Економічні науки

УДК 338.12

Паславська Оксана Ігорівна

асистент кафедри адміністративного та фінансового менеджменту

Національний університет «Львівська політехніка»

АНАЛІЗ ПОТЕНЦІЙНИХ РИЗИКІВ ТА ПРЕВЕНТИВНІ ЗАХОДИ ЩОДО ЇХ УСУНЕННЯ ДЛЯ БІЗНЕСУ В СУЧАСНИХ УМОВАХ

Анотація. *Досліджено діяльність підприємств в сучасних умовах та виокремлено потенційні ризики, які впливають на їх діяльність. Також виокремлено основні заходи, які допоможуть мінімізувати вплив цих ризиків та ефективніше управляти бізнесом в умовах невизначеності.*

Ключові слова: *бізнес-середовище, захист інформації, антикорупційний комплаєнс, аудит, рейдерство.*

Економіка України сповільнилася взимку 2019-2020 року і почала вільне падіння навесні. На активність бізнесу різко вплинули слабкий зовнішній попит, карантинні заходи та непевність у своєму майбутньому.

Український бізнес опинився в унікальній ситуації. Події 2020 року стали довготривалим форс-мажором, який змусив більшість компаній змінити наявний формат роботи.

Як виявилося, більшість топменеджерів вважають перехід на дистанційний формат виправданим. Йдеться не тільки про переведення співробітників на дистанційну (повну або часткову) зайнятість. Зміни набагато глибше: починаючи з автоматизації бізнес-процесів, закінчуючи перебудовою ідеології менеджменту в компанії.

Бізнес пристосувався до нової карантинної реальності та побачив у ній переваги. Компанії скоротили адміністративні витрати – на утримання

офісів, діловодство. Відбувся перегляд критеріїв оцінки результативності співробітників. Одна річ, коли вся команда в зборі, зовсім інша – коли потрібно добитися продуктивності на відстані. Це вимагає серйозної самоорганізації та самодисципліни з боку як підлеглих, так і управлінців.

За даними онлайн-опитування суб'єктів підприємницької діяльності та ділових об'єднань Інституту економічних досліджень та політичних консультацій було виявлено, що пандемія вірусу COVID-19 і пов'язані з нею карантинні заходи негативно вплинули на більшість опитаних представників підприємств та організацій. Більшість з опитаних витримають від 1 до 3 місяців збереження існуючого обсягу карантинних заходів (рис.1) [1].

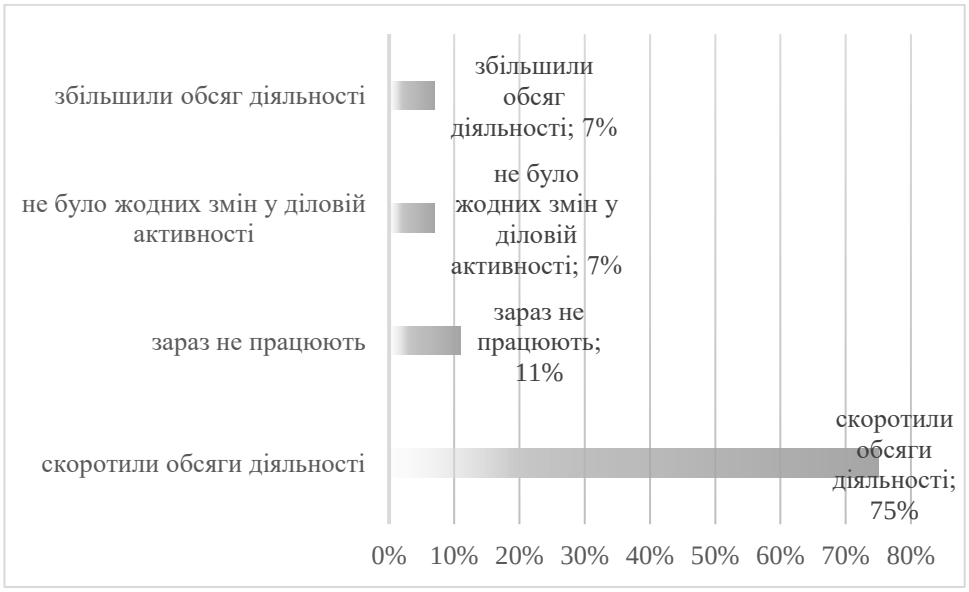

Рис. 1. Зміни ділової активності підприємств за час карантину

Серед основних ознак, що характеризують вплив карантинних заходів на підприємства та організації: необхідність переведення усього або частини персоналу на віддалену роботу та зміна графіку роботи; зменшення попиту на продукцію або послуги опитаних підприємств; складнощі з транспортуванням працівників; збільшення додаткових витрат; брак фінансових ресурсів для виплати заробітних плат та необхідність відправки

частини персоналу у відпустки; брак фінансових ресурсів для виконання контрактних зобов'язань та сплати податків (рис.2) [1].

