Лекція 12-13

УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ В ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

1. Аналіз ризиків втрати інформації підприємства.
2. Контроль ризиків втрати інформації підприємства.
3. Мінімізація ризику втрати інформації підприємства.
4. Мінімізація ризику втрати інформації підприємства.
5. Характеристика складників інформаційного забезпечення підприємства

1.Аналіз ризиків втрати інформації підприємства

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 господарської діяльності.

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 господарської діяльності 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 господарської діяльності 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 господарської діяльності 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 господарської діяльності 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).

2. Контроль ризиків втрати інформації підприємства

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 господарської діяльності 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 господарської діяльності 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. 1). Зі 100 % працівників суб'єктів підприємництва 75 % можуть здійснити посягання на інформацію суб'єктів.

3.Мінімізація ризику втрати інформації

Питання мінімізації ризику втрати інформації є доволі серйозним для суб'єктів господарської діяльності 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.

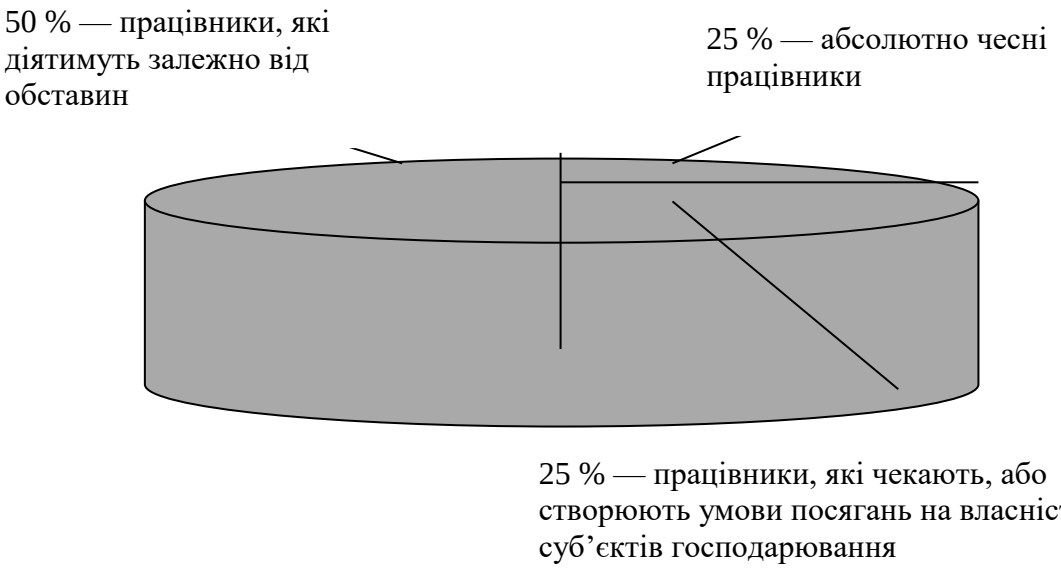

Рис. 1. Структура виробничих колективів за критерієм готовності до посягань на інформацію суб'єкта господарської діяльності

Водночас для зниження (мінімізації) ризику втрати інформації суб'єкти господарської діяльності 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 господарської діяльності. 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 господарської діяльності;

- 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.

4.Види ризиків втрати інформації

Управління ризиками, що виникають у процесі формування суб'єктами господарської діяльності інформаційного ресурсу, носить особливий характер. Справа в тім, що тут існує певна проблема, пов'язана з необхідністю суттєвого інформаційного забезпечення діяльності суб'єктів господарської діяльності відсутністю для цього відповідного правового регулювання. Як уже вказувалось, нині в Україні немає законодавства, яке регулювало б права, умови та порядок доступу суб'єктів господарської діяльності 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 господарської діяльності 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 господарської діяльності встановлюють відповідні відносини.

Ризик відсутності інформації може виникати, коли суб'єктам господарської діяльності 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 господарської діяльності 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 господарської діяльності 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.)

