

*Всесвітнє дослідження економічних
злочинів та шахрайства 2018 року:
результати опитування українських
організацій*

Виведення шахрайства з тіні



Ми раді поділитися з Вами результатами опитування українських організацій в рамках Всесвітнього дослідження економічних злочинів та шахрайства 2018 року. Дане дослідження є однією з провідних публікацій свого роду для організацій з різних економічних сфер.

Це вже дев'ята публікація Всесвітнього дослідження економічних злочинів та шахрайства, яка підготовлена на основі відповідей, отриманих від більш ніж 7,000 респондентів із 123 країн світу.

Дане дослідження проводиться в Україні кожні два роки, починаючи з 2009 року, що дозволило нам спостерігати за тенденціями стосовно найбільш поширених видів економічних злочинів та шахрайства і їх впливом на українські організації, а також відслідковувати зміни в заходах, які вживають організації для попередження шахрайства.

За результатами дослідження 2018 року, 48% українських організацій постраждали від випадків економічних злочинів та шахрайства протягом останніх двох років, порівняно з 43% у 2016 році. Хабарництво та корупція залишається одним із основних видів економічних злочинів, негативний вплив яких зазнають українські організації – 73% респондентів відповіли, що їхні організації стали жертвами випадків хабарництва та корупції протягом останніх двох років. До п'ятірки найбільш поширених видів економічних злочинів та шахрайства також входять: незаконне привласнення майна, шахрайство у сфері закупівель, шахрайство у сфері управління персоналом та кіберзлочини.

Незважаючи на той факт, що обізнаність українських організацій щодо випадків шахрайства зростає, за результатами цього річного дослідження кожен сьомий випадок шахрайства в організації був виявлений випадково.

Результати нашого дослідження ілюструють, що шахрайство б'є по кишені організацій в Україні – 12% респондентів зазначили збитки їхніх організацій досягли від 1 млн. дол. США до 50 млн. дол. США. Проте, це ще не всі негативні наслідки. Українські організації відзначають, що від економічних злочинів та шахрайства найбільше постраждали їхня репутація/бренд, відносини з бізнес-партнерами та взаємодія з регуляторами.

Як підкреслюють результати даного дослідження, зараз найкращий час ніж будь-коли запитати себе: чи робимо ми все можливе в нашій організації, щоб запобігти випадкам економічних злочинів та шахрайства, та чи не втрачаємо ми із поля зору щось важливе у цій боротьбі?

Коли цифрові технології активно розвиваються, вони набувають подвійного значення – є водночас і загрозою для організації, і засобом її захисту. У сучасних реаліях цифрові технології охопили усі аспекти діяльності організації, у той самий час вони використовуються для скоєння економічних злочинів та шахрайства. Проте, коли йдеться про застосування новітніх інструментів та методів для виявлення шахрайства та реагування на нього (наприклад, аналітика даних, тестування транзакцій, моніторинг електронної пошти), українські організації відстають від решти світу. Крім того, більшість організацій в Україні недостатньо підготовлені до кібератак, лише кожна третя організація в Україні має програму кібербезпеки.

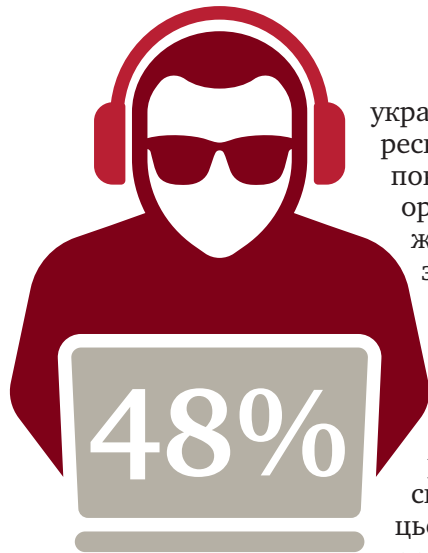
Тому, в рамках даного Всесвітнього дослідження економічних злочинів та шахрайства 2018 року ми звертаємо особливу увагу на зростаючу загрозу «білих плям» у боротьбі з економічними злочинами та шахрайством, які має кожна організація незалежно від її розміру, галузі та розташування. Також, ми розглянемо заходи з протидії економічним злочинам та шахрайству, які організації можуть застосовувати, щоб вивести шахрайство з тіні.



