


Рис. 9.2. Схема побудови дезінформуючих повідомлень в умовах загострення конфлікту

Особлива небезпека за таких умов полягає у тому, що дезінформуючий вплив здійснюється за допомогою незадіяних до цього джерел, які маскуються як внутрішні, тобто самого суб’єкта, що сприяє підвищенню рівня довіри до такої інформації. Більше того, за умов загострення конфлікту дезінформація може подаватися з декількох джерел, до того ж упродовж певного періоду, тобто щодо певного суб’єкта підприємництва починає проводитися серйозна інформаційна кампанія.

Оцінювання ризиків, пов’язаних з формуванням інформаційного ресурсу, може визначатися через ціну (вартість) певної операції, щодо якої здійснюється інформаційне забезпечення або обсяги прибутку, які може отримати суб’єкт підприємництва у разі прийняття рішення на основі

об’єктивної інформації. Тобто, ціна ризику визначається обсягом зроблених суб’єктом вкладень та очікуваного прибутку. Водночас обсяги операцій чи прибутків не можуть повною мірою давати оцінку ризикам, пов’язаним з формування інформаційного ресурсу. Такими обсягами може вимірюватися ризик відсутності інформації, тоді як на оцінювання інших ризиків суттєво впливатиме якість інформації, якою забезпечується певна операція чи рішення. Показниками якості інформації є її достовірність, повнота та актуальність. Достовірною буде вважатись інформація, отримана з двох і більше незалежних джерел або одного надійного джерела, а також та, об’єктивність якої підтверджена додатковою перевіркою. Повною буде вважатись інформація, з якої можна скласти характеристику об’єкта, достатню для формування об’єктивного уявлення про нього. Актуальною вважається інформація, в якій на цей час має потребу суб’єкт підприємництва. За таких умов інформація, яка є достовірною, повною та актуальною, вважатиметься якісною зі ступенем ризику її використання, який можна прийняти. Інформація, щодо якої є сумніви стосовно її достовірності, з якої неможливо скласти необхідні характеристики про об’єкт зацікавленості та яка неповністю відповідає нагальним потребам суб’єкта підприємництва, буде вважатись низької якості (неякісною). Усі інші характеристики якості інформації, які знаходяться в межах від неякісної до якісної вважатимуться такими, що формують певний ризик використання інформації. Тобто, під час використання якісної інформації ризики можуть бути мінімальними і бути прийнятими суб’єктом. За наявності неякісної інформації ризики можуть бути доволі суттєвими, і за таких умов буде сенс відмовитися від певних дій чи вживати додаткових заходів з підвищення якості інформації. В усіх інших випадках слід вживати заходів щодо мінімізації як інформаційних ризиків, так і ризиків, пов’язаних з тими чи іншими діями суб’єктів підприємництва. Використання якісної інформації може формувати рівень ризику з коефіцієнтом від 0 до 0,2, неякісної – від 0,5 до 1,0. Усі інші коефіцієнти приймаються для інформації, яка за своєю якістю

вища, ніж така, що може вважатися неякісною. За таких умов, оцінювання ризику формування інформаційного ресурсу для інформаційного забезпечення певної операції чи рішення визначатиметься як добуток від обсягу операції (угоди, рішення) та відповідного коефіцієнта якості інформації.

Контроль ризиків, пов'язаних з формуванням інформаційного ресурсу, передбачає проведення аналітичної роботи з усіма видами інформації, яку отримує суб'єкт підприємництва і планує використати для забезпечення його діяльності. Під час аналітичної роботи інформація узагальнюється, порівнюється, переперевіряється, відомості щодо яких є сумнів у їх достовірності, вилучаються з інформаційного ресурсу. Уся інформація підлягає обробці, у результаті якої отримуються інформаційні дані, використання яких матиме мінімальний ризик для суб'єкта.

Крім того, з метою контролю ризиків, що можуть виникати під час формування інформаційного ресурсу, суб'єкти підприємництва намагаються встановити постійні та надійні зв'язки з джерелами інформації, підтримувати стабільні взаємовідносини з ними. Водночас суботи дбають про розширення мережі джерел інформації, аби забезпечити її отримання з якомога більшої кількості джерел і здійснювати контроль не лише за надходженням інформації, а й за поведінкою самих джерел.

Мінімізація ризиків, що виникають під час формування інформаційного ресурсу суб'єкта підприємництва, інформаційного забезпечення його операцій та управлінських рішень, здійснюється через проведення відповідних заходів, передусім інформаційного спрямування. Насамперед звертається увага на організацію інформаційно-аналітичної роботи, яка повинна виконуватись як один з необхідних видів інформаційного забезпечення підприємницької діяльності. Ця робота має передбачати збирання та обробку інформації з різних джерел різними підрозділами суб'єкта підприємництва. На жаль, у більшості суб'єктів цьому питанню не приділяють належної уваги, у кращому разі завдання

інформаційно-аналітичної роботи покладають на службу безпеки й цим обмежуються. Тому інформація зазвичай є неповною та односторонньо висвітлює події, явища, об'єкти. Коли ж суб'єкти підприємництва організовують інформаційно-аналітичну роботу як один із елементів їх інформаційного забезпечення, то формування інформаційних ресурсів здійснюється системно по трьох інформаційних рівнях: інформація від маркетингової діяльності, інформація від проведення інформаційного моніторингу та досліджень контрагентів, клієнтів, партнерів і інформація, отримана від заходів комерційної розвідки. Крім того, така робота передбачає періодичне проведення в підрозділах суб'єктів підприємництва інформаційного аудиту, під час якого виявляється необхідна для забезпечення конкретної їх діяльності та операцій юридична, комерційна, фінансова, технологічна та інша інформація. Уся інформація, отримана від маркетингової діяльності, інформаційного моніторингу та аудиту, а також комерційної розвідки, узагальнюється, аналізується, за необхідності перевіряється й формується у відповідні бази даних. Тобто основними засадами мінімізації ризиків під час формування інформаційних ресурсів суб'єктів підприємництва є створення ними власної інформаційної бази даних. Якраз зазначена база має стати головним джерелом інформації для інформаційного забезпечення операцій та управлінських рішень в діяльності суб'єктів підприємництва . Водночас така база має постійно оновлюватись і доповнюватись, щоб не допустити її старіння й формування певного ризику її використання.