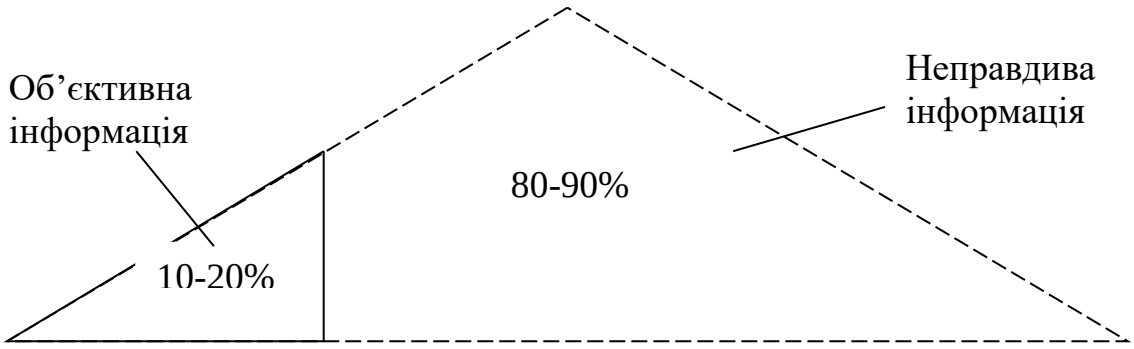

Рис. 2. Схема побудови дезінформуючих повідомлень в умовах загострення конфлікту

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 втрати інформації. 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 господарської діяльності, 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 господарської діяльності. 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 господарської діяльності і планує використати для забезпечення його діяльності. Під час аналітичної роботи інформація узагальнюється, порівнюється, перевіряється, 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 господарської діяльності 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 господарської діяльності, 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 господарської діяльності. Ця робота має передбачати збирання та обробку інформації з різних джерел різними підрозділами суб'єкта господарської діяльності. 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 господарської діяльності 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 господарської діяльності. Водночас така база має постійно оновлюватись і доповнюватись, щоб не допустити її старіння й формування певного ризику її використання.

5.Характеристика складників інформаційного забезпечення підприємства

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. 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 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. 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, судовий розгляд 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 розраховуються у банку, можна буде зробити об'єктивний висновок щодо надійності позичальника в його взаємовідносинах з банком.

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 господарської діяльності можуть бути:

- ризик втрати суб’єктом свого іміджу на певному ринку;
- ризик конфліктних ситуацій з власним персоналом, клієнтами, акціонерами, державними органами, 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 господарської діяльності 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 формуватися 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 господарської діяльності 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 господарської діяльності, 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 господарської діяльності 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 загальною 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 господарської діяльності 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 господарської діяльності 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 господарської діяльності, 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 господарської діяльності 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 господарської діяльності 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 господарської діяльності 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 господарської діяльності 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 господарської діяльності, формування в них фірмового патріотизму. Важливою частиною заходів мінімізації ризиків інформаційного тероризму є заходи з формування довіри до суб'єктів господарської діяльності 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, інформаційні ризики необхідно розглядати не як окремо взяті, а у сукупності з іншими ризиками господарської 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 господарювання у своїй діяльності.

🕮 Список рекомендованої літератури

1. Конституція України. Закон України від 28 червня 1996 р. *Відомості Верховної Ради України.* 1996. №30. Ст. 141.
2. Господарський кодекс України: Закон України від 16 січня 2003 р. № 436-IV. *Відомості Верховної Ради України*. 2003. №№ 18, 19–20, 21–22. Ст. 144.
3. Цивільний кодекс України від 16 січня 2003 р. № 435-IV. Відомості *Верховної Ради України.* 2003. № 40-44. Ст.356.
4. Про інформацію: Закон України від 2 жовтня 1992 р. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650.
5. Зубок М. І. Інформаційно-аналітичне забезпечення підприємницької діяльності. К.: ГНОЗІС, 2015. 216 с.
6. Кормич Б. А. Інформаційне право. Підручник. Харків: БУРУН і К., 2011. 334 с.
7. Крегул Ю.І., Зубок М.І. Правове регулювання безпеки підприємницької діяльності: навч. посібник. К.: КНТЕУ, 2013. 216с.