Будь-який бізнес – це сукупність певних ресурсів. До цих ресурсів належать ті, що мають матеріальне вираження: нерухоме майно, обладнання, корпоративні права, так і ті, що виражені у нематеріальні формі: інформація щодо діяльності підприємства, її комерційні таємниці. Одним із ключових ресурсів є люди – топменеджмент та інші працівники компанії.

Чим масштабнішим стає бізнес, тим складніше стає його контролювати. Якщо на початку тримати все під контролем може його власник чи директор, то з його розвитком одній особі стає складно якісно організовувати всі процеси.

Одже, які на яких процесах контролю потрібно зосередити увагу, щоб ефективно управляти підприємством:

По-перше, це захист інформації. XXI століття це не стільки про вартість нерухомого майна, яке належить підприємству, скільки про захист інформації, яка обробляться ним. Втрата певних відомостей може призвести до різних негативних наслідків. Від витоку клієнтської бази, яку недобросовісні конкуренти можуть використати на власний розсуд, до протиправного заволодіння майном підприємства (так званого, рейдерського захоплення).

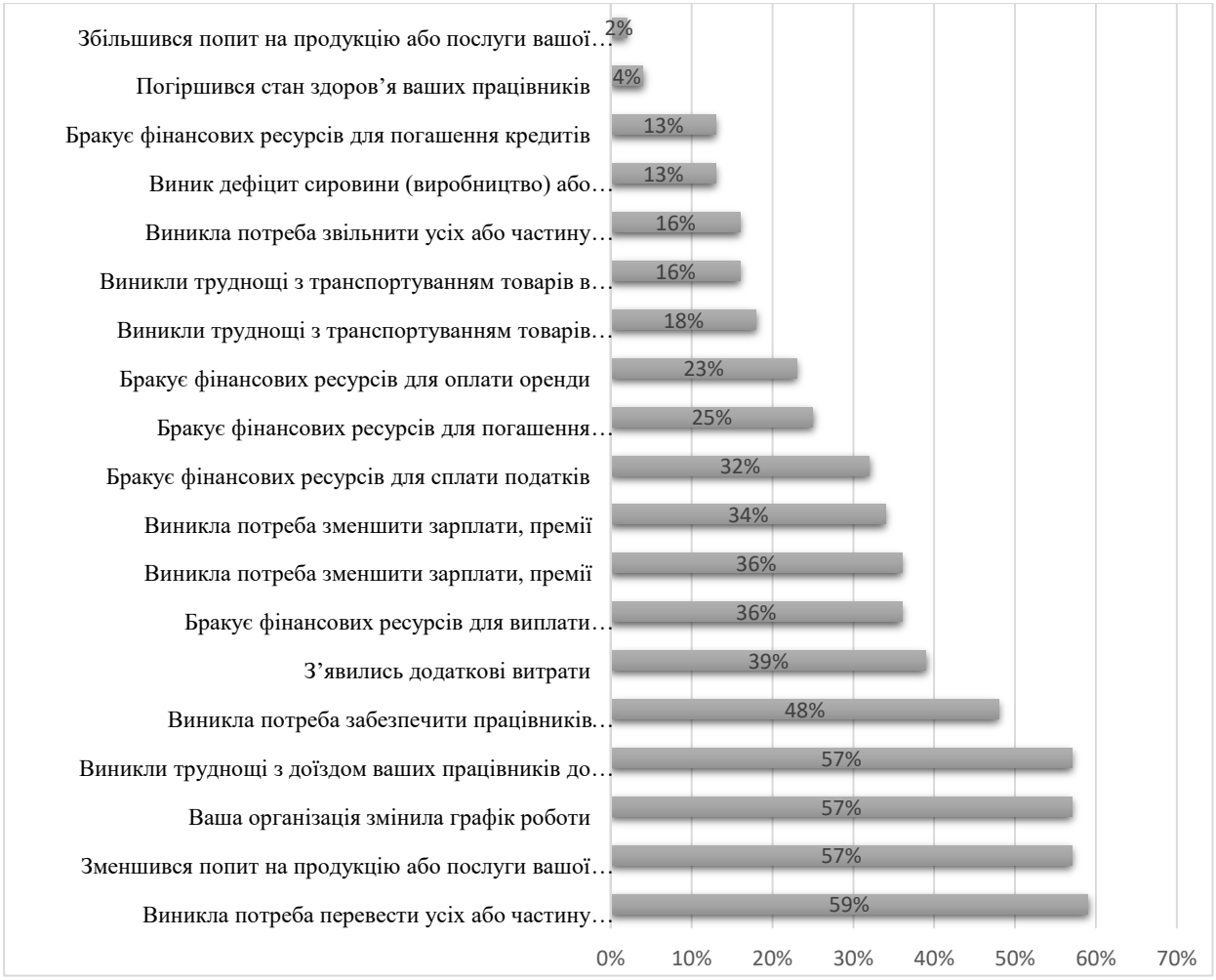

Рис. 2. Вплив карантину на діяльність організацій

Превентивні заходи відіграють істотну роль у системі контролю за обігом інформації на підприємстві. До таких заходів може бути віднесено [2]:

- Розробка політик конфіденційності, які повинні бути доведені до відома всіх працівників.
- Підписання договорів про конфіденційність із чіткими вимогами щодо фіксування наслідків витоку інформації (не захмарні штрафи, як це полюбляють вказувати більшість роботодавців, а чітка система встановлення грошового розміру шкоди).
- Використання ліцензованого програмного забезпечення для роботи із операційними завданнями бізнесу.

- Формування практик зберігання операційних документів у «хмарних середовищах».
- Запровадження електронного документообігу.
- Інші заходи у сфері IT, що спрямовані на попередження витоків інформації та хакерських атак на підприємство.

По-друге, контроль за людськими ресурсами. Серед наслідків недбалого ставлення до відбору працівників на підприємстві є корпоративне шахрайство, шпигунство за комерційною інформацією та ноу-хау, надання допомоги зовнішнім зловмисникам для рейдерського захоплення бізнесу, мобінг та булінг серед колективу працівників.

