SAYENKO KHARENKO

pwc

Оцінка безпеки ведення бізнесу в Україні

Опитування серед керівників та власників середнього та великого бізнесу

100+
респондентів

Україна
місце проведення

Період проведення: ЧЕРВЕНЬ-ВЕРЕСЕНЬ 2021

Сергій Погребной

2020 рік, 2021 рік та попереду 2022 рік. Три роки пандемії, три роки ситуації, з якою ніколи не стикалося наше покоління та наш бізнес. Нові ризики, нові обмеження, нові можливості. Війна, що триває, й очікувана економічна криза в новому постковідному світі. На загальносвітовому фоні в нас і свої не найсприятливіші очікування для бізнесу: закон 5600, реформи правоохоронної та судової систем, що тривають, зміна частини складу Кабінету Міністрів України, санкції, різке зростання ціни на газ і багато інших політичних і державних подій.

Аби зрозуміти, як змінюються загрози та ризики для бізнесу із року в рік і які тенденції цих змін, Sayenko Kharenko та PwC, SK Security, за підтримки АПКБУ та ASIS Ukraine, більшості бізнес-асоціацій, бізнес-клубів та ТПП провели це опитування. Ми вдячні кожному, хто знайшов час та відповів на наші запитання. Ми сподіваємося, що всі ваші відповіді, отримана нами статистика та показники на їхній основі, будуть враховані та використані бізнес-спільнотою України, державними структурами, включаючи РНБО, Кабінет Міністрів України та відповідними комітетами Верховної Ради на загальне благо.

«Попереджений – значить озброєний» – стара істина, яка зараз діє, як ніколи. Звичайно, ви ознайомитеся з усіма даними у звіті, але необхідно зазначити деякі факти окремо: 2 % підприємств зазнали терористичних атак, минулого року ніхто не вказував цей факт, у півтора рази зросли корпоративні конфлікти, майже чверть підприємств зазнали нападів, крадіжок та грабежів. Є й добрі новини, на чверть зменшилася кількість кризових ситуацій із правоохоронними органами.

Ми будемо вдячні за зворотній зв'язок після ознайомлення зі звітом. Ми запрошуємо тих, хто ніколи не брав участі в опитуванні, приєднатися до нас у 2022 році, аби наші дані стали ще більш коректними та реально відображали стан безпеки ведення бізнесу в Україні.

Ми сподіваємося, що ваші команди з безпеки та ризик-менеджменту врахують наші дані для розвитку бізнесу в новому році і вони допоможуть вам стати успішними у 2022 році.

З повагою,
Сергій Погребной

Партнер Sayenko Kharenko
Голова Опікунської Ради АПКБУ
Віцепрезидент ASIS Ukraine

Андрій Третяк

Сучасний світ стрімко змінюється. А разом із ним – не лише бізнес-середовище, а й виклики, які постають перед компаніями. В цьому контексті питання безпеки й надалі залишаються в пріоритеті для забезпечення сталого розвитку бізнесу в Україні (як локального, так і міжнародного), а також відіграють важливу роль в контексті економічного розвитку України та її інвестиційної привабливості.

Команда форензік експертів PwC Україна та команда юристів Sayenko Kharenko об'єднали досвід та експертизу, щоб зрозуміти, з якими проблемами в частині безпеки бізнесу найчастіше стикаються компанії, а також підготувати практичні рекомендації щодо шляхів їх вирішення. На нашу думку, саме синергія юридичних консультантів та форензік-фахівців є найефективнішою для боротьби з шахрайством – як з нормативно-правової точки зору, так і з точки зору розробки антикризової бізнес-стратегії та мінімізації внутрішніх ризиків.

Ми вважаємо, що запорукою успіху є не лише інвестиції в операційну діяльність, але також розробка і впровадження програм, інструментів та технологій для її належного захисту.

Сподіваюсь, результати нашої спільної роботи будуть цікавими та корисними для вас. А також, допоможуть вам та вашому бізнесу впевнено та злагоджено протистояти сучасним викликам й досягати нових вершин.

З повагою,
Андрій Третяк

Керівник практики Форензік PwC в Україні
Сертифікований експерт з питань шахрайства (CFE)

Основні відомості

Традиційно для нашого опитування ми намагаємося обрати релевантну аудиторію респондентів. І цього разу наша добірка відображає рівномірну присутність груп компаній, що відрізняються за кількістю персоналу, наявністю або відсутністю власної СБ та походженням капіталу.

Ці показники ми тримали в центрі уваги й минулого року, хоча вони були дещо відмінні: тоді в опитуванні взяли участь так само понад 100 компаній, але майже половина з них мала понад 500 працівників у штаті.

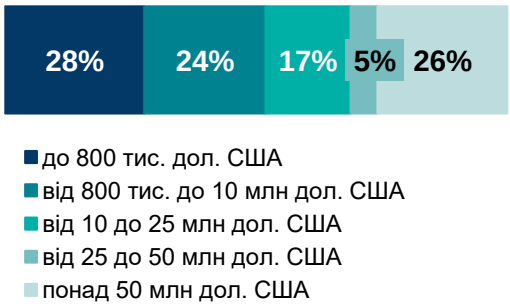
Походження капіталу

68 %
Український бізнес

32 %
Бізнес з іноземними інвестиціями

Кількість співробітників

Розмір капіталу



Галузь компанії

Виробництво/промисловість	19 %
Професійні послуги	13 %
Сільське господарство	10 %
Сервісні послуги	9 %
Споживчі товари	5 %
Проектування та будівництво	5 %
Інформаційні технології	5 %
Управління активами	4 %
Роздрібна торгівля	4 %
Енергетика	4 %
Благодійність та ГО	4 %
Фінансові послуги	2 %
Оборона та безпека	2 %
Автомобільна галузь	2 %
Юридичні послуги	1 %
Інші галузі	9 %

Ставлення до професійної безпеки

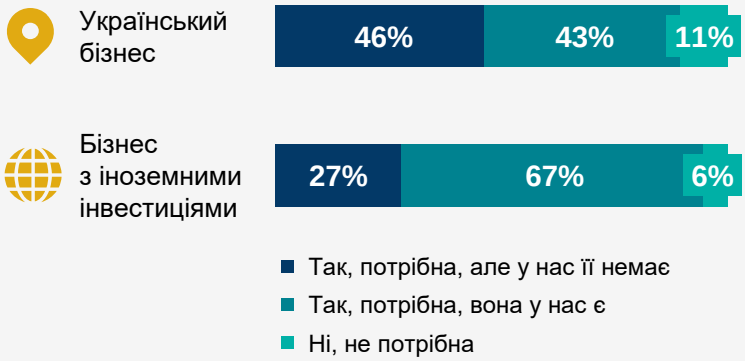
Пропорції компаній з різним за походженням капіталом не змінились, а от кількість компаній, що мають власну службу безпеки збільшилась і наразі складає половину серед усіх респондентів (минулого року серед опитаних респондентів їх було лише 32 %).

У цьогорічному опитуванні ми зробили, на нашу думку, вагоме уточнення щодо вибірки компаній, у яких немає власної служби безпеки.

Виявилось, що приблизно п'ята частина з них не має такої потреби, або на сьогодні так вважає.
Ми з обережним відчуттям доброї перспективи для системних безпекових та консалтингових компаній констатуємо, що до 40 % респондентів відчувають потребу в створенні власних служб безпеки. А може, це свідчення «розігрівання» ринку послуг безпеки, який дехто вважає «занадто холодним»?

Наявність у компанії власної служби безпеки

Погляд бізнесу, у якого ще немає власної СБ, на реальну потребу в ній



Вдосконаливши методологію досліджень, під час опитування, ми додали новий варіант відповіді. Він дав змогу уточнити пропорції компаній, що мають або не мають власну службу безпеки. Виявилось, що 11 % українських компаній вважають, що за чинних умов їм не потрібна власна СБ взагалі.

Ми вважаємо такий висновок перебільшеним, спираючись на отримані статистичні дані про великі компанії, серед яких лише 2,9 % вважають так само, та думку бізнесу з іноземними інвестиціями, серед якого про непотрібність власної служби безпеки також повідомили лише 5,6 % респондентів.

Сприйняття бізнес-клімату в Україні

Майже половина (48 %) респондентів переважно негативно оцінюють бізнес-клімат у країні: 10 % вкрай негативно і 38 % погано. Позитивно характеризують ситуацію 52 %, з яких 46 % вважають бізнес-клімат задовільним і лише 6 % позитивним.

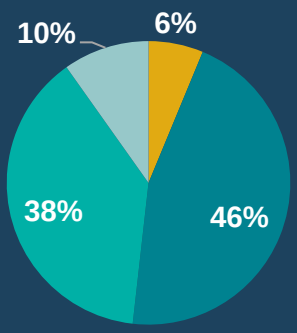
Цього року, незважаючи на загальний негативний настрій через глобальні кризові ситуації (в геополітиці, макроекономіці, охороні здоров'я тощо), відповіді респондентів загалом виглядають позитивнішими (різниця у порівнянні з минулим роком у 12 % суттєва і знаходиться за межами статистичної похибки). Так минулого року 60 % респондентів оцінювали бізнес-клімат в Україні переважно негативно, і лише 2 % - добре.

Розміри компаній (як за кількістю персоналу, так і за капіталом) впливають на оцінювання бізнес-клімату. Більші за розміром компанії оцінюють бізнес-клімат в Україні позитивніше, якщо точно - на 5 %.

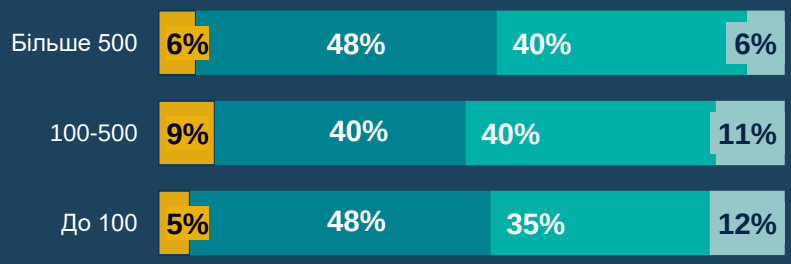
Але ще більша різниця в позитивному сприйнятті серед компаній, найбільших за розміром капіталу – ця тенденція простежується за графіком вище: компанії з розміром активів вище 25 млн доларів США переважно позитивно оцінюють бізнес-клімат, тоді як менші за розміром – переважно негативно.

На нашу думку, це цілком закономірно й може пояснюватися й тим, що у менших за розміром компаній ми виявили найбільшу потребу у створенні власних підрозділів безпеки - таких 71 %.

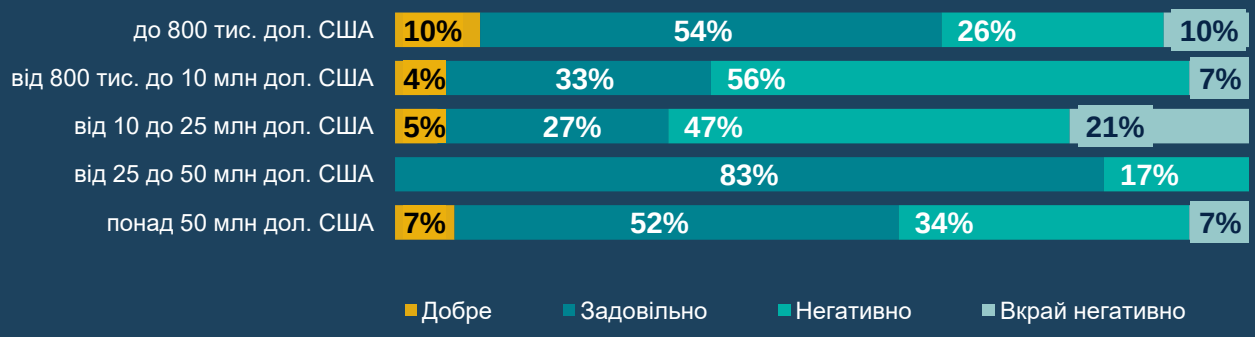
Оцінка бізнес-клімату в Україні



Залежно від розміру компанії



Залежно від розміру активів компанії



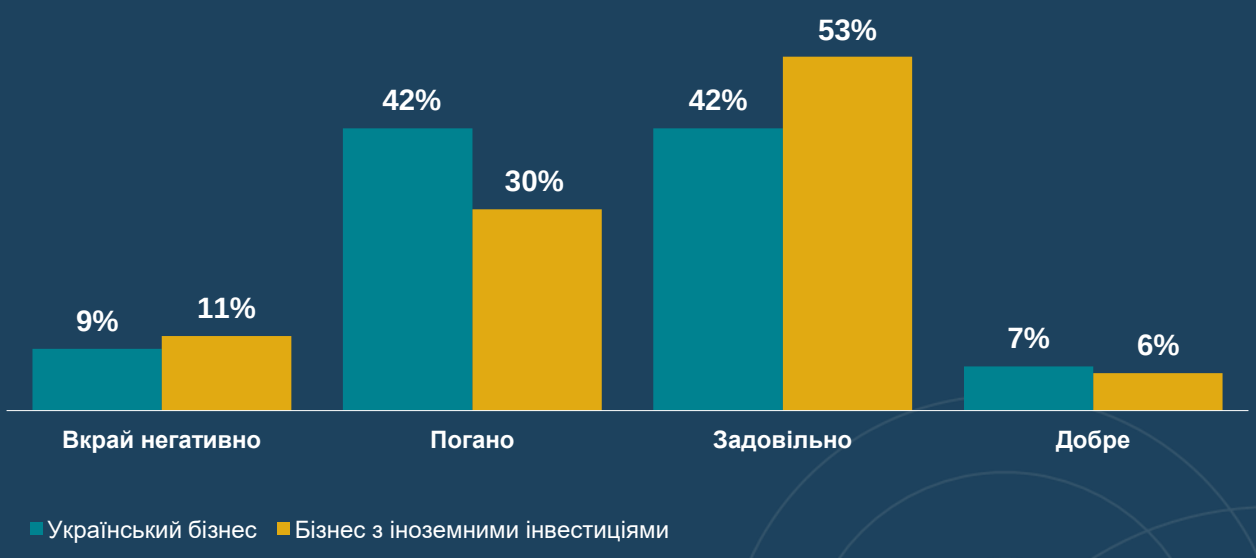
Сприйняття бізнес-клімату різними за походженням капіталу компаніями

Походження капіталу компанії впливає на оцінювання бізнес-клімату. Представники українського бізнесу констатують більш негативний стан, порівнючи з бізнесом із іноземними інвестиціями: 52 % негативних оцінок проти 42 % відповідно. Як цілком добрі оцінюють умови ведення бізнесу лише приблизно 6 % - 7 % респондентів. Порівнюючи з даними минулого року, коли добрим бізнес-клімат вважали в середньому 2 % респондентів, здається, маємо позитивну тенденцію, але треба зважити на коронакризу, як чинник, який вже другий рік поспіль вносить суттєвий дисбаланс у сприйняття стабільності загалом, а не лише в економіці.

Можливо ми (респонденти) у 2021 році пристосувалися до життя в умовах коронакризи?

Зазначені дані корелюються з рівнем уваги до професійної організації безпеки: майже половина українського бізнесу (46 %) не має у власній структурі підрозділу, головним завданням якого, є забезпечення безпеки діяльності компанії, а 67 % бізнесу з іноземними інвестиціями навпаки – має власну службу безпеки.

Сприйняття бізнес-клімату різними за походженням капіталу компаніями



Світові тренди корпоративної безпеки бізнесу 2022

Віктор ПАНЧАК, CPP®

Віцепрезидент SK Security
Голова Правління ASIS Ukraine
Член Правління АПКБУ

Вступ

Якщо розглядати поняття «*безпека бізнесу*», як своєрідний мікс оборонної та наступальної стратегії організації, то ставки на перемогу в цьому змаганні зросли, як ніколи раніше, і стали особливо критичними. Адже, як тільки бізнесу вдається усунути вже виявлені ризики та загрози, з'являються нові та ще більш вишукані вразливості, через які *фізична безпека* стикається з безпрецедентними проблемами, а атаки на *кібербезпеку* компаній стають ще більш організованими та технічно вдосконаленими.

В глобалізованому світі бізнесу нові ризики вимагають нових правил взаємодії. Вони демонструють відповідь ринку корпоративної безпеки у 2022 році на існуючі виклики, а також показують, якими будуть наступні кроки щодо захисту активів бізнесу чи його антикризового управління.

Дискусія професіоналів та експертів індустрії безпеки на ці та інші нагальні теми відбувалася протягом останнього тижня вересня 2021 року у м. Орландо (Флорида, США), де проходила наймасштабніша подія року у світі корпоративної безпеки – форум **Global Security Exchange (GSX) 2021.**

Платформа GSX

Форум GSX спирається на 65-річну історію передового досвіду індустрії, що об'єднує професіоналів з корпоративної безпеки, кібербезпеки, представників приватного і державного секторів, а також провідних виробників і постачальників рішень та сервісів у галузі.

GSX 2021 довів, що глобальна спільнота індустрії безпеки, як і раніше, прагне до розширення обміну знаннями, передовим досвідом та широкими зв'язками, щоб професіонали з безпеки в різних дисциплінах і на всіх етапах кар'єри могли отримати доступ до якісної інформації та професійних ресурсів, необхідних для досягнення успіху.