Марчин Клімчак

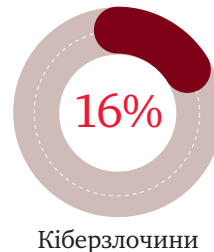
Партнер, лідер практики форензик PwC у Польщі, Україні та країнах Балтії

Дізнайтесь як виглядає шахрайство



українських респондентів повідомили, що їхня організація стала жертвою економічних злочинів та/ або шахрайства протягом останніх двох років, що в середньому відповідає світовому рівню в 49%, проте свідчить про зростання цього показника порівняно з 43% у 2016 р.

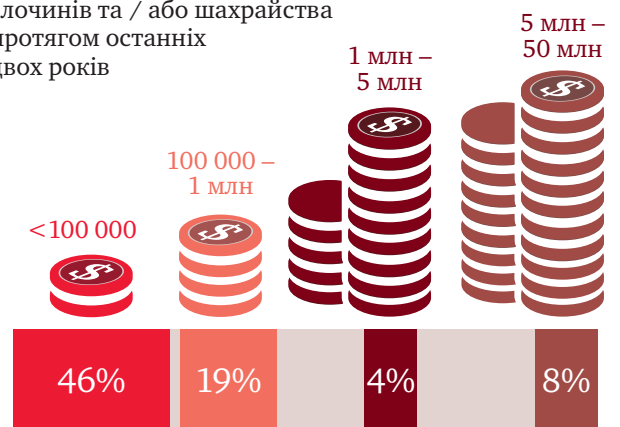
Топ 5 видів економічних злочинів та / або шахрайства, які, згідно очікувань українських респондентів, будуть найбільш суттєвими для організацій з точки зору фінансових збитків або інших наслідків у наступні два роки



Топ 5 видів економічних злочинів та / або шахрайства в 2018 році:



Фінансові збитки у доларах США, яких зазнали українські організації від випадків економічних злочинів та / або шахрайства протягом останніх двох років



36% випадків шахрайства були скоєні третьою стороною (у світі: 40%).
56% випадків шахрайства були скоєні співробітниками організації (у світі: 52%).



Інші респонденти або не знали або утримались від відповіді

55% випадків шахрайства, скоєних співробітниками організації, були вчинені її вищим керівництвом, порівняно із 27%, зазначеними у 2016 р.



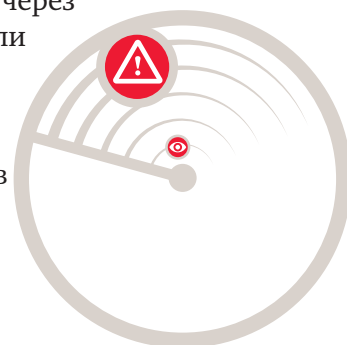
українських респондентів відповіли, що основною причиною, що спонукала співробітника у їхній організації до вчинення шахрайства була можливість його скоїти

1 із 3 організацій в Україні має програму кібербезпеки



14% випадків шахрайства були виявлені в результаті моніторингу підозрілих дій або шляхом інформування через неофіційні внутрішні канали

14% випадків шахрайства були виявлені випадково



33% українських респондентів відповіли, що їхня організація отримувала пропозицію дати хабаря протягом останніх двох років, порівняно із 13% респондентів, які зазначили такі випадки у 2016 році



Чи знаєте Ви про випадки шахрайства у Вашій організації?

Випадки шахрайства стають все більш публічними та видимими ніж будь-коли раніше – та чи дійсно ми виявляємо всі випадки шахрайства?

За даними нашого дослідження рівень шахрайства в українських організаціях виріс із 43% у 2016 році до 48% у 2018 році. Насправді, ці цифри більше демонструють випадки шахрайства, які було виявлено, аніж фактичний рівень шахрайства в організації.

Незважаючи на той факт, що обізнаність українських респондентів щодо випадків шахрайства в їхніх організаціях зростає, за результатами цього річного дослідження 1 з 7 випадків шахрайства в організації був виявлений випадково. З огляду на цей факт,