HR підрозділи та служби безпеки більшості підприємств вважають поліграф ефективним інструментом відбору кандидатів.

Процес проходження поліграфу є нормативно неврегульованим. Основне, чого вимагає чинне законодавство – дозвіл на збір та обробку персональних даних у разі його проходження. Також необхідно обов'язково отримати згоду працівника на проходження поліграфологічного дослідження.

До інших систем контролю у сфері людських ресурсів належить віднести:

- Підтримання та оцінка психологічної атмосфери в колективі (аналіз можливих скарг працівників, особливо на неналежні умови оплати праці, такі нарікання можуть стати тривожним дзвіночком до корпоративного шахрайства).
- Аналіз ділового листування, яке здійснюється працівниками на корпоративній пошті (за завчасного повідомлення про це самих працівників), окремі слова можуть свідчити на підготовлюване шахрайство чи привласнення ресурсів.

- Систематичні навчання працівників про системи корпоративної безпеки, правила поводження з інформаційними ресурсами, правила комунікації із клієнтами.
- Наявність постійного зворотного зв'язку від клієнта про якість послуг, що надаються компанією (можливо, працівник надає послуги «в обхід» основного бухгалтерського обліку компанії).

Фактично, у питаннях людських ресурсів досить важко сформувати письмові документи, які б визначали стандартні правила поводження працівників, адже людські взаємини важко піддаються формалізації. Водночас рекомендується розробити та довести до відома всіх дотичних працівників кодекс етики працівника компанії, правила ділового листування, правила комунікації із клієнтами, основні положення про системи запобігання корпоративного шахрайства.

По-третє, антикорупційний комплаєнс. Не всі юридичні особи зобов'язані розробляти антикорупційну політику. Однак це не означає, що бізнес, який не має відношення до державної форми власності, повинен анігілювати цей загальноєвропейський тренд.

До заходів антикорупційного комплаєнсу відносять розробку певних політик щодо поведінки із державними органами, правоохоронними органами, недопустимості «негласного спілкування» із працівниками цих органів для «пришвидшеного розгляду» питань від яких залежить діяльність підприємства.