Стосовно ж інформаційного забезпечення кожної конкретної операції, особливо тих, які пов'язані з вкладанням коштів, гарантіями та прийняття зобов'язань суб'єкти підприємництва зазвичай здійснюють інформаційно-аналітичні дослідження контрагентів, клієнтів незалежно від того, чи є відповідна інформація про зазначених осіб в їх базах даних, чи її немає (Рис. 9.3).

Інформаційно-аналітичне дослідження проводиться щодо правового статусу, фінансових можливостей, історії взаємовідносин з судами, правоохоронними та податковими органами, комерційної діяльності, осіб, з якими суб'єкти підприємництва планують вступати у взаємовідносини. Недостатність інформації про таких осіб формує певний рівень ризику взаємовідносин з ним. Так, з практики діяльності банків відомо, що під час проведення кредитних операцій деякі банки України та Росії визначають, так званий, ризик помилки вибору позичальника, в основу якого покладено повноту інформації, що характеризує кожного конкретного позичальника. Так, низький ризик визначається за умов, коли наявність інформації про позичальника складає не менш як 90 % необхідної банку. До позичальників з низьким ризиком відносять тих суб'єктів, щодо яких отримана інформація дає змогу зробити висновки про відсутність в їхній діяльності кримінальних зв'язків, стабільну комерційну діяльність, позитивну кредитну історію, багатопрофільну діяльність, наявність філій, хороший фінансовий стан.

Рис. 9.3. Складові інформаційного забезпечення комерційних операцій

Малий ризик визначається, коли банк отримав не менш як 80 % необхідної йому інформації про позичальника або коли отримана інформація дає змогу характеризувати його як суб'єкта, у діяльності якого відсутні

кримінальні зв’язки, підтримується стабільна комерційна діяльність на основі перспективного бізнесу, що здійснюється за участю багатьох партнерів. Крім того, отримана інформація дає можливість дійти висновку про хороший фінансовий стан та позитивну кредитну історію позичальника.

Середній ризик визначають для позичальників, про яких банк отримав не менше як 70 % необхідної йому інформації. Такий же рівень ризику встановлюється у разі коли інформаційні характеристики про позичальника вказують на його діяльність в ризиковій сфері бізнесу, факти несвоєчасного повернення кредитів і сплати податків або відсутність досвіду роботи з кредитними коштами, велику кількість рахунків у різних банках, частина з яких (рахунків) є непрацюючими.

Високий ризик визначають для позичальників, про яких банк отримав не менше 60 % необхідної йому інформації або яка свідчить про факти неповернення кредитів у діяльності позичальника, судові розгляди справ за позовами до позичальника, наявність кредиторських боргів, часту реорганізацію структури позичальника, велику плинність кадрів, нестійкий фінансовий стан, факти недобросовісної конкуренції до яких вдається позичальник.

Дуже високий ризик визначається за умов, коли банк отримує менш як 60 % необхідної йому інформації про позичальника. Крім того, такий рівень ризик визначається коли інформація характеризує останнього як такого, у якого відсутні ознаки реальної господарської діяльності, є непорозуміння з правоохоронними органами та факти недбалого ставлення до виконання своїх зобов’язань, а також з отриманої інформації неможливо скласти об’єктивний висновок про фінансовий стан позичальника та можливості й перспективи його підприємницької діяльності.

За такого підходу в сукупності з іншими видами ризику, які розрахо-вуються у банку, можна буде зробити об’єктивний висновок щодо надійності позичальника в його взаємовідносинах з банком.

На жаль, в умовах відсутності правового регулювання збирання необхідної суб'єктам підприємництва інформації чимало з них ведуть таку роботу не надто успішно й з ризиком, який не завжди дає змогу ефективно використовувати отриману інформацію. За таких умов вказані суб'єкти не повсякчас активно вдаються до такої роботи, а тому нерідко зазнають втрат від неправильно застосованої або недостатньої інформації під час прийняття тих чи інших рішень або проведення певних операцій. Особливо від цього потерпають фінансові та комерційні операції суб'єктів підприємництва, які найбільше вимагають об'єктивної інформації.

У нинішніх умовах, коли інформаційні технології отримали значне поширення в усіх сферах діяльності, важливого значення набувають аналіз, оцінювання, контроль і мінімізація ризиків інформаційного впливу.

Основними видами ризику інформаційного впливу для суб'єктів підприємництва можуть бути:

- ризик втрати суб'єктом свого іміджу на певному ринку;
- ризик конфліктних ситуацій з власним персоналом, клієнтами, акціонерами, державними оганами, контрагентами;
- ризик блокування роботи суб'єктів через численні перевірки їх діяльності.

Зауважимо, що здійснюючи свою діяльність, суб'єкти підприємництва активно використовують можливості та умови інформаційного середовища, а тому можуть у будь-який час зазнати дії ризиків інформаційного впливу. Різке якісне зростання інформаційних технологій та інформаційних продуктів поступово формує нові способи застосування інформації як виду інтелектуальної зброї. Тому, здійснюючи аналіз ризиків інформаційного впливу, суб'єкти підприємництва мають визначитися, з яким саме видом ризику вони можуть стикатись на певному етапі своєї діяльності або під час здійснення відповідної операції. Слід зауважити, що ризики інформаційного впливу можуть мати постійний характер, як результат певних відносин суб'єктів з різними особами, або формуватись як наслідок цілеспрямованої

дії певних осіб. У останньому разі найбільш характерним є так звані інформаційні атаки, коли з різних джерел одночасно або в невеликий проміжок часу в інформаційне середовище суб'єкта підприємництва подається негативна для нього інформація. Найімовірніше, що інформаційні атаки можуть здійснюватися за умов, коли суб'єкт підприємництва перебуває в стані конфронтації або конкурентного суперництва чи протиборства з іншими суб'єктами ринку або особами. Якраз за таких умов ризик потрапляння суб'єкта підприємництва в ситуацію активного нагнітання навколо нього негативної інформації буде доволі істотним. У цьому разі як наслідок виникають інші види ризиків, уже іншого характеру — зниження або втрати іміджу, втрати клієнтів, зменшення обсягів операцій, отримання збитків. Основними формами інформаційних атак, унаслідок яких може виникати ризик зниження іміджу суб'єкта підприємництва, є поширення чуток про недоліки в його діяльності, порушення його ліквідності та платоспроможності, безпідставне акцентування уваги в засобах масової інформації та виступах на окремих негативних випадках і подіях, що відбулись у суб'єкта, особливо пов'язаних з втратою ним коштів, поширення недостовірної та компрометуючої інформації стосовно окремих його посадових осіб, тенденційне висвітлення окремих фактів з його діяльності, модифікація виступів, публікацій, викладених посадовими особами суб'єкта у ході проведення інформаційних заходів (прес-конференцій, круглих столів, спеціальних телевізійних передач).