На форумі GSX окреслили ключові **світові тренди корпоративної безпеки бізнесу на 2022 рік.**

I. Поглиблення інтеграції фізичної безпеки та кібербезпеки.

Інтеграція, що розпочалася з періодом пандемії COVID-19, отримала свій власний термін – «*конвергенція*» (англ. *convergence*), або забезпечення спільної роботи функцій безпеки, управління ризиками і безперервності бізнесу, інформаційної безпеки в цілому та кібербезпеки з метою усунення прогалин і вразливостей, що виникли між цими функціями.

Повністю конвергентні функції, як правило, уніфіковані і взаємопов'язані та входять до кола обов'язків єдиного керівника служби безпеки. У них, зазвичай, загальні методи і процеси, а також єдина відповідальність за стратегію безпеки бізнесу. Конвергентні функції працюють разом та забезпечують більш інтегрований захист організації.

У 2020 році **ASIS International** провела ринкове опитування бізнесу щодо статусу конвергенції безпеки. В опитуванні взяли участь понад 1 000 професіоналів та експертів з безпеки, і суміжних безпекових сфер. Які ж були отримані результати?

24 % респондентів від бізнесу вже повністю об’єднали функції фізичної та кібербезпеки, а ще понад половина організацій (52 %) повідомили, що їхні підрозділи фізичної безпеки, кібербезпеки та/або забезпечення безперервності бізнесу тісно співпрацювали у напряму конвергенції, або інтегрувалися частко. Тенденція очевидна.

Переваги конвергенції безпеки та основні спостереження за результатами опитування:

a. Більш організоване загальне керівництво функцією безпеки бізнесу.

79 % опитаних згодні, що наявність єдиного лідера функції в організації підвищує загальну ефективність систем корпоративної безпеки та корпоративного управління бізнесу в цілому..

b. Конвергенція безпеки приносить матеріально вимірювану вигоду.

96 % організацій, що вже об'єднали дві або більше функцій безпеки, повідомили про позитивні результати від зміни, а 72 % вважають, що конвергенція дозволяє виміряти рівень оптимізації безпеки організації в матеріальних показниках.

c. Економія коштів не є основним драйвером конвергенції безпеки.

Лише 7 % тих, хто вже об'єднався, назвали зниження витрат на безпеку основною перевагою конвергенції. Водночас лише біля 20 % тих, хто ще не провів зміни, вказали потенційну економію коштів, як ключову причину, що може переконати їх об'єднати функції безпеки.

d. Ключовий чинник конвергенції – краще погодження загальної стратегії безпеки бізнесу з корпоративними цілями організації.

На запитання, що може бути найбільш переконливим у необхідності проведення конвергенції безпеки, 48 % тих, хто ще не провів зміни, назвали краще погодження загальної стратегії управління безпекою/ризиками з корпоративними цілями. Це найвищий показник категорії.

e. Відмінності в культурі та наборі навичок між видами безпеки – найбільша перешкода на шляху до конвергенції.

Ключовими проблемами, згаданими в компаніях, що вже провели конвергенцію функцій безпеки, були різні культури й набори навичок (36 %) та застаріла переконаність у тому, що кібербезпека вимагає виключно власного напряму роботи (21 %). Водночас, 22 % респондентів повідомили про очевидну відсутність таких проблем в підрозділах, що вже об’єдналися.

f. Пошук відповідного фахівця для керівництва об’єднаним підрозділом безпеки може виявитися доволі непростим завданням.

Різні види безпеки вимагають різного рівня кваліфікації, досвіду та професійної сертифікації фахівців. Наразі ще не має єдиного набору навичок «для всіх». Галузь конвергенції безпеки бізнесу лише стала на шлях розвитку та напрацювання глобального стандарту, тому ця робота відчиняє вікно можливостей для фахівців індустрії безпеки бізнесу.

g. Конвергенцію безпеки необхідно адаптувати до потреб бізнесу, культури індустрії та з обґрунтуванням причинно-наслідкового зв’язку.

Наприклад, у багатьох аеропортах чи лікарнях кібербезпека реалізується у форматі загального сервісу (shared service) на всіх об’єктах організації загалом, у той час, як фізична безпека забезпечується персоналом по-різному в окремо взятих місцях.

Для зазначених вище галузей бізнесу кібербезпека є централізованою, тоді як, фізична безпека - децентралізованою. І ці чинники необхідно дуже виважено аналізувати та оцінювати їхні ризики окремо.

II. Вдосконалення технологій безпеки для належної підтримки змін.

З початку пандемії злочинці насолоджувалися вразливістю компаній, що переходили на віддалену роботу, попри те, що підрозділи IT-безпеки компаній невпинно працювали над подоланням проблем, що виникали в процесі забезпечення належного рівня кібербезпеки. Водночас, більш технологічні компанії розпочали надавати нові та вдосконалені рішення безпеки для належної підтримки змін. Нижче наведемо прогнози таких тенденцій.

a. Перехід від кібератак інфраструктури до кібератак на окремих людей/працівників.

У той час, як атаки на вразливості систем, як і раніше залишатимуться одним з основних видів злочинної діяльності, треба очікувати зростання уваги до атак на окремих співробітників. Зростання кількості власних електронних пристроїв (так звані «BYOD») та пристроїв, що підключаються по бездротовій мережі і можуть передавати дані (так звані «IoT devices»), створюватимуть чималі проблеми в сфері кібербезпеки. Аутентифікація стане ще більшою проблемою, оскільки паролі будуть поєднуватися з іншими методами підтвердження, такими як смарт-карти, трифакторна аутентифікація, біометрія тощо.

b. Спроба вирішення складних завдань за допомогою комплексного підходу.

У 2022 році експертна спільнота індустрії безпеки очікує побачити певні «комплексні» рішення, спрямовані на забезпечення цифрової трансформації певних сегментів бізнесу. Зокрема:

- Нові інтегровані цифрові рішення для спрощеного пересування можуть замінити довгі черги реєстрації пасажирів у аеропортах, прикордонних пунктах тощо завдяки проведенню віддаленої перевірки особистості через смартфон.
- Гібридні платіжні цифрові рішення: об'єднання наявних технологій випуску фізичних платіжних карт із захищеними цифровими можливостями. Споживачі віддаватимуть перевагу поліпшеним функціональним можливостям програмних продуктів і онлайн послуг при виборі банків, установ та інших оплачуваних послуг. Це потребуватиме посиленого захисту і безпеки та зумовить виникнення додаткових ризиків.

c. Актуалізація принципу «нульової довіри» до технологій безпеки.

Підхід «нульової довіри» (англ. zero-trust) – принцип, за якого ви не довіряєте й перевіряєте все, що стосується користувачів та пристроїв, припускаючи, що мережа є «ворожою», і надаєте найменш привілейований доступ, необхідний для виконання програмних функцій. Звіт компанії «Entrust» за 2021 рік, опублікований у вересні 2021 року, показав значне збільшення технології перевірки ідентичності, а 36 % таких технологій використовують перевірку мобільних ідентифікаторів, що надає користувачам облікові дані на мобільному телефоні, аби отримати доступ до інформації всередині організації.

d. Захист даних, пов’язаних зі здоров’ям людей/працівників.

Акцент на обмін персональними даними стане ще більш поширеним у сфері охорони здоров’я. Зростання кількості програм, що стосуються системи охорони здоров’я, очевидно призведе до збільшення ризиків, пов’язаних з погіршенням способу поводження з персональними даними про здоров’я та їх масовий витік.

III. Кібербезпека. Переформатування кібербезпекових злочинів.

Кіберзлочини залишаться однією з найбільш суттєвих загроз. Дані відкритих джерел свідчать, що кіберзагрози лише за 9 місяців 2021 року призвели до колосальних збитків на загальну суму у майже 6 трильйонів доларів США.

Фактично за нинішніх темпів зростання таких злочинів у середньому на 15% «вартість» кіберзлочинності, як очікується, сягне 10,5 трильйонів доларів США до 2025 року. Тож на що ж слід очікувати бізнесу?

a. Посилення програми інформування та обізнаності користувачів.

Оскільки компанії усвідомлюють ризики кіберзагроз та вірогідну вартість завданих ними збитків, вони будуть змушені вкладати кошти у навчання та інформування співробітників. Окрім технологічного впровадження щодо захисту свого обладнання, програмного забезпечення та мереж, компаніям треба докласти більше зусиль для покращення знань співробітників за допомогою навчальних програм та семінарів. Звіти спеціалізованих досліджень показують, що дев'ять з десяти користувачів не можуть розрізнити авторизовану та фішингову електронну пошту. Навчання персоналу допоможе організаціям розпізнати, та хоча б частково пом'якшити зазначені вище ризики у сфері кібербезпеки.

b. Розширення локалізованих фішингових загроз із географічним націлюванням.

Опитування показали, що фішинг – найпоширеніша кіберзагроза, з якою стикаються компанії. У 2022 році очікується, що ця загроза переростатиме у ще більш персоналізований та цільовий ризик, зробивши працівників найбільш вразливими мішенями. За даними експертів, один із восьми працівників ненавмисно регулярно ділиться інформацією на фішингових вебсайтах. Ще одним чинником є те, що майже третина (32 %) від ВСІХ втрат даних бізнесу є результатом фішинг-листів.

Вивчення того, як організувати фішингову атаку теж допомагає протистояти цим загрозам. А поширення знань, отриманих за допомогою програм поінформованості всередині компанії, суттєво пом'якшує ризики зазначених фішингових загроз.

c. Актуалізація кіберпроблем, як наслідок формату тривалої віддаленої роботи.

Пандемія започаткувала для бізнесу тенденцію віддаленої роботи у світовому масштабі. Великі компанії заявляють, що продовжать надавати працівникам можливість віддаленої роботи і надалі. Проте такий формат організації бізнесу спричиняє новий комплекс проблем безпеки, які компанії все ще намагатимуться подолати у 2022 році. Зокрема, залежність від технологічних пристроїв, перехресне зараження даних, витік даних, погана безпека «хмар», фішинг та інсайдерські загрози.

Висновок

Передбачити точні шляхи розвитку комплексних безпекових тенденцій у бізнесі непросто, але фахівцям індустрії треба зважати на напрями та статистику, озвучені під час форуму GSX з корпоративної безпеки 2021, аби передбачити, як буде виглядати безпека бізнесу вже найближчим часом. Компанії та професіонали з безпеки і далі навчатимуться тому, як зміцнити свій захист та зберегти активи від ризиків та загроз. Тому ми чітко усвідомлюємо, що сучасні тенденції індустрії безпеки дають важливе уявлення про те, що саме нас чекатиме у наступному році.

Сприйняття кризових ситуацій різним за походженням капіталу бізнесом

Основними кризовими ситуаціями, з якими стикалися компанії у 2021 році, є незаконні дії державних органів (зазначили 43 % респондентів), незаконні конкурентні дії (42 %) та незаконні дії правоохоронних органів (33 %). Порівнюючи з минулим роком, незаконні конкурентні дії перемістилися у рейтингу кризових ситуацій з третього на друге місце.

Вони збільшилися не надто суттєво – лише на 3 %, але таке збільшення відбулося по ринку загалом, тому що пропорційне співвідношення кризових ситуацій, з якими стикалися компанії з різним за походженням капіталом (66 % компаній з українським та 34 % - з іноземним походженням капіталу), майже збігається з Портретом респондента (68 % на 32 % відповідно).

Кризові ситуації, з якими стикалися респонденти

Незаконні дії державних органів	43 %
Незаконні конкурентні дії	42 %
Незаконні дії правоохоронних органів	33 %
Медіа-атаки	25 %
Напади на активи, крадіжки, грабіж транспорту, врожаю, підприємств	23 %
Кібератаки	22 %
Корпоративні конфлікти	21 %
Кримінальні прояви	19 %
Жодних	15 %
Рейдерство	13 %
Напади на співробітників або власників компанії	4 %
Смерть власника компанії та вступ у спадщину спадкоємцем	4 %
Напади на власника та його родину	3 %
Інші	5 %

Сприйняття кризових ситуацій різним за походженням капіталу бізнесом

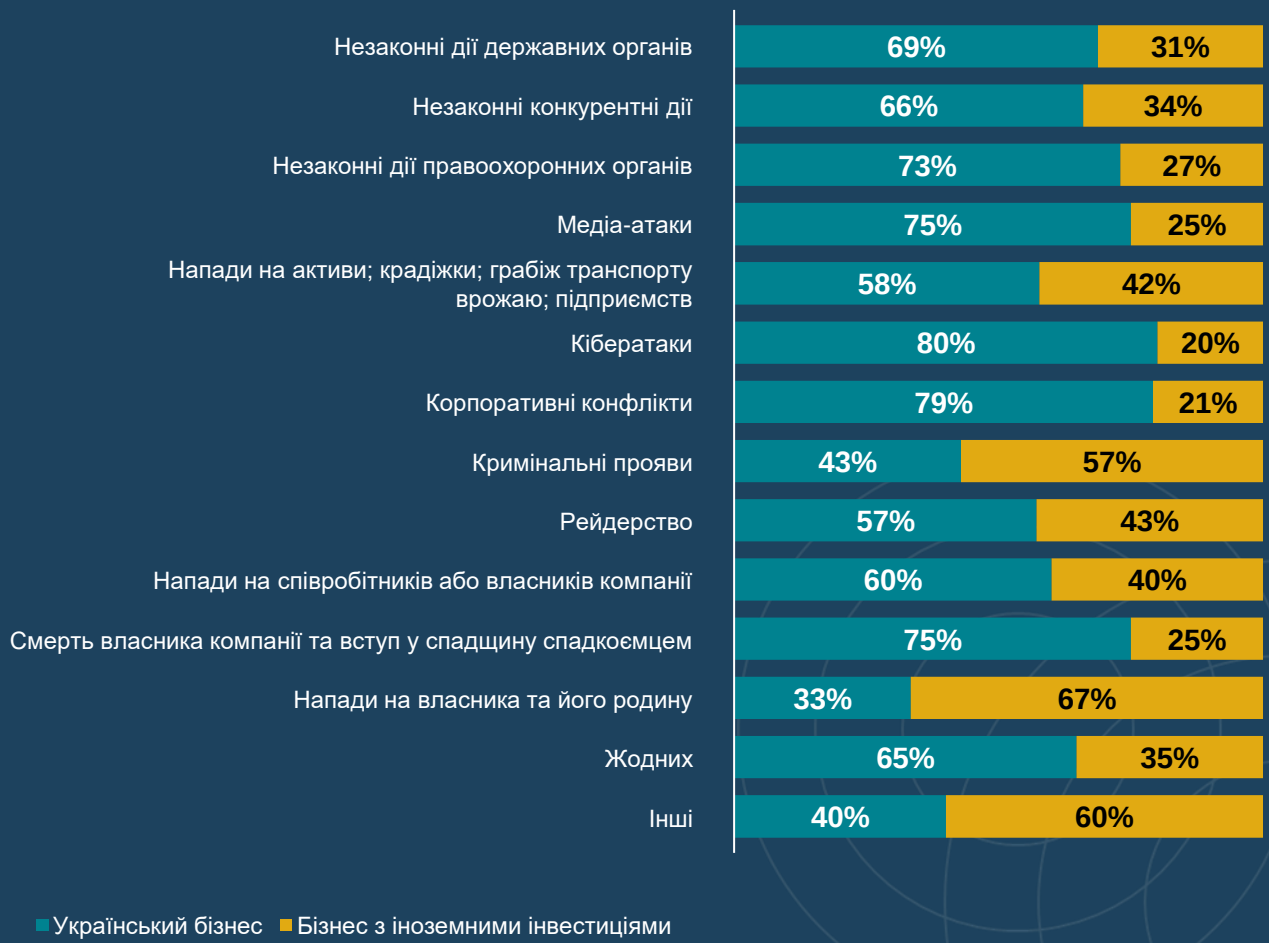
Відповідно до методології досліджень, ми порівнюємо між собою кількість випадків кожного виду кризових ситуацій, з якими стикались опитані компанії-респонденти.

Порівнюючи з даними 2020 року ми помітили зниження відсотків майже за кожним видом кризових ситуацій (окрім корпоративних конфліктів, кримінальних проявів та рейдерства).

Можливо, таке зниження інтенсивності відповідей респондентів, хоч якось пояснить аномальне збільшення кількості опитаних, які відповіли, що не стикались із жодними кризовими ситуаціями: таких цього року виявилось 15 %, а в минулому було лише 4 %.

Як і минулого року, вирізняється проблема кримінальних проявів та нападів на власника та його родину щодо бізнесу з іноземними інвестиціями, яка мала місце в 57 % та 67 % випадків відповідно. Український бізнес стикався з такими ситуаціями значно рідше – у 43 % та 33 % випадків відповідно.

Кризові ситуації з якими стикалися респонденти (за походженням капіталу)



Погляд на кризові ситуації з боку компаній, що мають власну СБ, та тих що її не мають

Не дивлячись на «статистичне» зниження інтенсивності кризових ситуацій, загалом, зберігається минулорічна тенденція, коли компанії без власної служби безпеки вказують, що рідше потрапляють у кризові ситуації. Виняток складають ситуації, пов'язані зі смертю власника та вступом у спадщину спадкоємця – про такі випадки у 75 % випадків повідомили саме компанії без власної служби безпеки.