Ці документи повинні бути не лише розроблені на підприємстві. Вони повинні бути доведені до відома всіх працівників, а також повинна бути прописала система їх впровадження в щоденну діяльність компанії. До такої системи належить як діяльність комплаєнс-офіцера, так і існування системи повідомлень про корупційні практики на підприємстві (заохочення whistleblowers).

Оцінюючи реалії національного ринку можна скептично поставитися до активного запровадження практики існування захищених каналів інформації, де працівник підприємства повідомлятиме уповноваженому офіцеру інформацію щодо підозрілих дій свого керівника чи іншого колеги. У той же час, світова практика рухається у цьому напрямку.

Більше того, недотримання певних правил чи політик компанії щодо запобігання корупції може мати суттєві наслідки:

- Ініціювання кримінального переслідування за корупційні злочини.
- Обшуки на території підприємства та тимчасові доступи (вилучення) документів, що становлять комерційну таємницю.
- Застосування заходів кримінально-правового характеру до юридичної особи (конфіскація майна, штраф та ліквідація компанії).

Таким чином, основним документом, який визначає напрямок внутрішнього контролю на підприємстві є антикорупційна програма, яка включає опис всієї системи антикорупційного комплаєнсу компанії із розподілом обов'язків серед структурних підрозділів та посадових осіб.

По-четверте, контроль нерухомого майна, та інших активів, що підлягають реєстрації. Не менш важливими активами компанії є нерухоме майно та корпоративні права. Вони можуть складати основні виробничі потужності підприємства, а тому їх фактична (та юридична) втрата може призвести до зупинення діяльності бізнесу.

Мова йде про рейдерство у різних формах: від фізичного «віджимання» бізнесу до використання недоліків статутних документів і конфлікту співвласників бізнесу. Так за допомогою судових спорів можна змінити розподіл часток у статутному капіталі та перереєструвати нерухоме майно.

До цього може призвести відсутність належного обліку рухомого майна, не введення в експлуатацію нерухомого майна, недосконала система

зберігання установчих документів та печаток компанії, існування практики проставляння підпису керівника замість нього іншими особами.

Заходи, для запобігання від ризиків у цій частині системи контролю [3]:

- Подбати про наявність «запасного аеродрому» (примірник нотаріально засвідчених установчих документів, альтернативні банківські рахунки, про які будуть знати лише засновники компанії).
- Відстежувати інформацію про компанію в реєстрах відкритих даних.
- Внести зміни до статутних документів щодо можливості припинення повноважень топменеджменту фірми із мінімальними ризиками для бізнесу (наявність законних підстав для розірвання контракту).

У контексті рейдерства є не менш важливим забезпечення фізичної охорони підприємства. Адже навіть за успішної юридичної роботи адвокатів (скасування неправомірних реєстраційних дій щодо майна та корпоративних прав підприємства), зазвичай, досить важко відновити фактичний контроль за бізнесом.

По-п'яте, аналіз контрагентів та конкурентів. Це виправдано не лише в контексті недбалого виконання домовленостей у майбутньому, а й в контексті потенційного кримінального переслідування керівника компанії за фінансування тероризму, ухилення від сплати податків та інших малоприємних речей.

Як відомо, для того, щоб привернути увагу правоохоронних органів до фінансування тероризму, не потрібно мати договори поставки певного обладнання із терористичними організаціями «ЛНР»/«ДНР». Достатньо бути трішки необачним та укласти договір із компанією, що є в санкційному списку або ж яка має певні філії на території вище згаданих організацій.

Усе це дасть можливість правоохоронним органам розпочати кримінальне переслідування, яке може і не минутися безболісно для бізнесу (внаслідок численних обшуків, конфіскації документації).

Основні політики, які можуть бути спрямовані на запобігання цій категорії ризиків – придбання платних програм для аналізу контрагентів, розробка внутрішніх інструкцій, які врегульовуватимуть процедури внутрішнього аналізу контрагентів та документальної фіксації перевірки по кожному контрагенту.

По-шосте, контроль якості претензійної та позовної роботи. Перш за все, заборгованість повинна зазначатися у окремих видах фінансової та податкової звітності. З іншої сторони, недбале ставлення до дебіторської заборгованості (особливо, якщо це розрахунки у сферах, що пов'язані із освоєнням державного бюджету), може призвести до обґрунтованих підозр правоохоронців про причетність до привласнення бюджетних коштів [2].