Основними методами, які використовуються в інформаційних технологіях впливу і внаслідок дії яких для суб'єктів підприємництва може настати ризик втрати іміджу та інші види ризиків, є:

- інтрига — прихована послідовна система дій, яка через непряму мотивацію використовує сподівання, прагнення окремих людей, колективів чи соціальних груп на досягнення певної мети;

- ажіотаж — нарощування інтенсивності інформаційних повідомлень, зокрема і резонансних та створення інформаційного завантаження середовища суб'єктів відомостями сенсаційного характеру;

мозаїка подій — штучно створені події, які «вбудовуються» в загальну тематику подій і подаються в інформаційне середовище суб'єктів;

- провокація — «вбудовані» в загальну тематику мозаїки подій, факти, неправдиві твердження, які породжують в уяві суб'єктів інформаційного середовища доволі значні для них наслідки та у зв'язку з цим можуть мотивувати їх до певної поведінки щодо суб'єктів підприємництва;

- інсинуація — надання в інформаційне середовище певних відомостей з метою введення в оману його суб'єктів або ославлення певних подій, фактів чи осіб, пов'язаних з конкретними суб'єктами підприємництва;

- інспірація — поширення інформації, здатної викликати у відповідних осіб негативну реакцію щодо суб'єктів підприємництва, їх діяльності чи окремих посадових осіб (підбурювання);

- корекція — спеціально підібране доповнення інформаційних характеристик діяльності суб'єктів підприємництва або подій, пов'язаних з ними з метою формування або утримання необхідного уявлення у інших суб'єктів інформаційного середовища про них або зазначені події;

- інкорпорація — вбудова видуманих або дійсних подій у загальну тематику подачі інформації.

Особливістю поведінки сучасної громадськості є підвищена чутливість до інформаційного впливу, насамперед сприйняття інформаційних продуктів, що мають сенсаційний характер. Така довіра до слова та образу, логічного твердження ґрунтується на поступовому впровадженні у свідомість громадян неправильної істини про непогрішимість тверджень та ідей, що професійно пояснюються (нав'язуються) суспільству різноманітними експертами, критиками, аналітиками, оглядачами, черговими «борцями за краще майбутнє» та іншими особами. Як наслідок — громадяни стають затиснутими компетентністю таких осіб і в умовах тотального інформаційного перевантаження зага-

льною інформацією та інформаційного вакууму в необхідній їм інформації починають вірити в ті відомості, які подаються в інформаційне середовище за допомогою відповідних технологій та методів. Тобто здійснюється відповідний вплив на свідомість, а отже, й на поведінку громадян, якими можуть бути працівники суб'єктів підприємництва, їх акціонери чи клієнти.

Таким же чином може поширюватись інформація, що створює ризик потрапляння суб'єктів підприємництва у різні конфліктні ситуації. Ризик блокування їх роботи через численні перевірки діяльності створюється шляхом поширення в інформаційному середовищі та безпосередньо в органах контролю та нагляду негативної інформації про діяльність суб'єктів.

Під час аналізу ризиків інформаційного впливу насамперед вивчаються умови взаємовідносин суб'єктів підприємництва із зовнішнім інформаційним середовищем, окремими його суб'єктами та власним персоналом. У процесі вивчення виявляються найбільш критичні відносини, з яких може надходити відповідна загроза й утворюватися певні ризики інформаційного впливу. На підставі результатів вивчення зазначених умов прогнозуються ймовірність та можливі терміни появи відповідного ризику впливу.

Оцінювання ризиків впливу спрямовується на визначення сфери діяльності та взаємовідносин суб'єктів підприємництва, щодо яких може поширюватись негативна для них інформація в той чи інший період їх діяльності і таким чином утворюватися певний ризик. Методик визначення розміру моральної чи матеріальної шкоди за результатами реалізації ризиків інформаційного впливу поки що не існує.

У процесі контролю ризиків здійснюється моніторинг інформаційного середовища суб'єктів підприємництва з погляду виявлення ознак, які можуть указувати на передумови появи або безпосередню появу ризиків інформаційного впливу.

Для мінімізації інформаційних ризиків впливу суб'єкти підприємництва вдаються до таких заходів:

- періодичне поширення через різні інформаційні канали позитивної інформації про суб'єктів, оприлюднення їх досягнень та активна реклама продукції, послуг, робіт;

- періодичне інформування інформаційного середовища суб'єктів, насамперед персоналу, акціонерів і клієнтів про результати їх роботи;

- формування фірмового патріотизму у персоналу та акціонерів суб'єктів, пропаганда позитивного їх іміджу на ринку;

- проведення спеціальних інформаційних операцій стосовно зміни об'єктів інформаційного впливу, дезорієнтації суб'єктів, що вдаються до заходів впливу, заходів контрпропаганди та антикопроментації.

Серед ризиків інформаційного впливу особливу небезпеку становить ризик потрапляння суб'єктів підприємництва під дію інформаційного тероризму, що є нині доволі ймовірним. Ураховуючи відчутні наслідки, до яких можуть призвести дії інформаційного тероризму, суб'єкти підприємництва не повинні ігнорувати такий вид ризиків і мають виробляти відповідну політику щодо їх мінімізації. Насамперед має проводитися постійний аналіз та оцінювання умов формування таких ризиків. У процесі аналізу суб'єкти підприємництва повинні визначити, наскільки уразливі до атак інформаційного тероризму їх комунікаційні системи та мережі, особливо засоби, мережі та інформація, які обслуговують платіжну систему банків. Має визначатися ступінь доступності інформаційних систем і мереж для атак інформаційного тероризму. Крім того, вивчається діяльність суб'єктів з погляду її вразливості від інформаційних атак компрометуючими матеріалами, розраховується критична межа, за якої пропаганда та реклама суб'єктів будуть неефективними під впливом заходів інформаційного тероризму. Тобто, межа, за якою інформаційний вплив від актів тероризму призведе до руйнування іміджу суб'єктів підприємництва, їх взаємовідносин з іншими суб'єктами, породжуватиме конфліктні ситуації у виробничих колективах та ін.