З огляду на те, що такі ситуації мають найменший ступінь латентності, це лише підтверджує виявлену нами минулорічну тенденцію. Вона вказує на те, що компанії без власної служби безпеки насправді стикаються з такими проблемами, проте часто не ідентифікують їх, так і залишаючи латентними.

Додатково зауважимо, що таку тенденцію підтверджує й статистика найменших у нашій вибірці компаній, 71 % з яких потребують, але ще не створили власних служб безпеки.

Кризові ситуації з якими стикалися респонденти

Оцінка кризових ситуацій різними за розміром компаніями

Незаконні дії державних органів є основним видом кризових ситуацій (43 %), проте цього року майже стільки ж компаній відповіли, що стикаються з незаконними конкурентними діями (42 %). Серед останніх, найбільші за розміром компанії зазначили збільшену кількість випадків незаконної конкуренції (43 %), що вказує на триваючу останніми роками тенденцію до нарощування можливостей сил корпоративної безпеки.

Порівнюючи з минулим, цього року суттєво збільшилася кількість корпоративних конфліктів, особливо серед невеликих за розміром компаній (54 % проти 13 % минулого року).

Обидва статистичні спостереження запевняють нас у думці, що ринок послуг корпоративної безпеки якісно зростає і у найближчому майбутньому зростатиме. Додатково цей висновок підтверджують і статистичні дані про довіру до реально діючих інституцій, на які спирається бізнес у вирішенні конфліктних ситуацій (див. далі), згідно з якими, приватні (недержавні) структури безпеки вже котрий рік поспіль отримують найвищий рейтинг довіри. Цей рік не виняток – 43 %.

Кризові ситуації з якими стикалися респонденти (за кількістю співробітників)

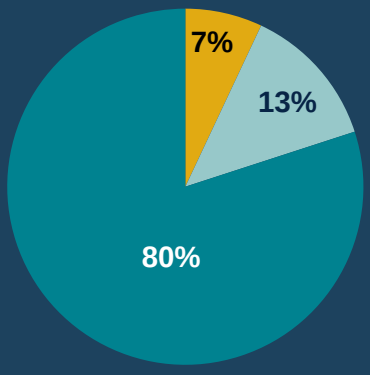
Способи вирішення кризових ситуацій, з якими стикається компанія

13,4 % компаній покладаються виключно на внутрішні ресурси у вирішенні будь-яких кризових ситуацій, 7 % практикують залучення зовнішніх експертів. Здебільшого опитані (80 %) комбінують підходи залежно від ситуації. Ця статистика майже не змінилась із минулого року, лише несуттєво укріпилася тенденція до використання внутрішніх ресурсів, але виключно завдяки українським компаніям, які діють у такий спосіб у 93 % випадків.

Можемо лише із сумом констатувати про послаблену роль аутсорсингу послуг безпеки, але це надихає у перспективах і свідчить про можливість розширення ринку корпоративної безпеки для системних «гравців», що будуть здатні завоювати довіру українського бізнесу.

З огляду на те, що питома вага українського бізнесу складає понад двох третин респондентів (68 %), ми бажали б відмітити, як вельми позитивний факт, що доля компаній, які залучають зовнішніх експертів, складає 50 %. Проте, цей позитив нейтралізує переважаюча доля «сірої зони». До якої належать компанії, що при вирішенні криз, ситуативно обирають, використовувати зовнішні або обмежитися внутрішніми ресурсами. Це свідчить лише про те, що здебільшого компанії (майже 80 %) не готуються до свого захисту заздалегідь (не укладають партнерських контрактів з адвокатами або безпековими компаніями, не складають угод про нерозголошення та не створюють технічних можливостей із сервісними компаніями), залишаючи це рішення до моменту настання кризової ситуації або її наслідків.

Всі компанії



- Залучаєте зовнішніх експертів
- Залучаєте виключно внутрішні ресурси
- В залежності від ситуації використовуєте внутрішні або зовнішні ресурси

Залежно від походженням капіталу

- Український бізнес
- Бізнес з іноземними інвестиціями

Способи вирішення кризових ситуацій, з якими стикається компанія

Природньо, що компанії без власної служби безпеки частіше (62 %) намагаються залучати зовнішні ресурси у вирішенні криз. Також очікувано, що ці ж компанії у 73 % випадків готові покладатися виключно на внутрішні ресурси (ймовірно вони на шляху до створення власних СБ).

Проте доволі цікава статистика щодо компаній, які мають власну службу безпеки, але покладаються на внутрішні ресурси лише у 26 % випадків. Водночас, вони менше залучають зовнішніх експертів (37 %), що передбачувано, але більше тяжіють до ситуативного вибору дій (56 %) ніж ті, хто не має власних СБ. Можливо, це свідчить про гнучкість, або про невпевненість у власній спроможності самостійно вирішувати кризові ситуації.

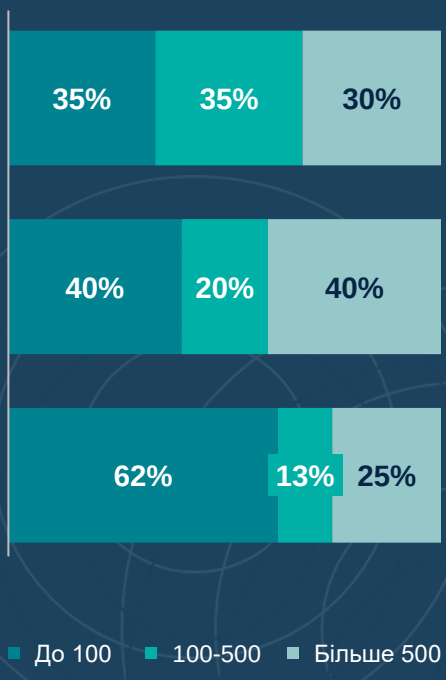
Особливо великий бізнес, як і минулого року, не залучає зовнішніх експертів для вирішення кризових ситуацій, тому що у 85,7 % таких компаній у штаті є фахівці, які мають її вирішити.

Найменші компанії, навпаки, найчастіше залучають зовнішніх експертів (у 62 % випадків).

Водночас, про готовність залучати виключно внутрішні ресурси вказали по 40 % респондентів, як з найбільших, так і з найменших компаній. Та мотивація такого рішення принципово різна: найбільші компанії мають можливість, а найменші – вимушені використовувати внутрішні ресурси. «Сіра зона», тобто схильність до ситуативного вибору дій, розподілена аналогічно Портрету респондента.

Різниця підходів у вирішенні кризової ситуації з боку компаній, що мають власну СБ, та тих, що її не мають

Як змінюється підхід до вирішення кризових ситуацій залежно від розміру компанії

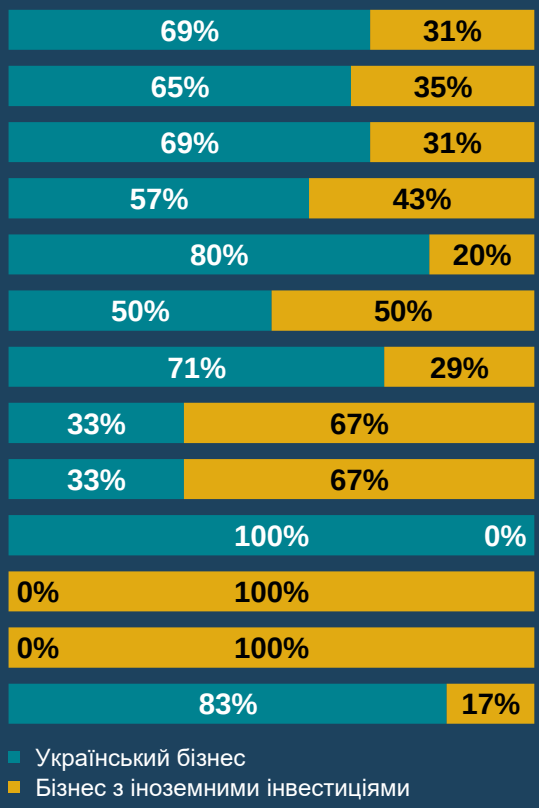


Довіра бізнесу до державних структур

Як відрізняється довіра до державних структур з боку українського та іноземного бізнесу

Всі компанії

За походженням капіталу



Рейтинг довіри респондентів збудовано на даних понад 100 опитаних компаній. Він, безумовно, нерепрезентативний, щоби гарантувати його цілковиту справедливість. Але мета опитування - виявлення тенденцій. Для цього ми ретельно відібрали респондентів, які рівномірно відображають компанії, що відрізняються за кількістю персоналу, наявністю або відсутністю власної СБ та походженням капіталу.

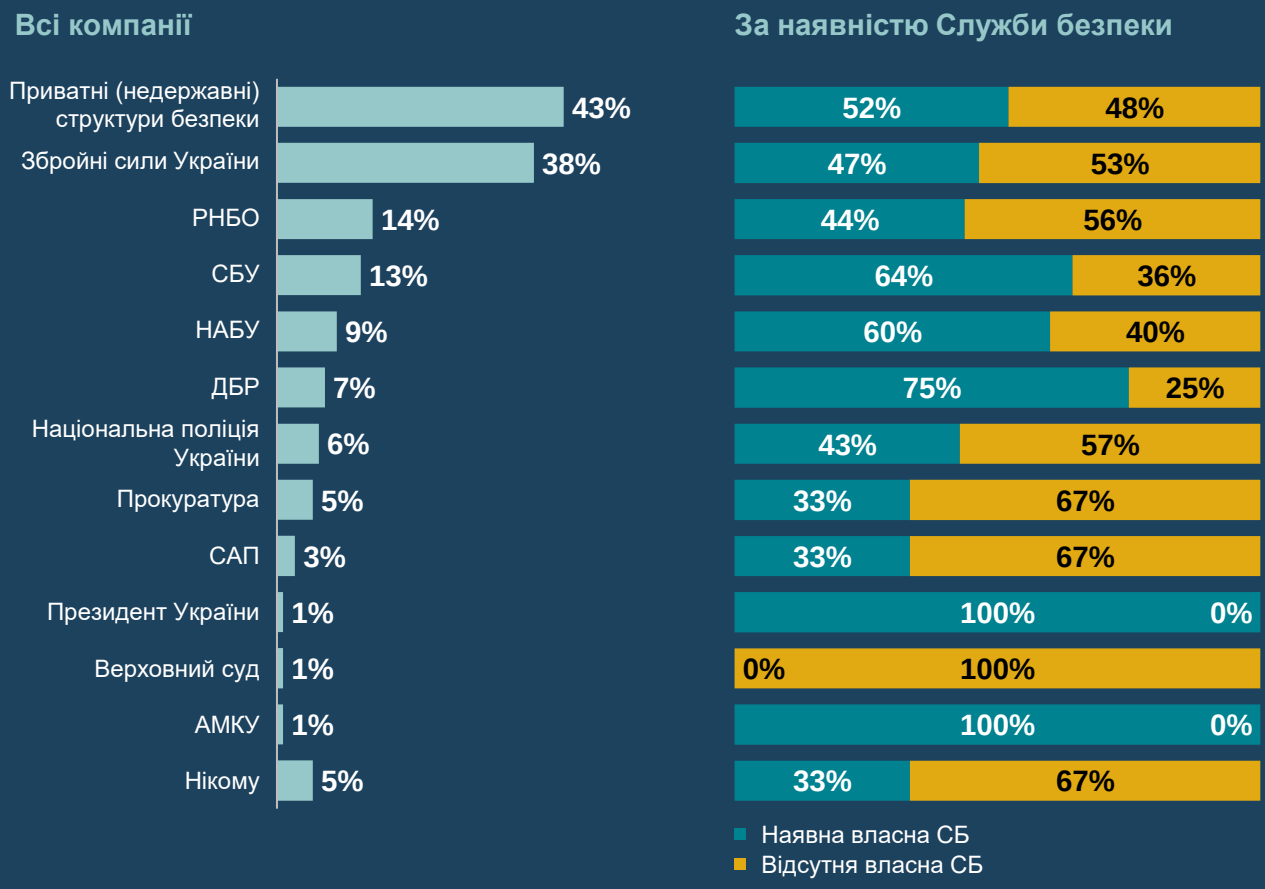
Рейтинг цього року проводився вперше, свою цінність він покаже в наступних роках, відтворюючи тенденції та даючи змогу більш ретельно аналізувати бізнес-клімат.

Проте він і зараз засвідчує довіру 43 % компаній (як українських, так і з іноземним капіталом) до приватних структур безпеки. Водночас, у ТОП-3 структура відповідей майже тотожна до Портрету респондента, що лише підкреслює правильну статистичну закономірність.

5 % респондентів взагалі не мають довіри до будь якої структури, водночас так вважають переважно компанії з українським капіталом (83 %).

Довіра бізнесу до державних структур

Як відрізняється довіра до державних структур в залежності від наявності у компанії власної Служби безпеки



Серед компаній, що не довіряють жодній структурі, переважають компанії, в яких не має власної служби безпеки (на 16 % більше у порівнянні з Профілем респондента).

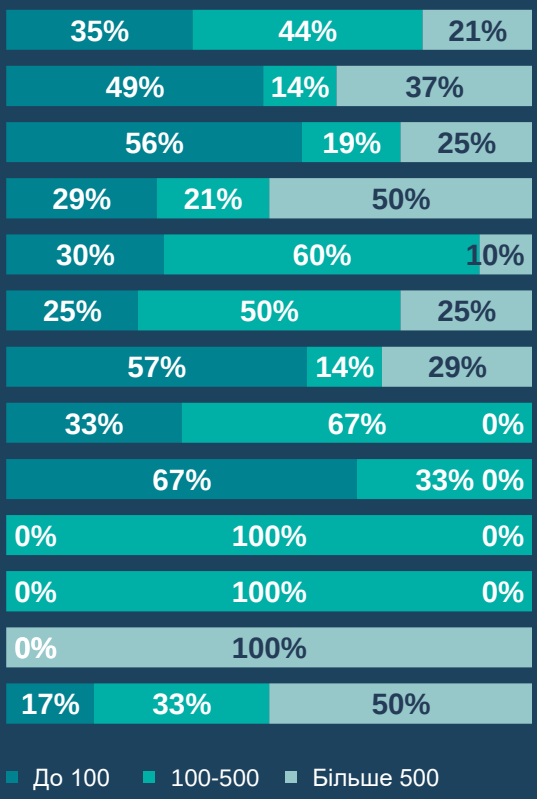
Інших інформативних закономірностей щодо залежності ступеню довіри від наявності у респондентів власної служби безпеки не виявлено. Але найбільша інформативність від оцінювання довіри до державних структур, на наше переконання, залежить від простеження динаміки змін, тому згодом аналіз буде покращуватися автоматично.

Довіра бізнесу до державних структур

Як відрізняється довіра до державних структур з боку різних за розміром компаній

Всі компанії

За розміром компанії (кількість співробітників)



Якщо не включати до підрахунку тих 5 %, хто не довіряє нікому, то майже кожна друга компанія найбільше довіряє приватним структурам безпеки. Цей факт є свідченням глобальної недовіри бізнесу до держави.

Формального пояснення потребує другий рядок рейтингу (38 % довіри), але це очевидно: Збройні сили України є державною структурою, що має найменші важелі впливу на бізнес, тому такий високий рейтинг довіри пояснюється високим ступенем патріотизму бізнесу.

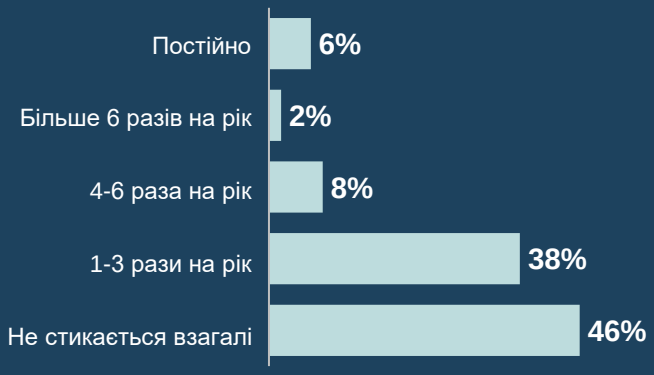
Серед компаній, що не довіряють жодній структурі, переважають найбільші за розміром компанії. Частка їхніх відповідей сягає 50 %.

Серед інших інформативних залежностей ступеню довіри від розміру компаній виділяються такі: про довіру до РНБО (56 %), Національної поліції (57 %) та САП (67 %) частіше вказують найменші за розміром компанії; найбільший бізнес менш за всіх довіряє приватним структурам безпеки (21 %), РНБО (25 %), НАБУ (10 %) та прокуратурі (0 %).