Звісно, підприємництво – це ризикова діяльність, і кожен власник бізнесу самостійно вирішує, яка заборгованість повинна ставати предметом судових процесів, а яка – ні. Однак якщо підприємство виконує певні роботи (чи надає послуги) за державні кошти, то будь-яке недбале ставлення до контролю за виконанням субпідрядних договорів може бути поставлене у вину керівнику компанії.

Інше питання – ділова репутація підприємства. Звісно, публічні комунікації важко віднести до тих сфер діяльності, які вимагають певних юридичних механізмів. Однак коли в Інтернет-просторі наявна певна негативна та недостовірна інформація про компанію, вона не повинна ігноруватися менеджментом. У цьому випадку, належить звертатися із позовами про захист ділової репутації компанії.

Для забезпечення цієї складової системи контролю на підприємстві повинно бути розроблено положення про договірну роботу, яке не лише включатиме порядок та відповідальність при розробці проектів договорів, а й порядок контролю за їх виконанням. Положення про посадові обов'язки працівників юридичного відділу дозволять чітко розподілити сфери відповідальності та убезпечити підприємство від ризиків у цій сфері.

По-сьоме, регуляторна, фінансова та бухгалтерська дисципліна. Незважаючи на прагнення Уряду зменшити регуляторний тиск на бізнес, залишається чимала кількість законів та підзаконних актів, які належить дотримуватися у тій чи іншій індустрії. Їх недотримання може цілком реально загрожувати кримінальною справою щодо керівника або ж певної посадової особи підприємства.

Найбільш поширений приклад – кримінальні правопорушення проти безпеки виробництва. До них можна віднести порушення правил охорони праці, які спричинили певні наслідки для здоров'я працівників.

Першою деталлю, на яку звертають увагу посадовці – наявність підписаних інструктажів про дотримання правил охорони праці на підприємстві (особливо це актуально для підприємств, які належать до сектору виконання робіт з підвищеною небезпекою).

Тому на підприємстві обов'язково повинен проводитись аудит на предмет дотримання регуляторного законодавства. Під час аудиту буде оцінено коло нормативних актів, яких повинне дотримуватися підприємство, виявлені конкретні порушення, а також заходи, яких належить ще вжити, щоб запобігти можливим виявленням правопорушень Держпраці, Держпродспоживслужби та інших державних органів [3].

Окремо слід відзначити про дотримання фінансової та бухгалтерської дисципліни. У той же час, не варто забувати про те, що за наслідками планової чи позапланової податкової перевірки (у випадку наявності порушень у податковій звітності) може бути ініційоване кримінальне провадження.

Методи правоохоронних органів в частині розслідування податкових злочинів є доволі різкими та такими, що «запрограмовані» на блокування роботи бізнесу. Відтак, належить із усією уважністю поставитися до комунікації із податковими органами, своєчасного оскарження податкових повідомлень-рішень з якими не погоджується підприємство.

Висновок. Порад та вимог можна визначати десятками, але без детального аналізу кожного окремо взятого підприємства впровадити дієву систему захисту бізнесу буде вкрай важко. Контроль повинен бути зовнішнім, тобто не залежати від діяльності компанії і не бути підпорядкованим одному засновнику чи керівнику. Тільки при такій побудові системи контролю на підприємстві можливо уникнути більшості згаданих ризиків та загроз.

Підхід до контролю вже сьогодні змінився через пандемію. Діяльність усіх компаній стала розмита, змінена, а часто й розбалансована. Як результат, з'явилася комерційна інформація на особистих незахищених носіях працівників. Доступи до баз даних тепер все частіше відбуваються через незахищені мережі, документація «розбіглася» по домівках працівників. І це лише та невелика частина щоденних викликів.

Література

1. Аналіз результатів online опитування суб'єктів підприємницької діяльності та ділових. URL: http://www.ier.com.ua/ua/institute/news?pid=6363
2. Україна у 2020-2021 роках: наслідки пандемії. Консенсус-прогноз. URL: https://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=5d3fea53-45e7-4641-8d48-f0c865a24471&title=VipuskukrainaU2020-2021-Rokakh-NaslidkiPandemii-Konsensusprognoz-kviten2020-
3. Звіт про проведення національної оцінки ризиків у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, та фінансуванню тероризму. URL: https://finmonitoring.in.ua/NRA2019.pdf