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

У процесі оцінювання ризиків інформаційного тероризму визначається, які наслідки можуть настати для суб'єктів підприємництва через інформаційні атаки терористів як з погляду економічного, так і з погляду їх іміджу. Тут можна формувати певні прогнози щодо таких наслідків (втрата клієнтів, звільнення провідних працівників з роботи, втрата інформації, що має обмежений доступ, викрадення коштів з рахунків суб'єктів та їх клієнтів, руйнування програмного забезпечення роботи інформаційної мережі та інформаційних систем). Стосовно конкретного виміру обсягу шкоди, завданої від актів інформаційного тероризму, то тут поки що відсутні якісь підходи. Практично неможливо передбачити, а тим більше прорахувати обсяги можливої шкоди від таких дій. Тому під час оцінювання зазначених ризиків обмежуються можливими категоріями наслідків, які можуть наступати у зв'язку з інформаційними атаками терористів.

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

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

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

Водночас слід зазначити, що дії, пов'язані з інформаційним тероризмом, є для суб'єктів підприємництва не лише небезпечними, а й такими, від яких побудувати гарантовану систему захисту, яка б виключала можливість проведення актів інформаційного тероризму, дуже складно. Тому суб'єкти підприємництва мають передбачати заходи своєї поведінки в разі здійснення таких актів, передусім спрямовані на забезпечення виживання в умовах інформаційних атак, а також заходи по ліквідації їх наслідків.

Таким чином, підсумовуючи, зазначимо, що інформаційні ризики необхідно розглядати не як окремо взяті, а у сукупності з іншими ризиками підприємницької діяльності. Саме в такий спосіб можна правильно прийняти рішення щодо ризику проведення певної операції чи діяльності загалом: прийняти ризики, тобто погодитися на можливі втрати у процесі негативного впливу ризику; вжити заходів щодо зниження ризику; передати ризик іншому суб'єкту (компенсацію можливих збитків покласти, скажімо, на страхову компанію або трансформувати інформаційний ризик в інші види ризику, з більш низьким рівнем втрат). Водночас за певних умов інформаційні ризики

можуть бути головними серед тих ризиків, яких зазнає суб’єкт підприємництва у своїй діяльності.

Висновки

Зміни, що відбулись в останні роки в інформаційному просторі суттєвим чином позначились практично на всіх сферах суспільної життєдіяльності. Інформація стала провідним фактором побудови взаємовідносин, економічного розвитку, інтелектуальних здобутків. Сформовані за допомогою інформації знання стали основою для прогресивного розвитку у науці, техніці, економіці, забезпечили розробку новітніх технологій виробництва. Сучасний інформаційний розвиток сприяв появі нових галузей економіки (інформаційної економіки) та діяльності – інформаційна діяльність. Інформаційні технології значним чином забезпечили прогрес у сфері комунікацій, суттєво вплинули на зміну світогляду людей, розширили можливості щодо їх інтелектуального розвитку. Сформувався так званий інформаційний образ життя в основу якого покладено сучасні знання, інформаційні зв'язки та елементи інформаційної культури. Внаслідок інформаційних трансформацій, що супроводжують розвиток сучасної інформаційної сфери відбулось формування потужного інформаційного потенціалу (інформаційна індустрія) та становлення інформаційного ринку. Сучасні інформаційні технології стали системоутворюючими у суспільному виробництві і діяльності окремих суб'єктів.

Активне поширення інформації практично на всі сфери життєдіяльності суспільства зумовило необхідність правового регулювання нового виду взаємовідносин – інформаційних. На початку 21 століття в Україні з'явилась ціла низка різного рівня правових актів, які забезпечують регулювання взаємовідносин у сфері вироблення, поширення та використання інформації, інформаційного забезпечення діяльності юридичних та фізичних осіб.

Однорідність та цілеспрямованість правових актів у сфері регулювання інформаційних правовідносин зумовили формування нового виду права –

інформаційного, яке отримало досить активний розвиток. В останні роки інформаційне право доповнено новими правовими актами (Закони України «Про захист персональних даних», «Про доступ до публічної інформації»), в окремі з них внесено суттєві зміни і доповнення.

Особливо результати інформаційного розвитку позначились на вітчизняному бізнесі. Сучасні інформаційні технології стали невід'ємною частиною виробничої діяльності суб'єктів підприємництва, що дало їм змогу суттєво підвищити свою конкурентоспроможність на вітчизняному та зовнішньоекономічному ринках. Формування перспектив розвитку суб'єктів підприємництва спирається на глибокі знання економічної, соціальної, внутрішньополітичної ситуації, досягнення науки і техніки, інформаційного прогресу. Інформація в діяльності суб'єкті підприємництва стала потужним та досить впливовим їх ресурсом, який має високу цінність та значний вплив на результати діяльності зазначених суб'єктів.

Разом з тим, інформаційний розвиток зумовив суттєві проблеми як з т.з. впливу на індивідуальну та суспільну свідомість, так і у сфері трансформації взаємовідносин. Останні все частіше стали будуватись під впливом інформації, якою активно наповнюється інформаційне середовище, зазвичай без якісного її аналізу і визначення об'єктивності.