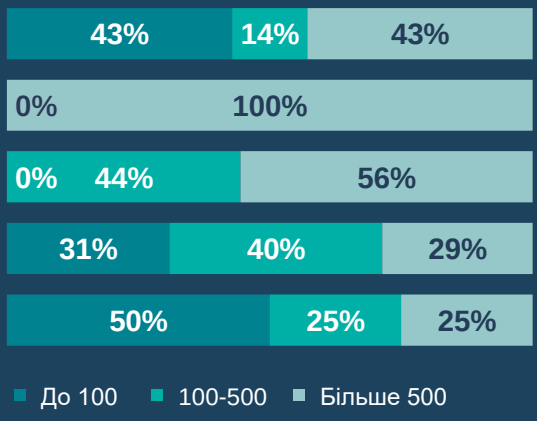
Особливості взаємодії з правоохоронними органами

Як часто бізнес стикається з активними діями правоохоронних органів

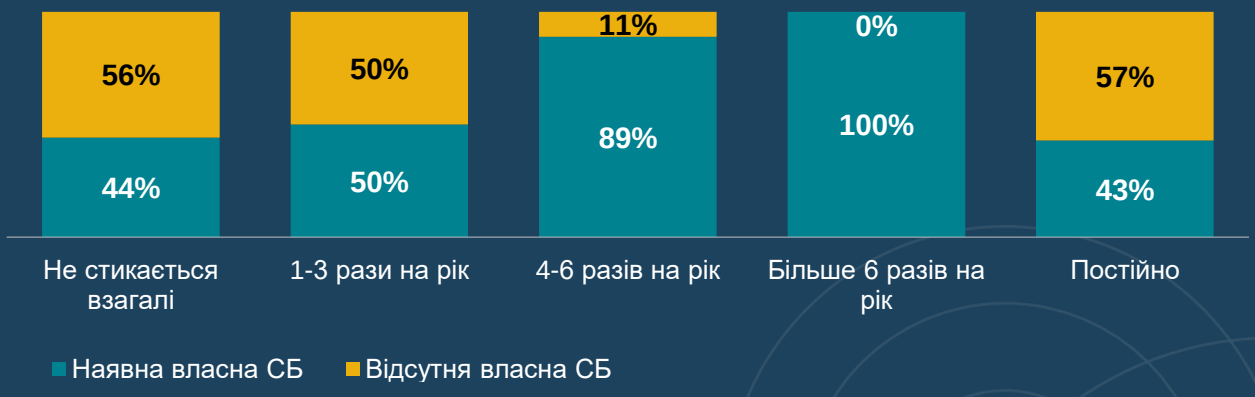
Всі компанії



За розміром компанії (кількість співробітників)



Як змінюється активність правоохоронних органів щодо компаній в залежності від наявності в них власної СБ



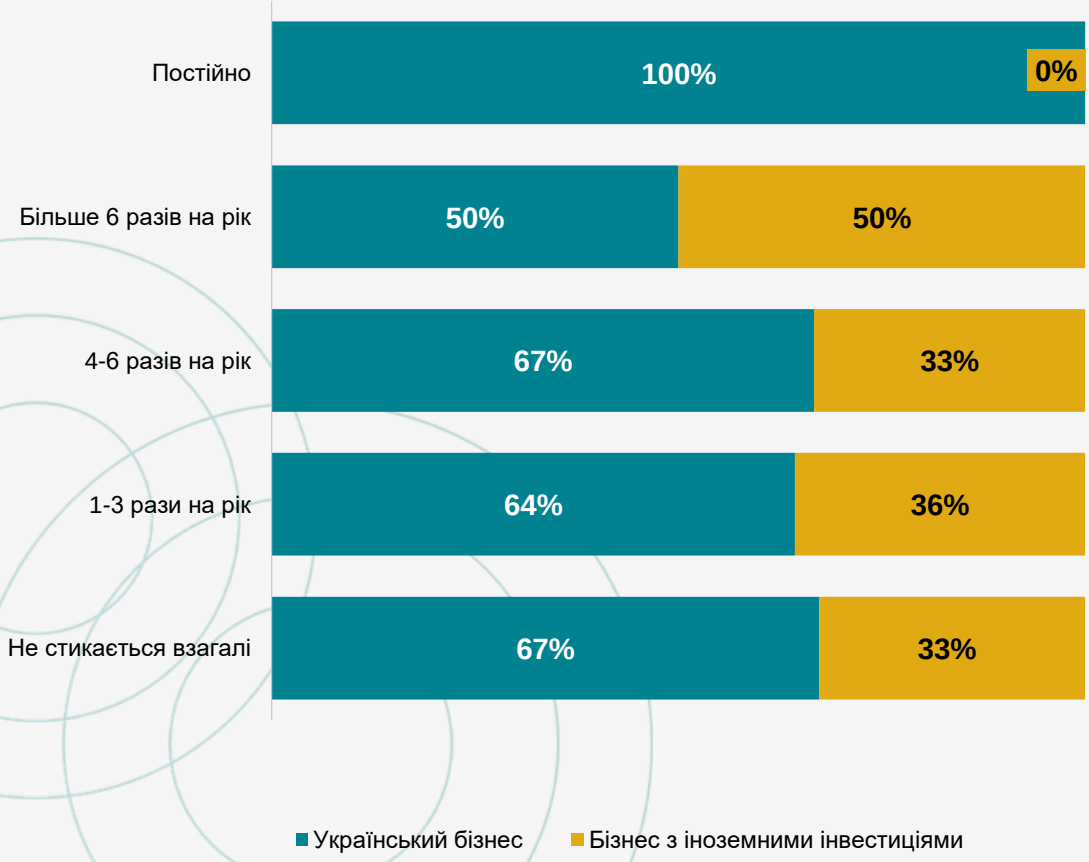
Особливості взаємодії з правоохоронними органами

Факт того, що 46 % респондентів не стикалися з активними діями правоохоронних органів виглядає аномалією, але лише на перший погляд. Треба врахувати, що процес відбору респондентів є добровільним, залежить від ініціативи і бажання витратити час на відповіді, тому природньо, що бізнес із «сірими» чи кримінальними схемами до нашої вибірки не потрапив.

Ще один вагомий чинник спостерігається на діаграмі вище – чим конкретніша відповідь, тим менша частка серед них надана компаніями, що не мають власної СБ. Так, відповіді «4-6 разів» та «більше 6 разів» були надані на 89 % і 100 % компаніями, в яких є власна СБ.

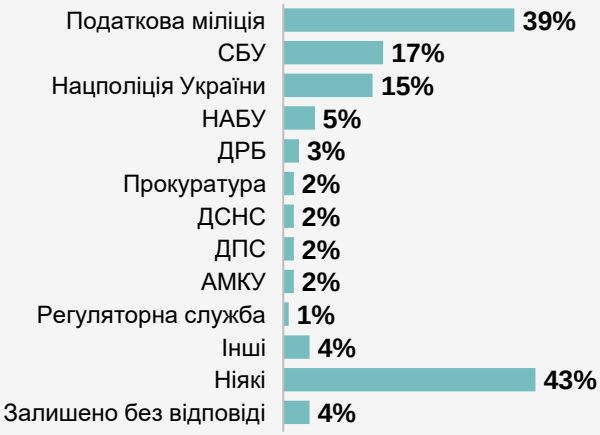
Проте, навіть бізнес, що дбає про власну безпеку і вважає себе «білим», відчув цього року активні дії правоохоронних органів у 54 % випадків. 6 % компаній, які повідомили про постійний тиск, є компаніями з українським капіталом, в усіх інших варіантах структура відповідей респондентів була майже аналогічною до Портрету респондента.

Сприйняття активності дій правоохоронних органів компаніями з різним походженням капіталу

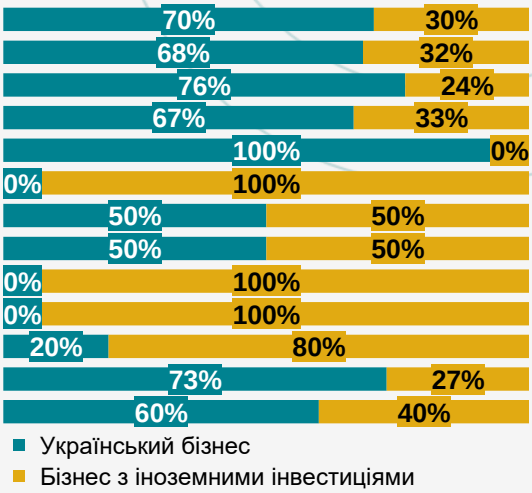


Оцінка «агресивності» державних структур до бізнесу

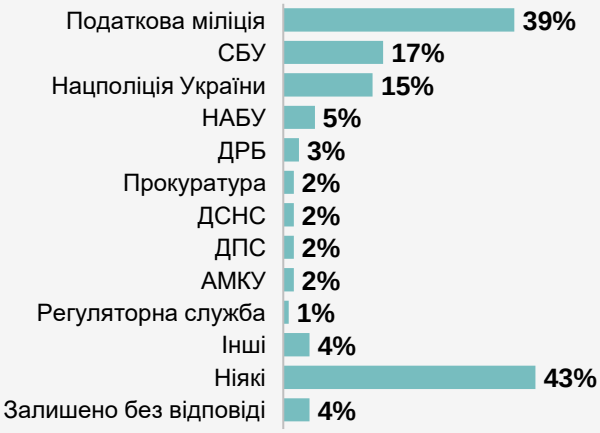
Всі компанії



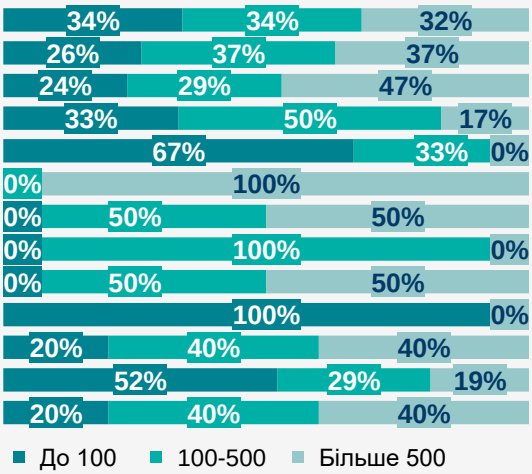
За походженням капіталу



Всі компанії



За розміром компанії (кількість співробітників)

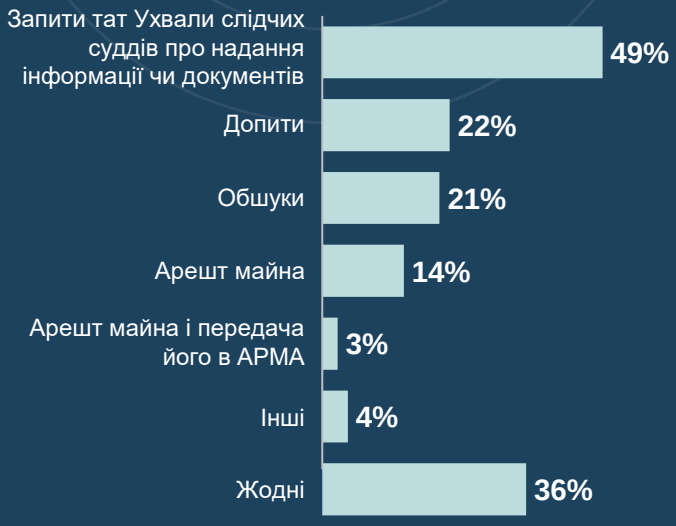


Незважаючи на те, що реформа фіскальних органів та органів фінансових розслідувань триває, бізнес добре запам'ятав назву «Податкова міліція», як найактивнішого державного органу, тому ми використали в запитанні цю застарілу назву. Виявилося, що агресивність податкової міліції і далі відчуває на собі, як мінімум кожна третя компанія. Податкова (39 %) удвічі лідирує з відривом від наступної структури, яка також є в стадії ліквідації – СБУ, що у 17 % випадків завдає тиску на бізнес. Потрапляння на перші два рядки зазначених державних структур ми вважаємо цілком серйозною аномалією.

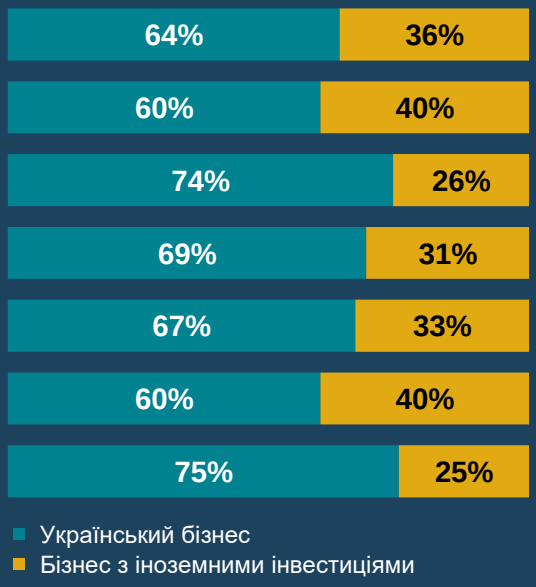
Бізнес розуміє, що за тривалий час реформування вони вже звикли виконувати свою роботу за принципом «кожен день, як останній», тому статистика дає змогу підтвердити ці висновки. Про відсутність тиску на бізнес повідомили 43 % респондентів, що адекватно корелюється з відповідями на інше, аналогічне запитання. Як ми раніше зазначали – 46 % респондентів відповіли, що не стикалися з активними діями правоохоронних органів. Якщо додати ще 4 % респондентів, які не визначились із відповіддю, то згадані вибірки майже збігаються.

Характер тиску на бізнес з боку державних структур (в розрізі різних типів бізнесу)

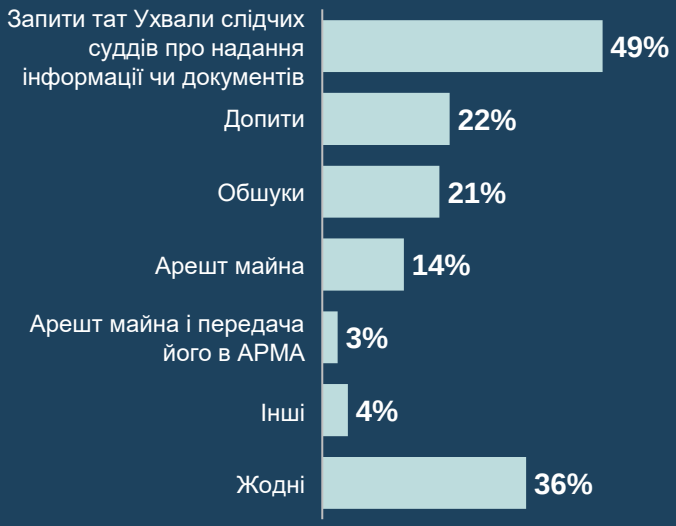
Всі компанії



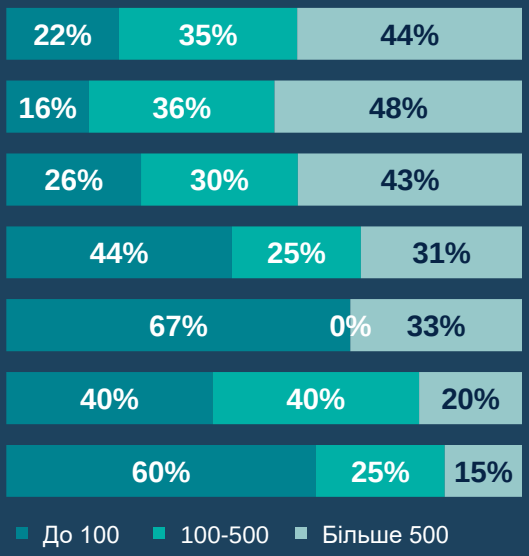
За походженням капіталу



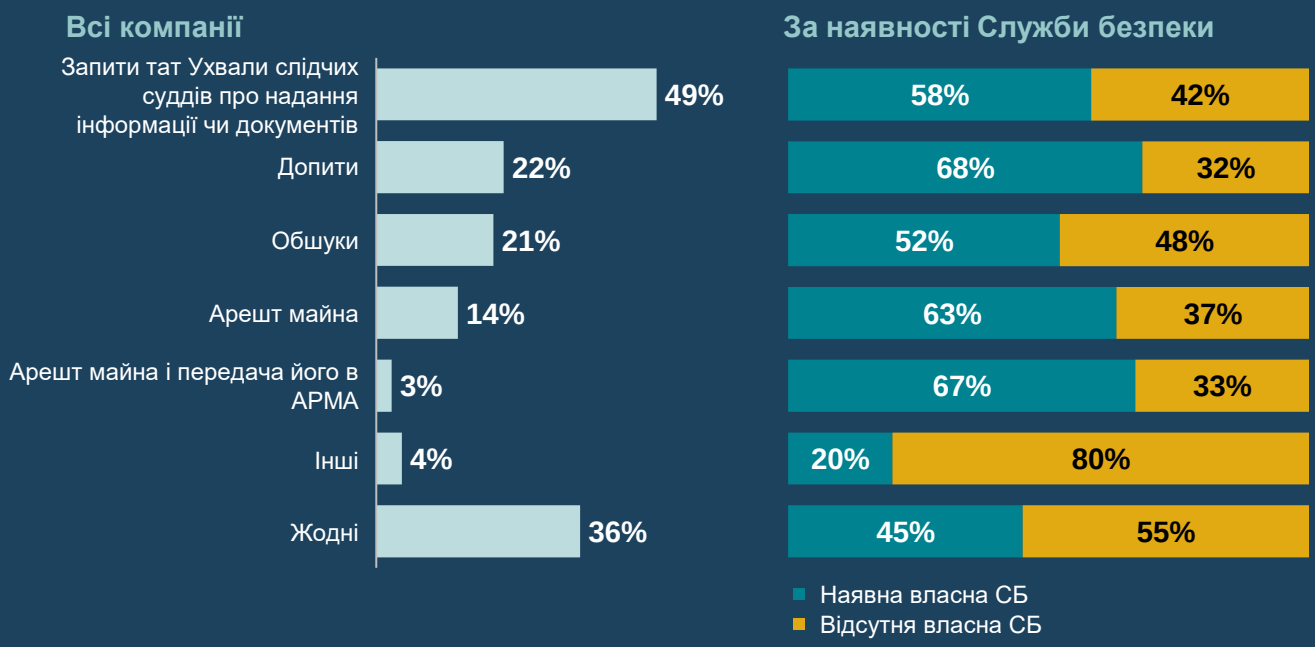
Всі компанії



За розміром компанії (кількість співробітників)



Характер тиску на бізнес з боку державних структур (в розрізі різних типів бізнесу)



Найчастіше бізнес сприймає, як агресивні дії правоохоронних органів, запити та ухвали слідчих суддів про надання доступу до інформації чи документів – з цим стикаються 49 % компаній. Цікаво, що 36 % респондентів відповіли, що не вважають агресивними жодні дії правоохоронних органів. Проте, чим менша за розміром компанія, тим частіше вона дотримується такої думки: 60 % відповідей надали найменші компанії, а 15 % - найбільші. Якщо зіставити ці дані з Портретом респондента, то зазначена тенденція може бути пояснена глибиною обізнаності: найменшим компаніям, 71,4 % яких не мають власної СБ, складніше відповісти на конкретне запитання, який саме різновид дій правоохоронних органів вони вважають найчастішим, та яка ступінь агресивності кожного виду цих дій, тому вони чесно відповіли «жодні» (читай – «не відомо»).