З'явились інформаційні технології спеціально призначені для формування відповідної суспільної думки та суспільної оцінки певних подій, діяльності суб'єктів підприємництва на ринку. В інформаційному середовищі значне місце займають різного роду інформаційні конструкції, які не рідко досить далекі від об'єктивної ситуації і з'являються лише з метою змінити (обґрунтувати) суспільні погляди у необхідному певним суб'єктам вигляді. Наявність подібних конструкцій та інших засобів, які характерні для недобросовісної інформаційної поведінки суб'єктів, певним чином відзначає їх взаємовідносини в інформаційному середовищі. Досить часто у них присутні інформаційне суперництво та протиборство. За певних обставин такі відносини можуть знаходитись у стані інформаційної війни. У

останньому випадку характерним є використання різного роду інформаційних продуктів та технологій руйнування іміджу суб'єктів підприємництва, несанкціонованого доступу до їх інформаційних ресурсів чи негативного впливу на сегменти ринку, в яких здійснюють свою діяльність окремі суб'єкти підприємництва. Тобто, в умовах сучасного інформаційного розвитку досить актуальним є забезпечення інформаційної безпеки суб'єктів підприємництва. В той же час, досвід забезпечення безпеки вітчизняного бізнесу показує, що інформаційна безпека має спрямовувати свої зусилля у трьох досить важливих напрямках: захист інформації суб'єктів підприємництва, інформаційне забезпечення їх діяльності, протидія інформаційному впливу на них та їх персонал.

Захист інформації в системі інформаційної безпеки є найбільш поширеним варіантом організації останньої, інколи навіть тотожним самій безпеці. На даний час заходи захисту інформації поширюються на економічну, правову, кадрову, організаційно-управлінську, технічну сфери діяльності суб'єктів підприємництва. Тобто, існує певний комплекс, об'єднаний в досить розвинену систему заходів захисту інформації. Разом з тим, як показує аналіз ефективності функціонування такої системи тут досить багато проблем, насамперед в організації захисту інформації. Сучасні системи захисту інформації досить складні, дорогі і не зовсім надійні. Більш того, вони недостатньо орієнтовані на особливості комерційної діяльності суб'єктів підприємництва. Захист інформації базується на традиційних підходах і в цілому задовольняючи вимоги підприємництва залишається не повною мірою досконалим. Найбільша увага тут приділяється технічному та програмному захисту електронної інформації.

Звертаючи увагу на інформаційне забезпечення підприємницької діяльності можна бачити, що переважна більшість підприємців визначають роль інформації у їх діяльності, але не мають ефективних інструментів для формування необхідних їм інформаційних ресурсів. Інформаційно-аналітична робота суб'єктів підприємництва у сфері забезпечення їх безпеки

ефективно використовується лише у великому бізнесі. Середній бізнес активізує цю роботу лише час від часу, у випадках суттєвої загрози їх суб'єктам від нестачі об’єктивної інформації. Малий бізнес питаннями інформаційного забезпечення переймається лише в межах управлінської діяльності, за рахунок можливостей його керівників чи власників. Такому стану інформаційного забезпечення вітчизняного підприємництва сприяє відсутність правового регулювання щодо питань збору інформації, її використання та поширення в бізнесі. Виконуючи заходи інформаційної роботи підприємці знаходяться на межі порушення певних правових норм чи прав власності інших суб’єктів. Організація ж ефективної аналітичної практики є дорогою і обмежується незначною кількістю фахівців-аналітиків, яких можна знайти на ринку. З таких же причин залишається недосконалою і робота суб’єктів підприємництва з протидії інформаційно-психологічному впливу на них. Заходи, що вживаються підприємцями в даній сфері здебільшого торкаються питань відновлення їх іміджу, торгової марки (бренду) на ринку і в суспільстві. Пропаганда зазвичай тут підмінюється рекламою продукції і займає незначну частку у боротьбі з заходами інформаційно-психологічного впливу. Можна говорити, що даний сегмент інформаційної безпеки суб’єктів підприємництва поки що проходить своє становлення.

Важливе місце у забезпеченні інформаційної безпеки суб’єктів підприємництва займає управління інформаційними ризиками. Основною особливістю тут є те, що це питання повністю покладається на підрозділи безпеки суб’єктів підприємництва і певною мірою залежить від їх можливостей. Зазвичай, управління інформаційними ризиками не інтегрується в систему управління ризиками суб’єктів підприємництва, яка є складовою процесу управління їх діяльністю. У такій ситуації роль управління саме інформаційними ризиками не виступає провідною. Подальший розвиток інформаційних технологій безумовно буде вимагати все більшої уваги до інформації взагалі і її використання у забезпеченні

підприємницької діяльності. Перетворення вказаних технологій в один із видів загроз (інтелектуальна зброя) і їх використання в конкурентній боротьбі суб'єктів підприємництва активізує пошук шляхів удосконалення інформаційної безпеки, що у свою чергу дасть поштовх змінам у її правовому регулюванні та буде сприяти підвищенню професійного рівня фахівців, залучених до забезпечення як безпеки бізнесу в цілому, так інформаційної безпеки зокрема. Тобто, є всі підстави вважати, що актуальність забезпечення інформаційної безпеки у діяльності сучасного підприємництва буде лише зростати.

Інформаційні джерела:

1. Прибутько П.С., Лук'янець І.Б. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. –К.: Видавець ПАЛИВОДА А.В., 2007. – 252с.
2. Информационно-психологическая безопасность в эпоху глобализации: учеб. пособ./В.М. Петрик,/В.В. Остроухов, А.А. Штоквиш и др. – К.: ГУИКТ, 2008. – 544с.
3. Почепцов Г.Г. Інформаційний та віртуальний простори України: кроки в майбутнє. [Електронний ресурс]. – Режим доступу: http://osvita.mediasapiens.ua
4. Кибертероризм, информацыонные войны и безопасность.-К.: ООО «Консалтинговая компания «СИДКОН». – 2014. – 60с.
5. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навч. посібник. – К.: Кондор, 2004. – 384с.
6. Панченко О.А., Бончук Н.В. Информационная безопасность личности. – К.: КИТ, 2011. – 672с.
7. Нестеренко О.В. Проблеми формування національної інформаційної інфраструктури та забезпечення її безпеки. [Електронний ресурс]. – Режим доступу: www.iprkiev.ua
8. Стратегія розвитку інформаційного суспільства в Україні, затверджена Розпорядженням КМУ від 15.05.2013р. №386 – Р. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua
9. Про захист інформації в інформаційно-телекомунікаційних системах, Закон України. ВВР, 1994, №31, ст. 281
10. Вільна енциклопедія «Вікіпедія»: [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org.
11. Про Концепцію Національної програми інформатизації, Закон України. ВВР, 1998, №27-28, ст.182
12. Карпенко В. Інформаційна політика та безпека. [Електронний ресурс]. – Режим доступу: http://ukrlife.org/main
13. Інформаційний простір України. Загальна характеристика. [Електронний ресурс]. – Режим доступу: http://com.ua
14. Ещенко П.С., Арсеенко А.Г. Куда движется глобальная экономика в XXI веке? – К.: Знания Украины,2012. – 479с.
15. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015роки, Закон Укріни. ВВР, 2007, №12, ст.102
16. Джон Перри Берлоу. Киберномика: к теории информацыонной экономики. [Електронний ресурс]. – Режим доступу: http://20khwedn.com

17. Мирясов Ю.А. Тенденции формирования информационного сектора экономики. [Електронний ресурс]. – Режим доступу: http://firearticles.com

18. Скворцов Р. Кризис информацыонной экономики [Електронний ресурс]. – Режим доступу: www.ueg.in.ua

19. Головний правовий портал України «Лігазакон» [Електронний ресурс]. – Режим доступу: www.ligazakon.ua.

20. Про інформацію, Закон України. ВВР, 1992, №48, ст.65

21. Зубок М.І. Інформаційна безпека: навч. посібник. – К.: КНТЕУ, 2005. – 133с.

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

23. Зубок М.І., Яременко С.М. Безпека банківської діяльності: підруч. – К.: КНЕУ, 2012. – 473с.

24. Гавриленко И. Организованная преступность в Украине// Служба безопасности. – 1997: №1, с.22-25

25. Преступность в зеркале цифр. // Служба безопасности. – 1997: №12, с.18-19

26. Офіційний сайт Державної служби статистики України. [Електронний ресурс]. – Режим доступу: www.ukrstat.gov.ua

27. Наша цель – за щитить человека // Служба безопасности. – 1996: №10, с.17-18

28. Поляруш А.А., Юрченко А.М. Информацыонная война против Украины: причины и соцыально-политические технологии. К.: КИЙ, 2011. – 200с.

29. Крутов В.В. Від патріотичного виховання боротьби з тероризмом… До недержавної системи національної безпеки: К.: Преса України, 2009. – 592с.

30. Нездоля А.И. Украина третього тысячелетия. – Донецк.: Каштан, 2005. – 460с.

31. Объём теневой экономики Украине – 350 миллионов гривен. [Електронний ресурс]. – Режим доступу: www.rada.kiev.ua

32. Социальные сети: парадоксы зависимости. [Електронний ресурс]. – Режим доступу: http://kuev.in.ua/obshestvo

33. Ерёмин А.Л. Ноогенез и теория интеллекта. – Краснодар.: Советская Кубань, 2005. – 356с.

34. Кохович Н.С. Влияние отрицательной информации на здоровье человека. [Електронний ресурс]. – Режим доступу: http://click.1september.ru

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

36. Шаваев А.Г. Система борьбы с экономической разведкой. – М.: Правовое просвещение. – 2000. – 240с.

37. Современные угрозы безопасности компаний и банков. – К.: ООО «Консалтинговая компания «СИДКОН», 2014. – 90с.

38. Корнеев И.К., Степанов Е.А. Защита информации в офисе. – М.: Проспект. 2008. 336с.

39. Конституція України. [Електронний ресурс]. – Режим доступу: www.rada.gov.ua

40. Про доступ до публічної інформації, Закон України. ВВР, 2011, №32, ст.314

41. Про захист персональних даних, Закон України. ВВР, 2010, №34, ст.481

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

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

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

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

46. Про банки і банківську діяльність, Закон України. [Електронний ресурс]. – Режим доступу: www.rada.kiev.ua

47. Про затвердження змін до правил зберігання, захисту, використання та розкриття банківської таємниці, Постанова правління НБУ від 11.07.2012р. № 292. [Електронний ресурс]. – Режим доступу: www.rada.kiev.ua

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

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

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

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

52. Зубок М.І. Правове регулювання безпеки підприємницької діяльності: навч. посібник. – К.: КНТЕУ, 2005. – 141с.

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

54. Зубок М.І., Зубок Р.М. Безпека підприємницької діяльності. Нормативно-правові документи комерційного підприємництва, банку. – К.: Істина, 2004. -144с.

55. Про захист економічної конкуренції, Закон України. [Електронний ресурс]. – Режим доступу: www.rada.kiev.ua

56. Рыков А.С. Аналитики – кабинетные рыцари шпионских войн. // Разведка. – 2010, №2, ст.50-55

57. Хант Г., Зарьтарьян В. Разведка на службе вашего предприятия. – К.: Укрзакордонвизасервис, 1992. – 160с.

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

59. Нежданов И.Ю. Аналитическая разведка для бизнеса. – М.: Ось-89, 2008. – 336с.

60. Деревицкий А. Комерческая разведка. – М.: Питер, 2006. – 208с.

61. Великий тлумачний словник сучасної української мови (з дод. і допов.) / укладач – Бусел. В. – К.: Ірпінь, 2005. – 1728с.

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

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

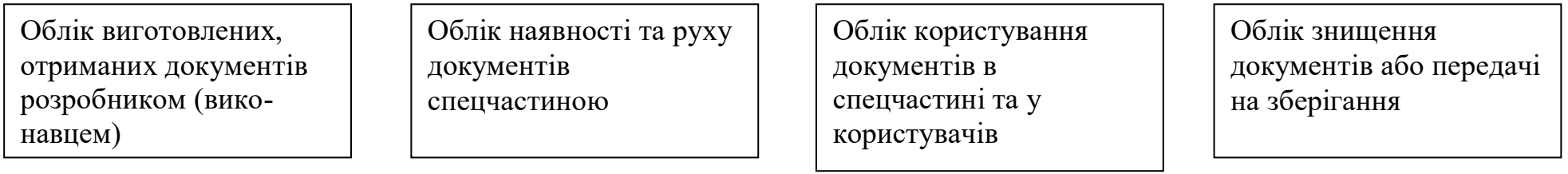
64. Меркулов А.Г., Ромашев Р.В. Энциклопедия деловой разведки и контрразведки. М.: Русь-Олимп, 2007.- 428с.