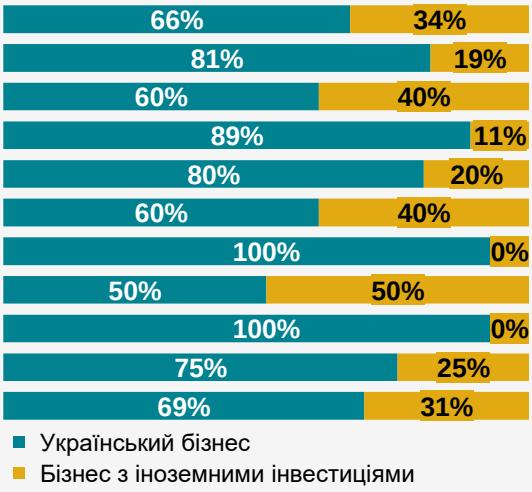
Більші за розміром компанії менш схильні так відповідати, тому що мають більшу обізнаність, ведуть облік і звертають увагу на поведінку та характер дій правоохоронних органів.

Більш детальний аналіз вказує, що до компаній без власної служби безпеки рідше надходять запити та ухвали слідчих суддів про надання доступу до інформації чи документів (42 %), рідше допити (32 %), обшуки (48 %) та рідше здійснюється арешт майна (37 %). Це складно було б пояснити, але попередній етап аналізу дав змогу виявити, що до найбільших за розміром компаній ці ж самі дії правоохоронних органів застосовуються навпаки частіше: запити та ухвали – 44 %, допити – 48 %, обшуки – 43 %. А з аналізу Портрету респондента нам відомо, що саме 85,7 % найбільших за розміром компаній мають власні СБ, тому саме їхні відповіді більше вплинули на формування пропорцій розподілу.

Погляд бізнесу на претензії з боку правоохоронних органів (в розрізі різних типів бізнесу)

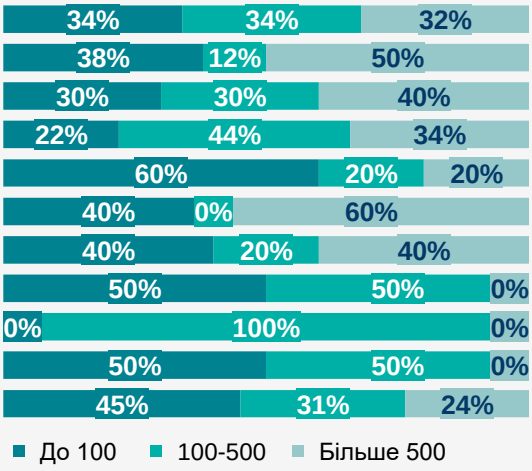
Всі компанії

За походженням капіталу



Всі компанії

За розміром компанії (кількість співробітників)



Цілком закономірно, що респонденти визначають найпоширенішими претензіями з боку правоохоронних органів - ухилення від сплати податків (42 %), поза як, податкова міліція з пропорційним відривом лідирує в рейтингу найбільш агресивних держструктур (39 %). Цю категорію тиску зазначає, як бізнес з українським, так і бізнес з іноземним капіталом (66 % та 34 % відповідно). Але під час порівняння з портретом респондента таких категорій, як «Корупційні правопорушення» (81,3 %), «Присвоєння чи розтрата майна» (88,9 %), «Фінансування тероризму» (80 %), «Злочини проти національної безпеки» (100 %) та «СТЗ» (100 %) ми маємо змогу констатувати, що український бізнес значно інтенсивніше відреагував на це запитання. З огляду на те, що здебільшого зазначені претензії стосуються компетенції СБУ, ми розуміємо, чому другою за агресивністю бізнес обрав саме цю структуру. І ще одне спостереження не на користь СБУ – 60 % респондентів, що відчули претензії щодо «Фінансування тероризму», є найменшими за розміром компаніями. За статистикою ЄРДР, 9 із 10 таких кримінальних проваджень закриваються.

АНАЛІЗ БЕЗПЕКИ ВЕДЕННЯ БІЗНЕСУ В УКРАЇНІ

Сергій ПОГРЕБНОЙ

Партнер Sayenko Kharenko
Голова Опікунської Ради АПКБУ
Віцепрезидент ASIS Ukraine

Вочевидь, український бізнес чекає «гаряча» зима 2021-2022. Кількість подій, що прямо стосуються бізнесу, величезна за цей період. Початок роботи БЕБ, судова реформа, закон 5600, закон «про олігархів», реформа СБУ, безперервна реформа в Національній поліції, ТСК у справі «вагнерівців», замах на Шефіра, податкова амністія, санкції, що продовжуються, під які вже почали потрапляти іноземні активи в РФ і ще багато іншого, що трапиться до виходу цієї статті. Чесно кажучи, я давно не пам'ятаю таку насичену різними законодавчими та політичними подіями осінь. На тлі всього, безліч корупційних скандалів, перші гучні процеси, що можна вважати «політичними», оскільки в них виявилися учасниками політики високого рангу.

Природно, що через реформу економічного блоку правоохоронних органів, тиск на бізнес різко посилився. Він проявляється у відкриттях фальсифікованих кримінальних проваджень щодо комерційних структур, про які вони ніколи не чули, і, зазвичай, не брали участі, що призвело до необґрунтованих обшуків, вилучення матеріальних цінностей та активів, призупинення діяльності підприємств. Здебільшого, всі ці справи успішно вирішувалися на користь бізнесу, але доводилося нести, як прямі витрати на адвокатів, комунікацію, простій виробництв і офісів у дні обшуків, так і непрямі – відволікання співробітників на обшуки, допити, підготовку матеріалів на запитувану інформацію, втрату репутації та потенційних замовлень.

Іноді складається враження, що держава веде проти бізнесу неоголошену війну, і використовує всю міць своїх правоохоронних, контролюючих та спеціальних органів. Скільки про це не писали, не створювали ТСК, Офісу із захисту бізнесу при МВС, Національні Офіси з інвестицій, скільки не проводилося Форумів із захисту бізнесу та круглих столів, але бізнес, як і раніше, залишається ціллю для корумпованих силовиків та чиновників, рейдерів, нечесних конкурентів та окремих політиків, які перерозподіляють свій вплив не тільки на «тіньовий ринок», а й цілком на легальні галузі..

Аби зрозуміти, в які кризові ситуації потрапляє бізнес в Україні, Sayenko Kharenko за підтримки SK Security, АПКБУ та ASIS Ukraine, більшості бізнес-спільнот, бізнес-клубів та ділових асоціацій, у партнерстві з PwC, проводять друге опитування «Оцінка безпеки ведення бізнесу в Україні». ТОП-5 кризових ситуацій, з якими стикається бізнес, не змінилися в порівнянні з минулим роком. Це незаконні дії державних органів – 43 %, незаконні конкурентні дії – 42 %, незаконні дії правоохоронних органів – 33 %, медіа-атаки - 25 %, напади на активи та грабежі транспорту, врожаю та підприємств - 23 %. Дивно, що ніхто з учасників опитування не бачить корупцію кризовою ситуацією. Судячи з усього, тотальна боротьба з корупцією в суспільстві призвела до протилежного результату, бізнес просто звик до неї, як до «неминучого зла».

Сильно зросли в порівнянні з минулим роком і цифри у корпоративних конфліктах і рейдерстві, 21 % та 13 % відповідно, у 2020 році ці цифри були набагато меншими – 12 % та 9 %. Приємно здивували цифри щодо кібератак. Якщо минулого року було 33 %, то цього – 22 %. Судячи з усього, бізнес почав приділяти особливу увагу цьому напрямку.

Всі ці цифри явно показують, що кількість ризиків у країні для бізнесу, на жаль, не зменшується, а рівень захисту або залишається на тому ж рівні, або знижується.

Як показує досвід, у будь-якій із цих ситуацій, бізнес часто виявляється віч-на-віч або з державними структурами, або конкурентами чи рейдерами та криміналом. Бізнес зміг згуртуватися в асоціації, клуби та спільноти, але всі ці структури, зазвичай, виконують лише дві ролі: GR та PR, а вирішення цих ситуацій лежить також ще у сфері адвокатури, корпоративної безпеки, силового захисту, кібербезпеки. У багатьох бізнесах є внутрішні служби безпеки, але вони або не володіють необхідним досвідом, або у них бракує синергетичних можливостей та фінансів для моментального захисту бізнесу. Та і впровадження на ринку стандартів корпоративної безпеки йде вкрай повільно, тож більшість внутрішніх СБ не встигають за тенденціями розвитку, дослідженнями та стандартами світової приватної безпеки.

Навіть якщо бізнесу і вдається тим чи іншим способом вирішити загрозу і прибрати ризики, цей досвід залишається всередині бізнесу і втрачається для бізнес-спільноти.

Тепер уявіть, що в Україні вже створено сервіс захисту бізнесу, що накопичує досвід, аналізує його, зберігає для всієї спільноти і готовий застосувати в будь-який момент часу і в будь-якій точці земної кулі. Що в ідеалі хоче бізнесмен? Він хоче займатися улюбленою справою, розвивати бізнес, заходити на нові ринки, створювати нові проєкти та продукти, будувати заводи, заробляти гроші і ще багато чого. І, зрештою, реалізовувати свої мрії, в тому числі і про польоти в космос, як це вже вдалося американським та деяким українським бізнесменам. На певному етапі свого розвитку бізнесмен хоче займатися благодійністю, підтримувати мистецтво, розвивати систему освіти, змінювати світ та вкладати у майбутнє країни, зокрема, підтримуючи молодь у її прагненнях.

А що насправді? Більшість бізнесменів країни, як мінімум, прямо стикається з усіма переліченими вище ризиками, конфліктами та кризовими ситуаціями, і змушена займатися ними, прямо втрачаючи свій час, нерви, гроші та можливості. Чи можна повністю уникнути участі у вирішенні ризиків і загроз своїй безпеці? Ні, цілком не можна, але можна максимально дистанціюватися від них та передати управління у професійні руки. Єдине запитання залишається тоді – в які? І це, напевно, найважливіше запитання довіри, життя і смерті свого бізнесу.

Якою би хотів бачити свою безпеку будь-який практичний бізнесмен в Україні? Ідеальна ситуація – коли він навіть не дізнавався про те, що щось загрожує його бізнесу, а всі ризики виявлялися і вирішувалися далеко до кордонів бізнесу. А якщо вони й наступили, то автоматично спрацьовувала би система безпеки і виявляла, керувала та мінімізувала такі ризики, а ще краще знижувала їх на максимально можливий відсоток. Найідеальніша ситуація – коли бізнес дізнавався про такі загрози чи ризики набагато раніше, на стадії їхнього планування чи зародження. Звучить фантастично, і здебільшого викликає усмішку, правда? Але бізнес прямо говорить про те, що для них це був би ідеальний варіант, без сліпих зон ризику або непередбачуваних ситуацій взагалі. Чи можливо досягти в Україні такого рівня безпеки для бізнесу чи ні?

Десь вже створено такий сервіс захисту бізнесу, з ситуаційними центрами, зокрема й мобільними, обладнанні найсучаснішими засобами зв'язку, і в тому числі, дрони. Розгорнутий аналітичний центр, який у режимі реального часу може проаналізувати будь-який конфлікт та передати ці дані для ухвалення правильного рішення.

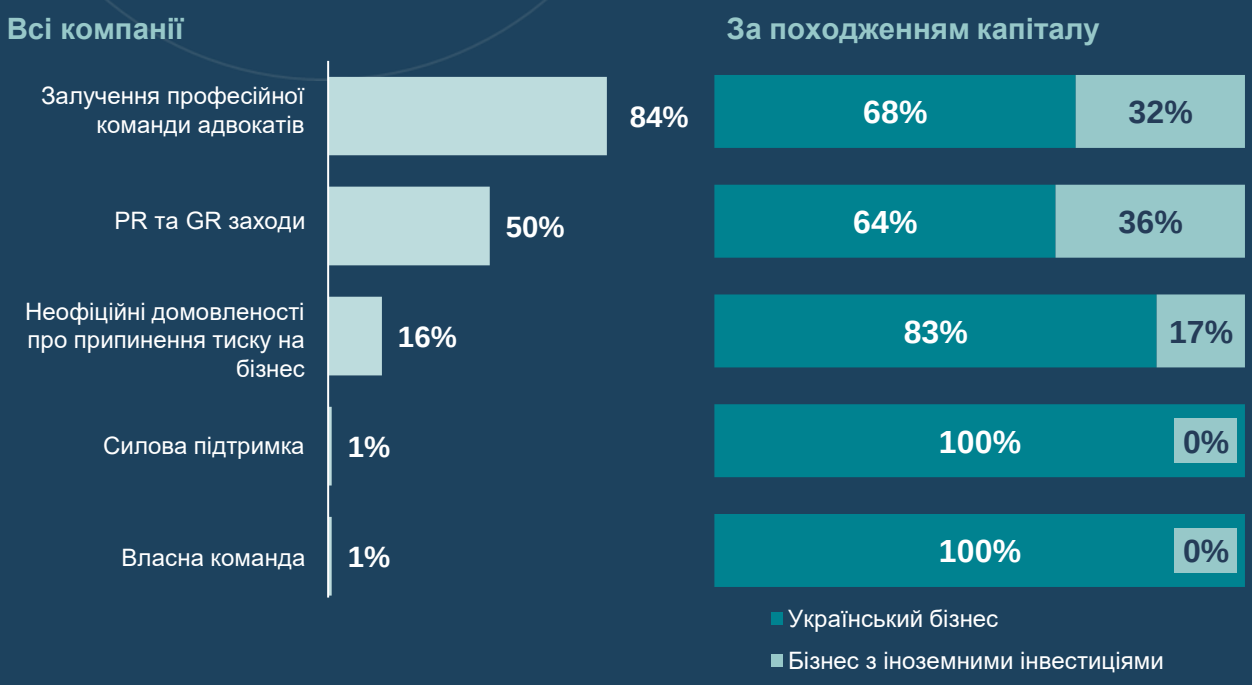
Є тактичні групи, до яких входять силові підрозділи, адвокати та журналісти, які можуть виїхати, вилетіти та припливти до будь-якої точки України і зробити це у найкоротший час. Де SOC кібербезпеки може підключитися до ваших мереж будь-якої секунди і почати захищати їх від кібератаки. Ситуаційний центр взаємодіє з усіма такими центрами державних структур і готовий залучити їх для захисту вашого бізнесу залежно від ситуації, а під кожну ризик-ситуацію створюється окрема відеокімната для вирішення ризику в режимі реального часу. А якщо піти ще далі, і уявити, що створений прогностичний комплекс, який, як оракул, передбачає ваші ризики на місяць, рік чи встановлене найближче майбутнє? А уявляєте, якщо до такого сервісу безпеки підключено 100 або 200, або 500 бізнесів? І отже, просто сервіс з безпеки бізнесу поступово перетворюється на клуб з безпеки бізнесу, з оборотом, наприклад, від двох до семи мільйонів євро на рік, або, навіть, більше. А ви вкладаєте у свою безпеку хоча б 250 тисяч євро чи один мільйон євро на рік? Думаю, що ні. А ось у такому клубі у разі загрози вашому бізнесу можна було б отримати професійний захист та підтримку на всю вартість клубу, а наскільки вона була більшою, залежало би від самих учасників клубу, їхніх внесків та поставлених завдань.

Багато хто, прочитавши цей абзац, скаже, що це просто фантастика або проєкт неймовірно далекого майбутнього. Але ні, такий прототип вже є в Україні, і зараз він працює з першими учасниками, і зветься сервіс із захисту бізнесу «Фортеця». І вирішує цілком реальні завдання у повсякденній діяльності бізнесменів та їхніх підприємств. Скажу більше, прототип уже успішно пройшов тестування у кількох кризових ситуаціях, зокрема, захищаючи клієнта від прямого нападу та загрози вбивства. «Фортеця» працює поки що лише по 11 із кризових ситуаціях, перекриваючи фактично 85 % найпоширеніших загроз та ризиків. Проте, ми сподіваємося, що зможемо охопити весь спектр загроз та ризиків до 95 % найближчим часом.

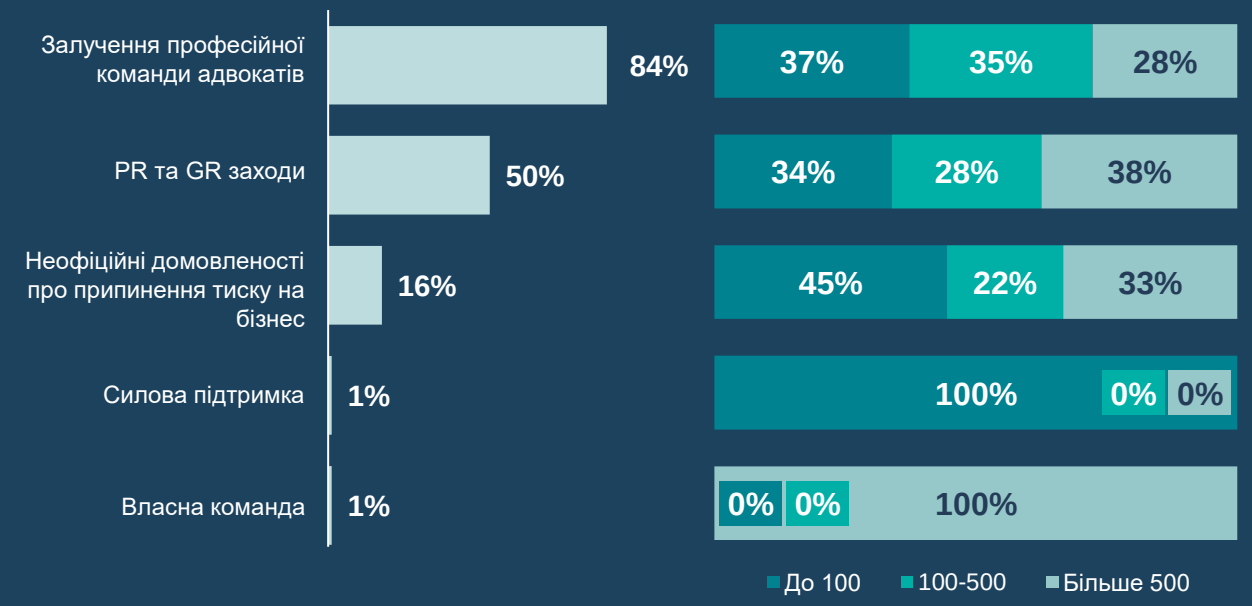
«За безпеку необхідно платити, а за її відсутність – розплачуватися». Знаменита фраза Уїнстона Черчілля багато в чому визначає наш сучасний світ, який за останні кілька років неймовірно змінився і породив непередбачувану кількість турбулентностей, як у звичайному житті, так і в бізнесі в Україні і у всьому світі. Можна звичайно самому проходити ці турбулентності і відчувати при цьому величезне навантаження на бізнес та його власників, а можна спробувати впорядкувати та структурувати своє майбутнє та розвиток у безпечнішому стані разом із «Фортецею». Рішення, як завжди, за вами – власниками бізнесу, його залишилося тільки прийняти.

Використання компаніями способів захисту від агресивних дій правоохоронних органів

Оцінка ефективності способів для захисту від агресивних дій правоохоронних органів в залежності від походження капіталу компаній

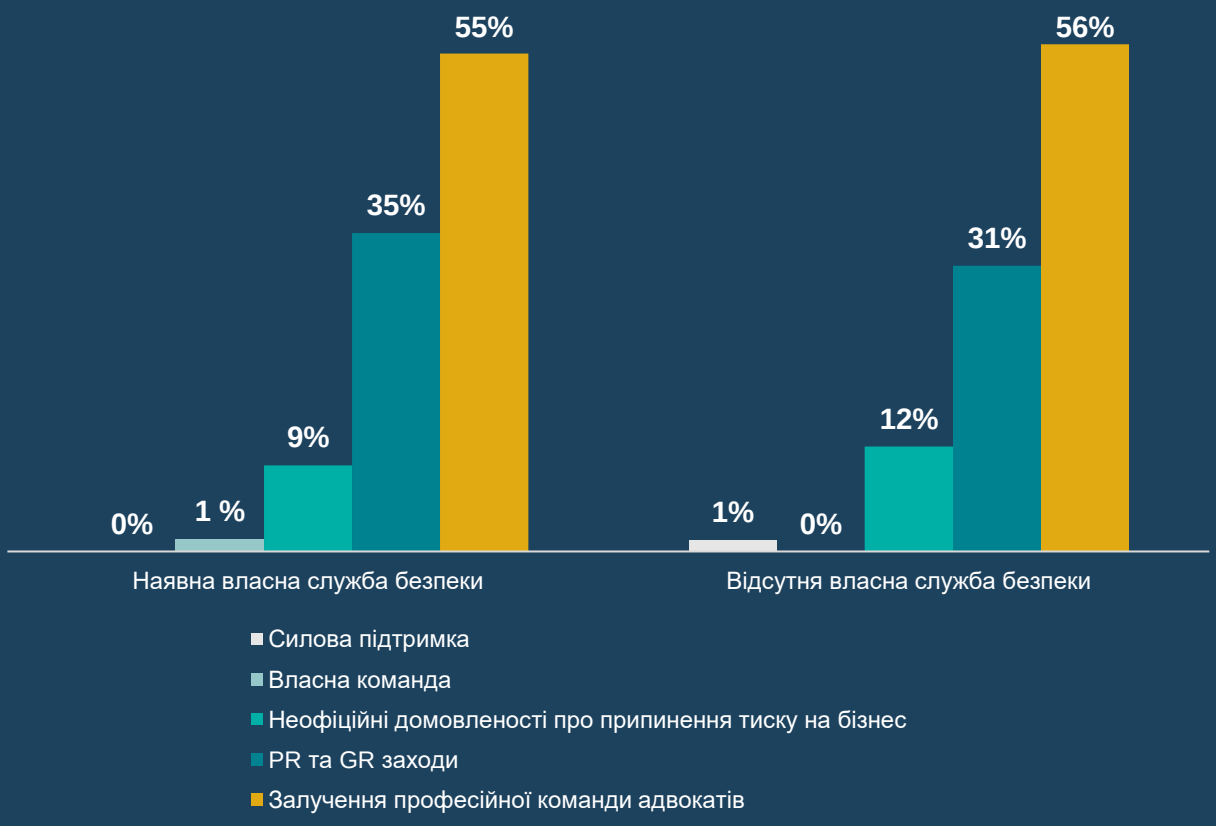


Оцінка ефективності способів для захисту від агресивних дій правоохоронних органів в залежності від розміру компанії



Використання компаніями способів захисту від агресивних дій правоохоронних органів

Оцінка ефективності способів для захисту від агресивних дій правоохоронних органів в залежності від наявності власної Служби безпеки



На перший погляд, статистика на графіках цього розділу може викликати гордість за країну, в якій лише 11 % бізнесу готові вдаватися до неофіційних домовленостей про припинення тиску на бізнес, а здебільшого воліють залучати професійну команду адвокатів (55 %) та застосовувати PR та GR заходи (33 %). Але такий висновок може викликати відчуття «конфлікту з реальністю», тому ми ще раз нагадуємо, що процес відбору респондентів є добровільним, певною мірою залежить від ініціативи і бажання витратити час на відповіді, тому бізнес із «сірими» чи кримінальними схемами до нашої вибірки не потрапив.

Проте деякі тенденції простежуються чітко: найменші українські компанії рідше залучають адвокатів (на 2 % менше, ніж компанії з іноземними інвестиціями), менше вживають PR та GR заходи (на 7 % менше, ніж компанії з іноземними інвестиціями) та частіше готові на неофіційні домовленості про припинення тиску на свій бізнес (на 7 % більше, ніж компанії з іноземними інвестиціями).

Різниця в оцінюванні найбільш ефективних способів захисту майже не залежить від наявності власної СБ.

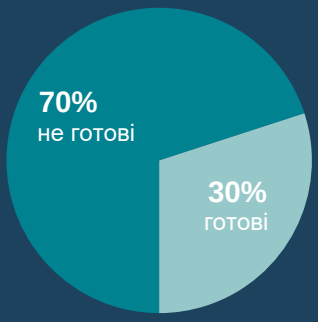
Готовність компаній до можливих військових дій на території України

Про готовність бізнесу до війни, не дивлячись на багаторічний військовий конфлікт, статистичних даних обмаль. Тому в нашому дослідженні 2021 року розпочато вимірювання готовності та основних підходів бізнесу з підготовки до можливих військових дій та убезпечення від збитків і подолання наслідків. Готується до війни на території України 30 % респондентів. Український бізнес готується на 13 % рідше, ніж бізнес з іноземними інвестиціями, 39 % представників якого це підтвердили.

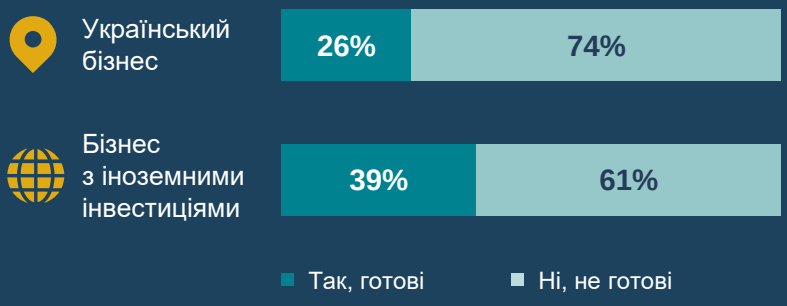
Ще більша різниця (19 %) між найменшими та найбільшими компаніями нашої вибірки. Ми віримо, що сприйняття військової загрози підприємцями, які ведуть бізнес на території України, приблизно однакове, а вказані статистичні відмінності сформовані більшим впливом комплаєнсу, якого частіше дотримуються великі компанії та компанії з іноземним капіталом.

Наявність власної СБ у компаніях також впливає на готовність бізнесу до можливих військових дій: там, де вони є, показник 37 %, там де їх немає – на 13 % менше.

Готовність компаній до можливих військових дій

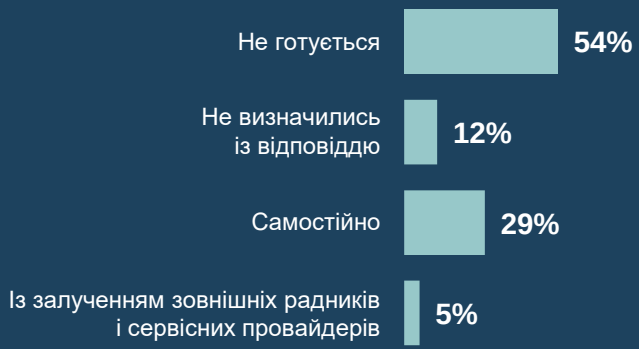


Сприйняття компаніями потреби у підготовці до можливих військових дій

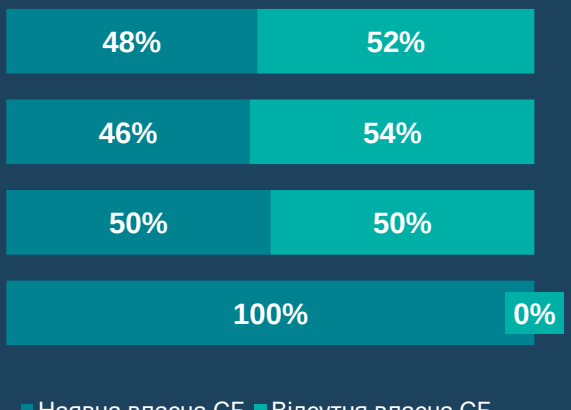


Як бізнес готується до можливих військових дій на території України

Всі компанії



За наявності Служби безпеки



Як змінюються підходи до підготовки серед компаній зі збільшенням їх розміру

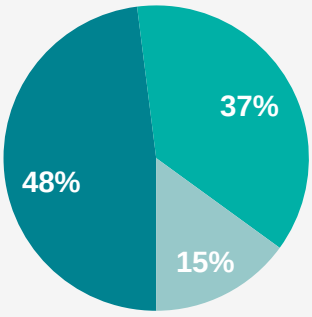
Залежно від розміру компанії (кількість співробітників)

Запитання про якість підготовки до війни виявило, що серед компаній, які визнали себе неготовими до можливих військових дій, є 12 % респондентів, що не визначились із відповіддю. Разом із респондентами, які обрали відповідь «Не готуються», їх 66 %. Це майже збігається із кількістю відповідей «Ні» на більш просте запитання попереднього етапу «Чи готується Ваш бізнес до війни на території України?», яких 70 %.

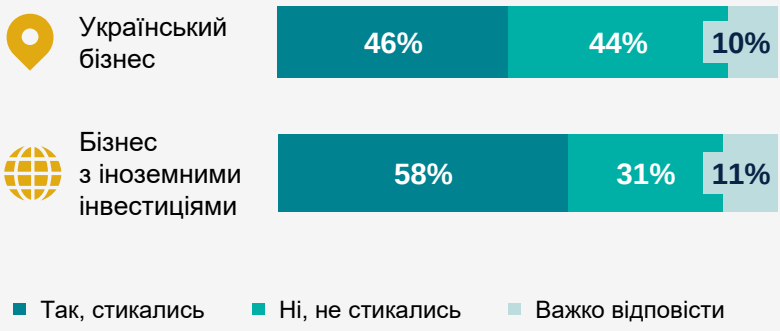
Окрема вибірка серед компаній, які готуються до можливих військових дій на території України, свідчить, що така підготовка здійснюється ними переважно самотужки (84 %). Залучення зовнішніх радників та сервісних провайдерів здійснюється частіше найбільшими і середніми компаніями (50 % і 33 % відповідно), а серед категорії найменших компаній про це вказали лише 17 %. Цілком очікувано, що всі компанії, які залучають зовнішніх радників та сервісних провайдерів для підготовки до можливих військових дій на території України, мають власні СБ

Економічні злочини та шахрайство в Україні

Всі компанії



За походженням капіталу



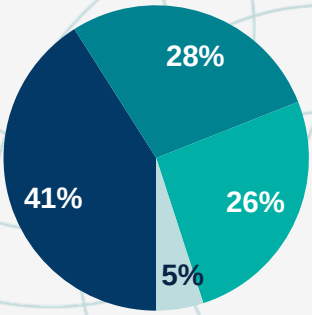
За результатами дослідження, 48 % респондентів постраждали від шахрайства, корупції або інших видів економічних злочинів у 2020 році. Цей показник не змінився, порівнюючи з результатами дослідження GECS, проведеного PwC у 2018 році в Україні.

Більша частина представників бізнесу з іноземними інвестиціями (58 %) стикалися із шахрайством, корупцією або іншими видами економічних злочинів у 2020 році, порівнюючи з 46 % українського бізнесу.

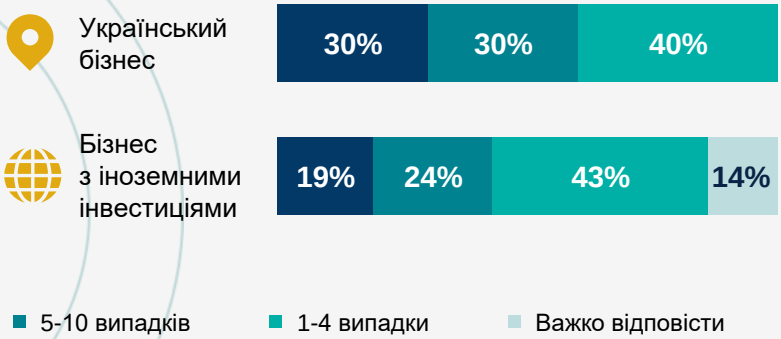
Більшість респондентів (69%) в Україні постраждали, як мінімум, від п'яти випадків шахрайства, корупції або інших економічних злочинів у 2020 році. Походження капіталу компанії впливає на кількість випадків економічних злочинів та шахрайства.

Зокрема, представники українського бізнесу констатують більшу вразливість до шахрайства у порівнянні з компаніями з іноземними інвестиціями: 60 % українських компаній стикались, в середньому, з мінімум п'ятьма випадками шахрайства, порівнюючи з 43 % компаній з іноземними інвестиціями.