65. Ярочкин В.И., Бузанова Я.В. Корпоративная разведка.: М.: Ось-89, 2004. – 288с.

Додаток 1

Розробка таємних документів в установах суб'єктів підприємництва

Облік документів таємного та конфіденційного характеру



Додаток 2

Реєстрація таємних та конфіденційних документів в установах суб'єктів підприємництва

Реєстрація документу — фіксування факту створення або надходження документу шляхом проставлення на ньому умовного позначення — реєстраційного індексу з подальшим записом у реєстраційних формах необхідних відомостей про документ

Централізована реєстрація таємних та конфіденційних документів в установі суб'єкта підприємництва

Кожний документ реєструється лише один раз, вхідні — в день надходження, створювані — у день підписання та затвердження

Реєстраційний індекс складається з порядкового номера в межах групи документів, що реєструються і доповнюються індексами за номенклатурою справ, питаннями діяльності, кореспондентами тощо

Реєстрація документів здійснюється у відповідних журналах (окремо таємні та конфіденційні документи)

Запис про реєстрацію має містити назву документу, короткий зміст, адресата (виконавця), дату реєстрації, кількість сторінок, реєстраційний індекс гриф документа та номер примірника

Додаток 3

Робота з документами таємного та конфіденційного характеру в установах суб'єктів підприємництва

Роботу з документами здійснюють тільки ті працівники, яких допущено до відповідних відомостей таємного та конфіденційного характеру

Робота здійснюється на своїх робочих місцях при умові неможливості ознайомлення з ними інших осіб або у спеціально виділених приміщеннях

Робота з документами здійснюється тільки у визначений час, як правило, з обов'язковим їх поверненням до спецчастини в кінці робочого дня

Надання документів для роботи здійснюється з обов'язковим записом у відповідному журналі (реєстрі) під підпис особи, яка отримала зазначений документ

При тривалій роботі з таємними та конфіденційними документами (більше одного робочого дня) виконавець враховує документ у відповідному індивідуальному описі таємних та конфіденційних документів та зберігає його у особистому сейфі

Перевірка наявності документів таємного та конфіденційного характеру здійснюється виконавцем щоденно, керівником підрозділу щонеділі з відповідним записом у індивідуальному описі документів

Додаток 4

Зберігання документів таємного та конфіденційного характеру в установах суб'єктів підприємництва

Зберігання документів працівниками

- в індивідуальних сейфах;
- в металевих шафах при умові призначення відповідальної особи в підрозділі за доступ до таких шаф;
- кімнати, в яких знаходяться сейфи (металеві шафи), зачиняються на замок, опечатуються і передаються під охорону

Зберігання документів в спецчастині

- в металевих шафах по справах;
- кімнати спецчастин повинні мати спеціальне обладнання і відповідне технічне укріплення, зачинятись на замок, опечатуватись і здаватись під охорону;
- доступ до спецчастини має обмежене коло осіб

Зберігання документів в архівах

- в металевих шафах по справах;
- приміщення архіву повинно мати спеціальне обладнання та технічне укріплення, зачинятись на замок, опечатуватись та здаватись під охорону;
- доступ до архіву мають тільки працівники архіву

Зберігання документів таємного та конфіденційного характеру здійснюється окремо від інших документів

Захист інформації суб'єктів підприємництва у роботі з відвідувачами

Прийом відвідувачів повинен вестись тільки в години, визначені правилами трудового розпорядку роботи	Робота з відвідувачами проводиться у спеціально призначених для цього приміщеннях	Верхній одяг відвідувачів повинен залишатись зовні приміщення, в якому здійснюється їх прийом
Приміщення, в якому здійснюється прийом відвідувачів, повинні знаходитись недалеко від входу в офіс	Переміщення (перебування) відвідувачів по (на) території установи суб'єкта підприємництва не повинно бути неконтрольованим	Висвітлення загальної інформації про діяльність установи суб'єкта підприємництва на вході на його територію (КПП)
Забезпечення можливості консультації відвідувачів по телефону з можливістю фіксування розмови	Конфіденційна (таємна) інформація не може доводитись відвідувачам без необхідних на те підстав	Встановлення відповідного регламенту (порядку) відвідування установи суб'єкта підприємництва
Ознайомлення відвідувачів з конфіденційними документами здійснюється тільки в присутності працівника установи підприємства, банку	Факт ознайомлення відвідувачів з конфіденційними документами має письмово засвідчуватись	Відвідувачам забороняється робити виписки з конфіденційних документів

Додаток 6

Технології проведення інформаційного аудиту

Обстеження інформації на об’єкті	Обстеження інформації про об’єкт	Спеціальне обстеження сфери інформаційної уваги
• визначення належності інформації, яку необхідно виявити у ході обстеження; • визначення об’єкта обстеження; • визначення переліку джерел інформації, які підлягають обов’язковому обстеженню; • пошук ознак наявності необхідної інформації; • виявлення умов появи необхідної інформації на об’єкті та її повного обсягу; • виявлення зв’язку необхідної інформації з іншою, яка є на об’єкті; • відбір необхідної інформації у ході обстеження	• визначення основних інформаційних характеристик та ознак об’єкта; • прогнозування місць зосередження інформації про об’єкт, її можливих джерел; • обстеження інформаційних масивів з метою виявлення орієнтуючої інформації про об’єкт; • виявлення зв’язків орієнтуючої інформації, умов її появи в інформаційному середовищі; • пошук інформації, яка будь-яким чином пов’язана з об’єктом; • замовлення спеціальних досліджень, подання запитів з метою отримання інформації про об’єкт; • пошук джерел первинної інформації про об’єкт	• вибір сфери інформаційної уваги; • обстеження всіх об’єктів та джерел сфери інформаційної уваги з метою виявлення ознак важливої та цінної для суб’єкта підприємництва інформації; • пошук додаткової інформації, що підтверджує або суперечить попередній інформації; • виявлення обставин появи важливої для суб’єкта підприємництва інформації; • встановлення зв’язків важливої інформації з іншою