Всі компанії



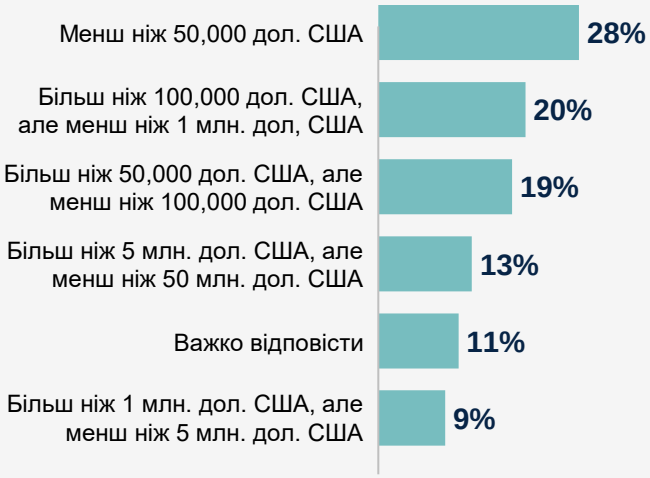
Як часто компанії стикаються з економічними злочинами та шахрайством в Україні



Оцінка наслідків економічних злочинів та шахрайства

Вартість економічних злочинів та шахрайства

Всі компанії



За походженням капіталу

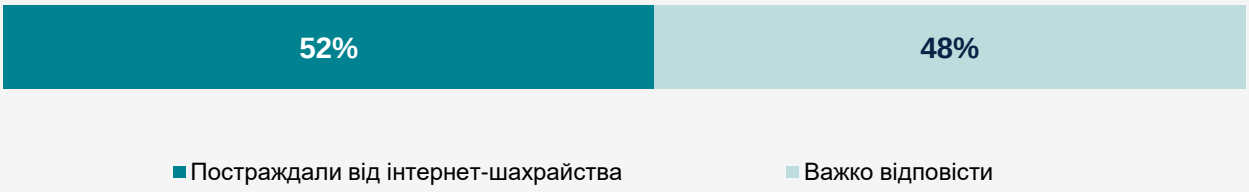
47 % компаній стикаються із шахрайством, корупцією або іншими економічними злочинами в Україні, що оцінюються в менш ніж 100,000 дол. США. Цей показник майже не змінився (46 %) у порівнянні з результатами дослідження GECS, проведеного PwC у 2018 році.

Для українського бізнесу вартість шахрайства зазвичай нижча, аніж для бізнесу з іноземними інвестиціями, та оцінюється менш ніж в 50,000 дол. США у 40 % випадків.

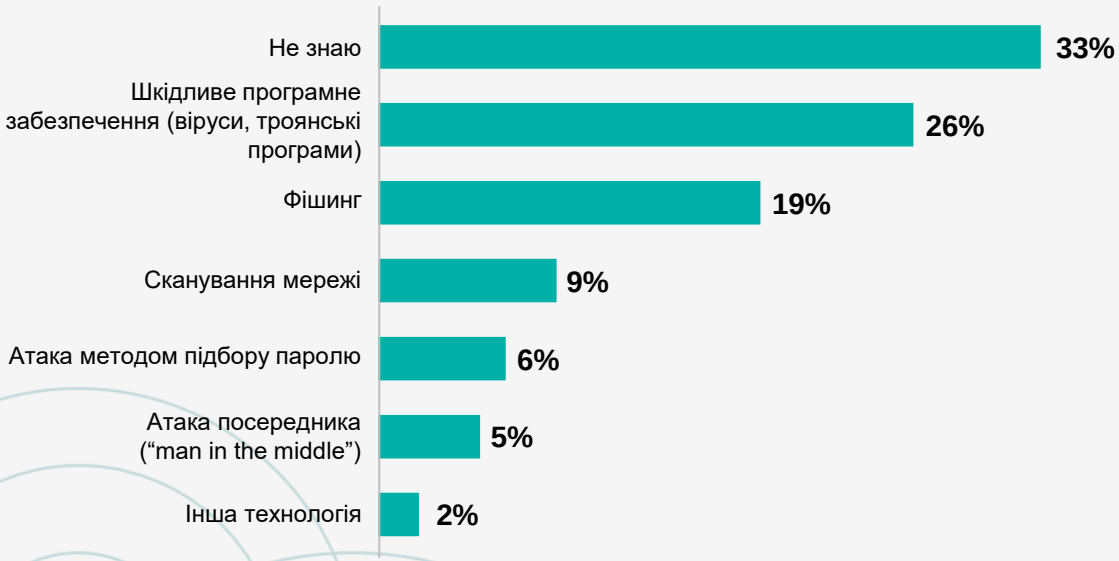
Водночас, незважаючи на те, що компанії з іноземними інвестиціями рідше стикаються з випадками економічних злочинів та шахрайства, проте наслідки таких випадків дорожчі та оцінюються більше ніж у 50,000 дол. США, але менше ніж у 100,000 дол. США (33 % випадків).

Інтернет-шахрайство та кіберзлочини

Рівень вразливості компаній до інтернет-шахрайства та кіберзлочинів



Основні види інтернет-шахрайства, з якими стикаються компаній найчастіше



Понад 50 % респондентів, які постраждали від шахрайства у 2020 році, як з українського бізнесу, так і бізнесу з іноземними інвестиціями, також мали справу з кібератаками та інтернет-шахрайством.

Решта респондентів (48 %) не володіють інформацією щодо наявних кіберзагроз для їхніх компаній. Можливо, вони стикаються з такими проблемами, проте через відсутність достатнього розуміння аспектів інформаційної безпеки, часто не ідентифікують їх.

Серед усіх респондентів, які постраждали від інтернет-шахрайства, третина (33 %) не змогла ідентифікувати із застосуванням якої технології було здійснено кібератаку в їхній компанії.

Однак, очевидним є те, що основними видами інтернет-шахрайства у 2020 році є фішинг та шкідливе програмне забезпечення (віруси, троянські програми та інші).

Види економічних злочинів та шахрайства

Види економічних злочинів та шахрайства, з якими найчастіше стикаються компанії

Незаконне привласнення майна	28 %
Шахрайство у сфері закупівель	20 %
Недобросовісна конкуренція	17 %
Хабарництво та корупція	15 %
Кіберзлочини	4 %
Інсайдерська торгівля	4 %
Відмивання коштів та санкції	4 %
Фальсифікація фінзвітності	2 %
Шахрайство споживачів	2 %
Шахрайство у сфері оподаткування	2 %
Важко відповісти	2 %

Найбільш суттєві економічні злочини та шахрайство, з якими стикалися компанії у 2020 році, є такі: незаконне привласнення майна (28 %), шахрайство у сфері закупівель (20 %), недобросовісна конкуренція / порушення антимонопольного законодавства (17 %), хабарництво та корупція (15 %).

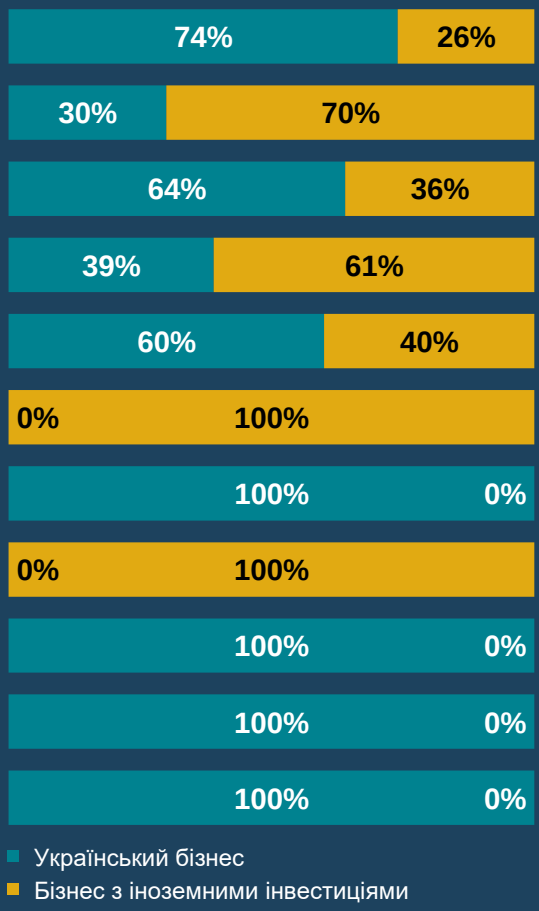
Серед українського бізнесу найбільш суттєвим економічним злочином вважається шахрайство у сфері закупівель (27 %), а представники компаній з іноземним капіталом оцінюють незаконне привласнення майна (33 %) як економічний злочин, що найбільш суттєво вплинув на діяльність компаній у 2020 році.

Прогнози на першу половину 2022 року

Прогнози щодо найбільш суттєвих економічних злочинів та шахрайства

Всі компанії

За походженням капіталу



На думку респондентів, найбільш суттєвим шахрайством, з погляду фінансових збитків, у першій половині 2022 року можуть бути шахрайство у сфері закупівель (20 %), недобросовісна конкуренція / порушення антимонопольного законодавства (18 %), хабарництво та корупція (15 %), незаконне привласнення майна (15 %) та кіберзлочини (13 %).

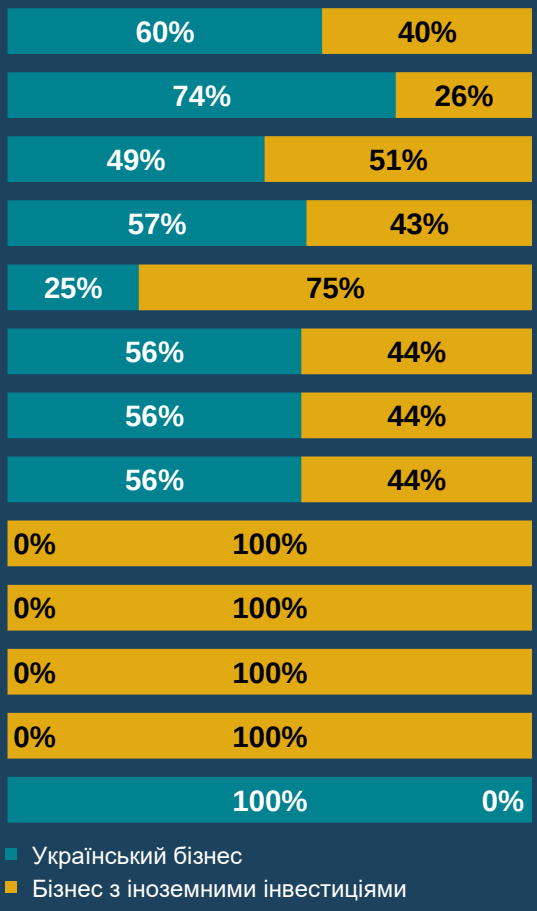
Представники українського бізнесу вважають, що великих збитків компаніям можуть принести шахрайство у сфері закупівель (28 %), хабарництво та корупція (18 %) та кіберзлочини (15 %).

Серед бізнесу з іноземними інвестиціями найбільш суттєвими видами шахрайства у 2022 році вважають недобросовісну конкуренцію / порушення антимонопольного законодавства (28 %), незаконне привласнення майна (19 %) та порушення прав інтелектуальної власності (14 %).

Як компанії виявляють економічні злочини та шахрайство в Україні

Всі компанії

За походженням капіталу



Основними інструментами виявлення шахрайства в компаніях є: корпоративна безпека, включно з IT та фізичною безпекою (19 %), вдосконалений аналіз даних (19 %) та моніторинг підозрілих дій (19 %).

Серед українського бізнесу популярними інструментами вважаються аналіз даних (25 %) та корпоративна безпека, включно з IT та фізичною безпекою (21 %). Представники бізнесу з іноземними інвестиціями констатують, що моніторинг підозрілих дій (19 %) та корпоративна безпека, включно з IT та фізичною безпекою (14 %), у 2020 році були найдієвішими інструментами виявлення суттєвих випадків шахрайства, корупції або інших економічних злочинів у компаніях.

Цікаво, що, згідно з результатами цього дослідження, внутрішній аудит не сприймається компаніями як потенційний інструмент виявлення економічних злочинів та шахрайства. Водночас, згідно з результатами GECS 2018, процедури внутрішнього аудиту вважались одним із основних інструментів корпоративного контролю у виявленні таких порушень, після корпоративної безпеки та моніторингу підозрілих дій.

ФОРЕНЗІК ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ШАХРАЙСТВУ

Ірина ЛУБСЬКА

Менеджер практики Форензік,
PwC в Україні

Сьогодні наше життя важко уявити без мобільного телефону або ноутбуку, адже все більше і більше інформації переходить у цифровий формат: контракти з постачальниками, бази даних клієнтів, реєстр транзакцій листування переписка у месенджерах з бізнес-партнерами та багато іншого.

За підрахунками Seagate та IDC, сфера даних у світі до 2025 року зросте більше ніж у 5 разів та складе 175 зеттабайт (один зеттабайт дорівнює 1 млрд терабайт). Згідно сайту Statista.com, кількість повідомлень електронної пошти також невпинно зростає. Якщо у 2018 році їх кількість складала близько 281 млрд, то до 2025 року вона виросте до 376 млрд листів в день.

Вражаючі цифри… Але такий розвиток цифрової інформації має і зворотну сторону медалі – окрім ризиків, що пов'язані із кібер-загрозами, великі обсяги електронної інформації створюють труднощі у протидії шахрайству, зокрема, в контексті проведення розслідувань – адже виникають ситуації, коли «серед копиці сіна необхідно знайти голку» у вигляді тих чи інших електронних даних.

Згідно дослідження PwC щодо економічних злочинів та шахрайства проведеного в Україні у 2020 році, кожне четверте шахрайство скоєно співробітником організації або внаслідок змови між співробітником та третьою стороною.

Відтак, зняття копій з електронних носіїв інформації та аналіз даних, що містяться на них, стає ще більш актуальними. Електронні докази суттєво допомагають протидіяти шахрайству у багатьох ситуаціях, серед яких: вивчення випадків фальсифікованої чи підміненої інформації, пошук джерел можливого витоку конфіденційної інформації, збір індикаторів, що можуть свідчити по потенційну або реальну змову між постачальником та співробітником організації для участі у тендері, виявлення фактів або спроб неналежного використання електронної пошти та інтернету на робочому місці та багато інших. Крім цього, належно зібрані електронні докази можуть бути використані в рамках комерційних спорів та кримінальних проваджень. Для цього важливо забезпечити легітимність їх збору. А це не так просто, як може здатися на перший погляд.

Перш за все, необхідно визначити джерела електронної інформації, адже залежно від цього фахівці з комп'ютерної криміналістики готують необхідне апаратне та програмне забезпечення, в тому числі таке, що унеможливлює запис або зміну наявної інформації на електронному носії. Як показує досвід PwC в Україні, організації найчастіше звертаються до нас із запитами щодо зняття копій з персональних комп'ютерів, ноутбуків, мобільних телефонів, серверів електронної пошти та планшетів.

У процесі зняття копій фахівці з комп'ютерної криміналістики також приділяють значну увагу процесу документування і формування ланцюга забезпечення схоронності (Chain of Custody). В даному контексті фіксуються подробиці того хто, коли, з якою метою працював із електронними пристроями, для підтвердження цілісності та автентичності інформації, та здійснюють необхідну фото-фіксацію процесу.

Після завершення процесу зняття копій обов'язково проводиться звірка відповідності хеш-значень у джерелі даних та в отриманій копії. Такий «цифровий відбиток» у подальшому дозволяє легко виявити будь-які зміни з скопійованими даними. Крім цього, завжди створюється резервна копія (бек-ап) знятої інформації з електронного носія.

Після того як зняті копії електронних джерел даних, постає питання: як правильно проаналізувати їх та знайти підтвердження необхідним гіпотезам у процесі розслідування? Додаймо ще до цього той факт, що інформація, яка записана на «копії» є неструктурованою та її зазвичай важко оперативно проаналізувати або здійснити пошук за атрибутами. Такими даними можуть бути: електронна пошта, переписка в месенджерах, файли користувачів тощо. Враховуючи великі обсяги інформації у випадку «ручного» аналізу, процес може затягнутися на кілька місяців, а це зовсім не той результат, якого прагнуть отримати організації у кризових ситуаціях.

У своїй роботі ми використовуємо спеціалізоване програмне забезпечення для роботи з такими неструктурованими даними, що дозволяє їх швидко перетворити у придатний для пошуку та подальшого аналізу формат. Також, в процесі аналізу електронних даних необхідно виключити дублюючі файли, здійснити розпізнавання тексту для окремих форматів документів та позначити файли, за якими не може бути здійснений пошук (наприклад, аудіо-файли) тощо.

Залежно від наявних гіпотез, що були сформовані для проведення аналізу, ми також готуємо перелік ключових слів, за допомогою яких додатково можна зменшити кількість інформації, яку необхідно знайти та проаналізувати.

Для здійснення процедур зняття копій з електронних носіїв даних та аналізу інформації організації часто залучають власних IT спеціалістів, створюють окремі підрозділи або передають процес на аутсорсинг компаніям, які мають власні лабораторії форензік технологій. Такі зовнішні фахівці проходять відповідне навчання, мають сертифікації, використовують спеціалізовані IT рішення, обладнання та ліцензоване програмне забезпечення, здійснюють необхідне документування та можуть брати участь у судових засіданнях як експерти з комп'ютерної криміналістики, з метою роз'яснення процедур, що були зроблені з метою отримання електронних доказів та методології, що використовувалась.

Враховуючи сенситивність питань, організаціям важливо мати «trusted advisors», які готові швидко мобілізувати команду для допомоги у кризовій ситуації.

СИСТЕМА ІНФОРМУВАННЯ ПРО ШАХРАЙСТВО: НЕОБХІДНІСТЬ ЧИ ПЕРЕВАГА

Анастасія МИРОШНИЧЕНКО

Старший консультант практики Форензік,
PwC в Україні

Шахрайство є серйозною проблемою, з якою під час своєї діяльності стикаються організації різних типів, розмірів та галузей. З кожним днем розслідувати шахрайство та інші види економічних злочинів стає складніше.

Протягом останніх років все більше організацій розуміють, що набагато раціональніше проактивно управляти ризиками шахрайства, попереджати та вчасно виявляти їх, аніж діяти реактивно, витрачаючи цінні ресурси на розслідування та усунення негативних наслідків. Як результат, організації вживають спеціальних заходів задля вчасного виявлення шахрайських дій або запобігання їх прояву. На сьогодні надійна програма протидії та боротьби з шахрайством передбачає, зокрема, побудову системи інформування, впровадження програми протидії шахрайству та навчання з питань запобігання шахрайству та порушенням.

Першим кроком до попередження та виявлення шахрайства є створення всередині організації середовища з нульовою толерантністю до шахрайства. Починати варто із впровадження системи внутрішнього контролю, ознайомлення всіх зацікавлених сторін (співробітників, постачальників, клієнтів) з принципами управління ризиками шахрайства, яких дотримується організація, а також впровадження системи інформування (англ. «whistleblowing system»), надавши можливість усім зацікавленим сторонам повідомляти про будь-яку протиправну чи неетичну поведінку, яка стала їм відома.

В Україні практика застосування системи інформування про шахрайство вперше з'явилася як обов'язковий елемент глобальних політик міжнародних компаній. Довгий час іншими організаціями, як приватного, так і в державного сектору, це сприймалось здебільшого як формальність. Це також підтверджується результатами нашого цьогорічного дослідження «Оцінки безпеки ведення бізнесу в Україні», проведеного разом з Sayenko Kharenko: лише 5 % компаній-респондентів використовують офіційний канал повідомлення про випадки шахрайства, корупції або інших економічних злочинів (англ. «whistleblowing hotline»).

Однак останніми роками все більше організацій свідомо запроваджують таку систему, завдяки чому викривають все більше випадків шахрайства та інших суттєвих порушень.

Звісно, є певний відсоток випадків, коли викривачі, повідомляючи про порушення, не використовують офіційні канали інформування (телефонна «лінія довіри», поштова скринька, e-mail або сайт). Натомість, вони надають перевагу повідомити про підозри своїм безпосереднім керівникам чи іншим зацікавленим особам. Розуміння того, як часто викривачі повідомляють про шахрайство, не використовуючи традиційні інструменти інформування, може допомогти організаціям відповісти на декілька важливих питань.

Зокрема, як слід реєструвати та передавати повідомлення, отримані поза межами офіційного механізму інформування? Та кого слід навчити розглядати повідомлення про підозри?

Згідно результатів дослідження Асоціації сертифікованих експертів з шахрайства у 2020 році одним із основних методів виявлення шахрайства в організації є вказівки (англ. «tips»). За їх допомогою було виявлено 43 % шахрайських схем у світі, половина з яких надійшла від співробітників організацій, які були або безпосередніми учасниками злочинної схеми, або свідками порушень. З огляду на статистику, завдяки вказівкам, які надходять через механізми інформування, випадки шахрайства виявляються особливо часто (47 % випадків) у невеликих організаціях (<100 співробітників), порівняно з більшими організаціями (31 %).

Очевидно, що механізм інформування про порушення надає співробітникам та бізнес-партнерам організації можливість конфіденційно та безпечно повідомити про ті ситуації чи події, що їх непокоять, зокрема – про ймовірні випадки порушень, що стосуються шахрайства, крадіжок, хабарництва чи інших зловживань. Тому надзвичайно важливо створити в організації сприятливі умови для інформування про порушення, забезпечити необхідні заходи в частині обробки отриманих повідомлень та реагування на інциденти (проводити розслідування та приймати фінальні рішення на основі його результатів). Більш того, щоб система інформування користувалась попитом серед співробітників та бізнес-партнерів, а також стала одним із основних інструментів для виявлення та протидії шахрайству в організації, необхідно, щоб вона відповідала певним критеріям:

- **Професійність** – для підтримки роботи системи інформування про шахрайство мають залучатися достатні та кваліфіковані ресурси.
- **Конфіденційність** – через системи інформування обробляється чутлива інформація, тому організації повинні поважати конфіденційність викривачів та захищати їх від можливих наслідків, в тому числі, усіх форм помсти.

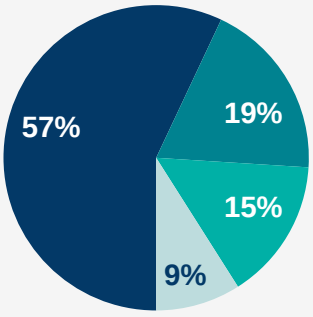
  Це зміцнює довіру до механізму та захищає організації від потенційної фінансової, правової та репутаційної шкоди.
- **Зворотний зв'язок** – організація повинна реагувати на всі отримані повідомлення та давати зворотний зв'язок викривачам. Співробітники будуть більш охоче використовувати механізми повідомлення про неетичні дії, якщо будуть знати, що організації серйозно ставляться до викорінення корупції та шахрайства.

Згідно зі статистикою, в середньому для того, щоб виявити шахрайство, організації потрібно 18 місяців. Водночас, в тих компаніях, де функціонують анонімні «лінії довіри», куди працівник або інші зацікавлені особи можуть подзвонити чи написати, проходить 12 місяців до моменту викриття шахрайства. Тому ефективність системи інформування про порушення пояснюється всім відомим висловом: «Час – гроші». Більш того, шкода, спричинена шахрайством, далеко не обмежується суто фінансовими збитками. Вона також може спричинити значний негативний вплив, ставлячи під загрозу відносини, репутацію та бренд, важливі для забезпечення неперервного успішного розвитку та зростання організації.

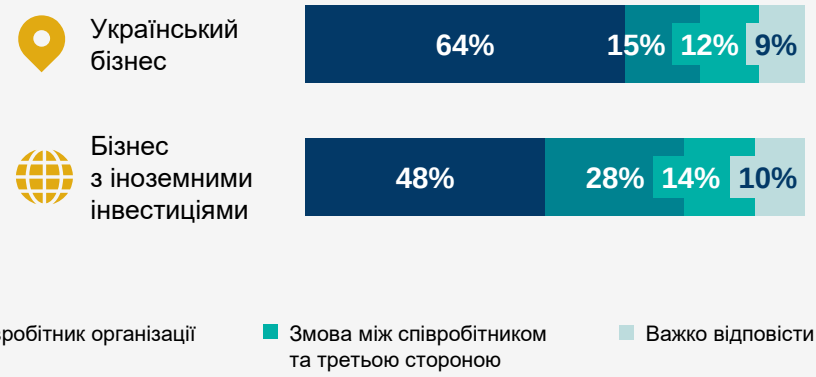
Хоча в українських організаціях до механізмів повідомлення про неетичні дії та до осіб, які ними користуються, відносяться як до пережитку радянських часів, на сьогодні налагоджена система інформування – найбільш ефективний та оптимальний метод попередження та виявлення шахрайства у будь-якій організації.

Шахрайство може з'явитися з будь-якого боку

Всі компанії



З яким типом шахрайства компанії стикаються найчастіше



57 % респондентів визначили недобросовісність третьої сторони як причину найсуттєвішого випадку шахрайства, корупції або інших економічних злочинів в їх компаніях за 2020 рік. Даний показник значно вищий, ніж середній у світі (39 %), проте, і для компаній з інших країн світу шахрайство з боку третіх сторін вважається причиною найбільш суттєвого інциденту шахрайства. Це й не дивно, адже все більше компаній використовують аутсорсинг для непрофільних сфер діяльності з метою зниження витрат.

Недоброчесна поведінка співробітника організації (19 %) або його змова з третьою стороною (15 %) теж є можливими причинами виникнення шахрайства, корупції або інших економічних злочинів у 2020 році. Випадки шахрайства, вчинені співробітниками, а тим більше керівництвом, як правило, важче прогнозувати, відстежувати і контролювати. При цьому, вони зазвичай спричиняють серйозніші наслідки для компаній, адже часто можуть призвести до цивільних або кримінальних справ проти організації та причетних осіб, зашкодити репутації, а в деяких випадках – до втрати бізнесу в цілому.

Як ефективно протидіяти шахрайству

Невід'ємною складовою ефективної системи протидії шахрайству в організації є управління відповідними ризиками. В його основі лежить розробка комплексного набору заходів з урахуванням специфіки діяльності організації та широкого спектру внутрішніх і зовнішніх факторів впливу, спрямованих на своєчасне попередження, виявлення, аналіз та реагування на ризики шахрайства, що можуть поставити під загрозу життєздатність компанії, її репутацію та спроможність реалізувати свою місію.

Процедура оцінки ризиків шахрайства складається з низки взаємопов'язаних кроків, проведення яких на регулярній основі допомагає досягти максимального ефекту від такої оцінки:

- **Ідентифікація ризиків** – виявлення джерел ризиків, дослідження подій, їх причин та можливих наслідків.
- **Аналіз ризиків** – документування та ретельне вивчення існуючих заходів контролю. Також проводиться вивчення рівня ризиків на основі ймовірності їх виникнення та наслідків у разі їх реалізації.
- **Оцінка ризиків** – оцінка того, чи знаходяться визначені ризики шахрайства в допустимих межах та якими повинні бути подальші дії.
- **Реагування на ризики** – визначення та впровадження заходів щодо виявлених ризиків спрямованих на їх уникнення, пом'якшення, прийняття та / або передачі третім сторонам.

Поширеною у світі практикою реагування на випадки шахрайства є залучення зовнішніх форензік-експертів для проведення оцінки ризиків шахрайства, аналізу та розслідування таких випадків, а також розробка практичних рішень, що сприяють запобіганню, виявленню і ліквідації наслідків шахрайства. В Україні ситуація виглядає інакше:

лише 11%

респондентів залучали зовнішніх форензік-фахівців, згідно результатів даного дослідження

67%

компаній проводять розслідування випадків шахрайства.

Незважаючи на збільшення витрат на боротьбу з економічними злочинами та шахрайством, багато українських організацій все ще не займаються профілактикою шахрайства, а лише реагують або захищаються, коли факт шахрайства вже скоєний

35%

респондентів повідомили про шахрайство, корупцію або інші економічні злочини у їх компанії свою Наглядову раду або правоохоронний орган

Повністю запобігти ризикам виникнення шахрайства та корупції навряд чи можливо (і економічно невиправдано), однак компаніям варто вдаватися до систематичних кроків, спрямованих на їх виявлення та попередження.

Поєднання проінформованості про можливі схеми шахрайства та корупції, ретельної оцінки ризиків, вчасного реагування на них, впровадження необхідних заходів контролю, а також проведення координованих розслідувань можуть значно мінімізувати ризики шахрайства та корупції.

ШАХРАЙСТВА З БОКУ БІЗНЕС-ПАРТНЕРІВ, КЛІЄНТІВ, ПОСТАЧАЛЬНИКІВ – ЯК ЗАХИСТИТИ СВІЙ БІЗНЕС

Яна ОМЕЛЬЧУК

Менеджер практики Форензік,
PwC в Україні

У 2021 році наші клієнти значно частіше, ніж раніше, зверталися до нас із запитами щодо перевірки репутації та благонадійності їх контрагентів: клієнтів, бізнес-партнерів та постачальників. І це не дивно.

Українські компанії зазначають, що кожен другий випадок шахрайства здійснюють їх контрагенти. Такі результати ми отримали в рамках дослідження з «Оцінки безпеки ведення бізнесу в Україні», що проводили спільно компанії Sayenko Kharenko та PwC Україна в 2021 році.

Виклики з якими стикається бізнес сьогодні

Очікувано, що під час кризи у людей та компаній зменшується рівень доходу. Це, в свою чергу, породжує додатковий зовнішній стимул для скоєння шахрайства.

Крім цього, віддалена робота певною мірою призводить до зниження якості виконання операційних бізнес-процесів в компанії, з різних причин: недостатньої автоматизації, слабкої комунікації та взаємодії між учасниками. Це призводить до погіршення якості виконання внутрішніх контролів в бізнес-процесах, створюючи можливості для вчинення шахрайства. Іншими словами – співробітники недостатнього добре перевіряють доброчесність контрагентів з якими ви співпрацюєте, їх директорів та власників.

Також, керівництву та власникам стає набагато важче віддалено демонструвати «тон зверху», транслювати цінності компанії та забезпечувати поінформованість співробітників про етичні та комплаєнс-вимоги. А в умовах кризи саме культурний аспект має визначальний вплив на запобігання виправданню співробітниками своїх шахрайських дій.

Стимул, можливість та виправдання – трикутник факторів, що призводять до шахрайських дій в компаніях.

Поширені індикатори шахрайства з боку контрагентів:

- Небажання контрагента розкривати структуру власності компанії
- Контрагент отримує 90-100 % доходу від вашого бізнесу
- Постійне розширення об’єму робіт та вартості контракту в додаткових угодах
- Дроблення контрактів на допорогові закупівлі для уникнення тендеру
- Пов’язаність директорів та власників контрагентів з вашими співробітниками: друзі чи родичі
- Негативні новини в медіа, що стосуються відмивання коштів, корупції, афіліації з політиками

На перший погляд, дані індикатори досить легко виявити та перевірити. Водночас, дослідження PwC щодо економічних злочинів та шахрайства, проведене в Україні у 2020 році свідчить, що багато випадків шахрайства не виявляються роками, а 14 % шахрайських схем взагалі виявляються випадково.

Як же тоді бізнесу захистись:

Здійснювати регулярну перевірку доброчесності контрагентів перед початком роботи з ними (ми називаємо «Integrity Due Diligence»), зокрема перевіряти: корпоративну структуру власності, судову історію, фінансові показники, списки санкцій та публічних діячів («PEPs»), Інтернет та медіа щодо негативної інформації про компанію, її керівників та власників. Варто здійснювати пошук інформації не тільки на локальних ресурсах, але й в міжнародних базах даних.

Крім цього, важливо періодично проводити аудит фінансових операцій з високим ризиком шахрайства, зокрема благодійність, розваги, консультації, маркетинг, IT-консультації, навчання. Необхідно перевіряти не тільки фінансові потоки, але й документацію, що супроводжувала прийняття рішень щодо початку роботи з контрагентом та первинні бухгалтерські документи (договори, рахунки-фактури, акти приймання-передачі).

Також, важливо проводити періодичний скринінг ризикованості портфелю всіх контрагентів. Ми використовуємо автоматизоване рішення – FAIT, яке дозволяє агрегувати дані з публічних реєстрів щодо контрагентів та проаналізувати ризики співпраці з ними за 40 критеріями (наприклад, юридична особа зареєстрована менше, ніж 3 місяця до початку контрактних відносин; реєстрація в квартирі; фінансова залежність контрагенту від бізнесу нашого клієнта, негативні новини в медіа).

Бізнесу насправді вигідно інвестувати в інструменти для запобігання шахрайству.

У керівництва та власників бізнесу завжди постає питання чи варто інвестувати у впровадження інструментів для попередження шахрайства з боку контрагентів – адже це додаткові витрати на IT системи, співробітників, навчання, консалтинг.

Варто замислитись про інше, а саме – скільки грошей втрачає ваш бізнес від шахрайства. Дослідження Асоціації сертифікованих експертів з шахрайства у 2020 році свідчить, що компанії втрачають 5 % річного доходу внаслідок шахрайських схем. Це зокрема пов’язано зі зривом бізнес-партнерств, нереалізованими проектами з розширення бізнесу та виходом на нові ринки, незапланованими зупинками в роботі та відтоком ключового персоналу.

Крім цього, середній збиток від одного випадку шахрайства може сягнути 125 тис. доларів, включаючи безпосередні втрати від нечесних схем та крадіжок, а також витрати, пов'язані з проведенням розслідувань та судовою тяганиною, штрафи та санкції регуляторних органів.

Контактні особи

SAYENKO KHARENKO

Сергій ПОГРЕБНОЙ
Партнер
Sayenko Kharenko
sp@sk.ua

Віктор ПАНЧАК, CPP
Віцепрезидент
SK Security
pvi@sksecurity.org

pwc

Андрій ТРЕТЯК, CFE
Керівник практики
Форензік послуги, PwC Україна
andrey.tretyak@pwc.com

Дарія РЯБОВА
Менеджер практики
Форензік послуги, PwC Україна
dariia.riabova@pwc.com