Додаток 7

Технології проведення інформаційного моніторингу

Контроль інформації за визначеними ознаками та індикаторами	**Контроль інформації по визначених джерелах**	**Повний контроль інформації, що з'являється в інформаційному середовищі**
• визначення ознак інформації, які характеризують необхідні суб'єкту підприємництва знання; • визначення інформаційних характеристик ознак; • контроль наявності ознак у складі інформації, яка подається різними джерелами; • виявлення зв'язків між ознаками у складі інформації різних джерел; • фіксація ознак і змісту важливих інформаційних повідомлень	• визначення джерел інформації відповідно до: - можливості появи необхідної інформації; - об'єктивності та вартості інформації; - доступності джерел; • постійний контроль інформації, яка подається визначеними джерелами; • фіксація важливих інформаційних повідомлень	• розподіл сил та засобів по групах джерел інформації; • визначення інформації, яка має бути виявлена у ході контролю інформаційного середовища; • визначення порядку (графіку) та видів (постійного, періодичного, вибіркового) контролю; • фіксація визначеної інформації у ході контролю

Додаток 8

Деякі прийоми пропаганди, що використовуються у підприємницькій діяльності

Посилання на авторитет

Поєднання стійкої репутації особи з певними факторами діяльності суб'єкта підприємництва, в т. ч. оцінки експертів, дані документів, звітів, результати досліджень

Буденна розповідь

Адаптація середовища до діяльності суб'єктів підприємництва в якій допущено певні порушення або є негативні наслідки з метою їх девальвації у свідомості громадян

Пікети, мітинги, голодування

Імітація соціальних протестів з метою емоційного впливу на оточення суб'єктів підприємництва та психологічного тиску на їх керівництво за для отримання необхідної реакції

Забовтування

Зменшення актуальності питань, які негативно характеризують суб'єктів підприємництва або формування ситуації розчарування щодо певних суб'єктів (конкурентів) через постійне нагадування про них в інформаційному середовищі

Інформаційна блокада

Утримання від надання інформації про діяльність (події в діяльності) суб'єктів підприємництва за для її (їх) власної інтерпретації на фоні інформаційного вакууму

Використання медіаторів

Поширення в інформаційному середовищі суб'єктів підприємництва необхідних їм міфів, чуток, думок, пліток з метою широкого їх обговорення в оточенні суб'єктів

Коментарі

Надання в інформаційне середовище суб'єктів підприємництва інформації у вигляді відповідних оцінок, позицій, точок зору, пояснень та розкриття суті подій, фактів

Додаток 9

Дезінформація в підприємницькій діяльності

Умови проведення	Вимоги до заходів дезінформації	Інструменти дезінформації
• Започаткування нового бізнесу або нового його напрямку • Проникнення на нові ринки в нові регіони • Розробка та вироблення нової продукції (послуг) • Реальні загрози комерційній діяльності чи окремим операціям • Необхідність утримання в таємниці певних комерційних задумів, планів в т. ч. і щодо часу, місця та виду нової діяльності	• Усі заходи мають базуватись на єдиному задумі і проводитись за єдиним рішенням • Оптимальне сполучення правдивої і неправдивої інформації • Збереження в таємниці відомостей про проведення заходів дезінформації • Заходи дезінформації не повинні бути тривалими чи проводитись постійно в діяльності суб'єктів підприємництва	• Публічні виступи керівництва і представників підприємства • Виступи, інтерв'ю третіх осіб з оцінками діяльності суб'єктів підприємництва • Повідомлення ЗМІ • Імітація дій, що можуть вказувати на певні наміри діяльності, поведінки суб'єктів підприємництва • Поширення чуток

Додаток 10

Використання чуток у бізнесі

Формування підтримки іміджу суб’єктів підприємництва	Захист від негативного впливу чужих чуток	Забезпечення впливу на споживачів, просування продукції, послуг на ринок
Привернення уваги до певних подій та ситуацій	Підготовка суб’єктів ринку до відповідних дій суб’єктів підприємництва	Уведення в оману конкурентів і суб’єктів загроз та їх компроментація
Зниження напруження в колективах установ суб’єктів підприємництва , середовищі клієнтів, контрагентів, споживачів	Отримання суспільної думки про діяльність суб’єктів підприємництва , їх послуги, роботи і продукцію	Вивчення настрою в колективах установ суб’єктів підприємництва
Протидія негативним інформаційним повідомленням	Активізація інформаційного середовища до певних дій суб’єктів підприємництва	Маскування подій, що відбулись в установах суб’єктів підприємництва і можуть мати для них негативні наслідки

Додаток 11

Використання чуток у бізнесі

Принципи утворення чуток

- Інформація повинна бути значима для суб'єкта впливу (торкатись його інтересів)
- Інформація має бути зрозумілою тим на кого спрямована, активно сприйматись в інформаційному середовищі
- Інформація з чуток має забезпечувати вигоду її автору (ам)

Формування чуток і подання їх в інформаційне середовище

Утворення (використання) інформаційного вакууму в інформаційному середовищі і заповнення його чутками

Зміст чуток впливу

Чутки, що ганьблять	Чутки, що славлять	Чутки, що захищають	Чутки, що співчувають
Факти корупції, зв'язку з криміналом, шахрайство, зловживання службовим становищем і т. і.	Позитивні відгуки, подяки від громадян, відзнаки, благодійна допомога	Спростування чуток, чутки проти чуток (античутки), викриття авторів чуток	Виправдання, поведінки, дій, обґрунтування позицій і точок зору

Поширення чуток здійснюється одночасно: як тих, що спрямовуються проти суб'єктів загроз, так і тих, що забезпечують дії, поведінку суб'єктів підприємництва

Додаток 12

Супроводження комерційної діяльності шляхом використання чуток

Поширення чуток з метою підготовки інформаційного середовища для позитивного сприйняття певних дій, поведінки суб'єктів підприємництва	Поширення чуток з метою супроводження певних програм, операцій, дій, поведінки суб'єктів підприємництва на ринку	Аналіз чуток як зворотної інформації про реакцію інформаційного середовища на певні дії, поведінку суб'єктів підприємництва
Аналіз чуток про реакцію суб'єктів ринку на програми, операції, продукцію, послуги, роботи суб'єктів підприємництва	Поширення чуток про високу ефективність, реалізації програм, послуг, продукції, робіт суб'єктів підприємництва	Поширення чуток, спрямованих на формування негативного враження від дій суб'єктів загроз або тих, які здійснюють недобросовісну поведінку на ринку