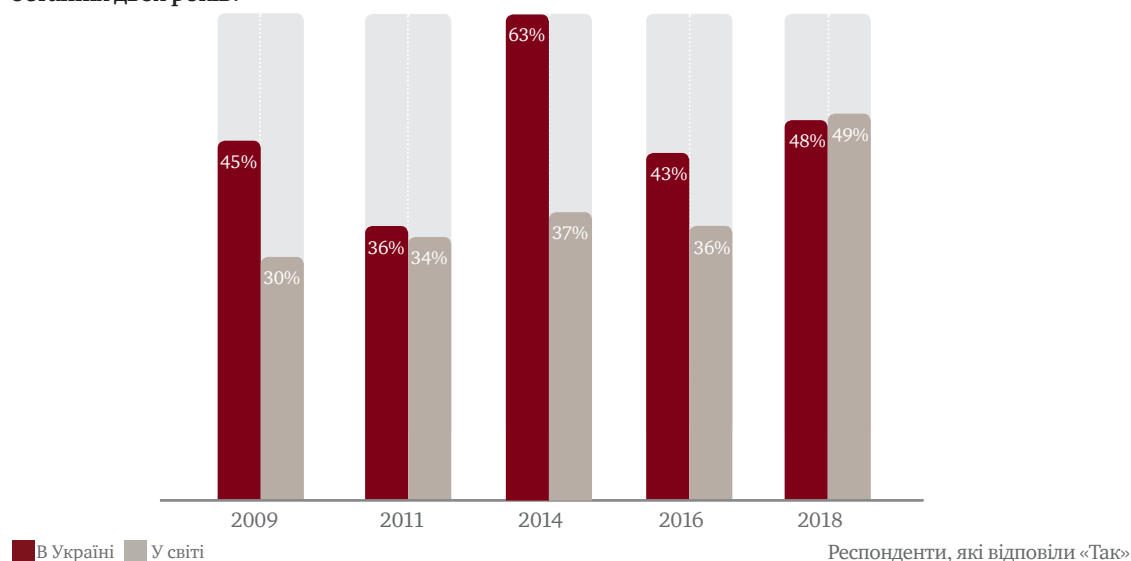
виникають питання: що не було виявлено? І головне, чому?

Кожна організація, незалежно від того, наскільки вона пильна, має «білі плями» у протидії економічним злочинам та шахрайству. Тому, пролиття світла на них може значно посилити цю боротьбу.

48%

українських респондентів повідомили, що їхня організація стала жертвою економічних злочинів та / або шахрайства протягом останніх двох років

Чи стикалася Ваша організація з випадками економічних злочинів та / або шахрайства протягом останніх двох років?



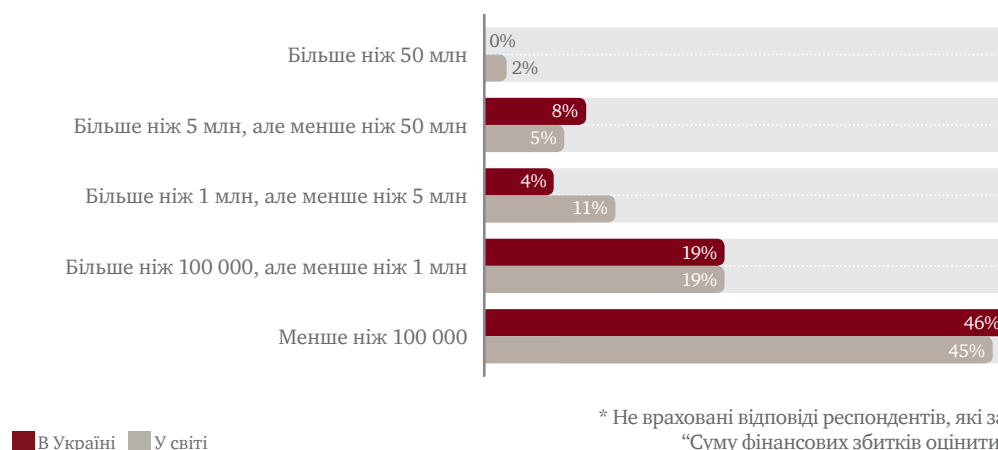
Шахрайство б'є по кишені організацій

Результати нашого дослідження ілюструють, що прямий фінансовий вплив на українські організації може бути досить значним – 31% респондентів відмітили, що збитки, яких зазнала їхня організація від найбільш суттєвих випадків шахрайства, становлять понад 100 000 дол. США, при цьому **12% із них зазначили збитки від 1 млн. дол. США до 50 млн. дол. США.**

З огляду на розміри можливих збитків, не дивно, що українські організації збільшують витрати на боротьбу із економічними злочинами та шахрайством до світового рівня.

34% організацій в Україні збільшили свої витрати на протидію шахрайству протягом останніх двох років (у порівнянні з 42% організацій у світі), а 37% планують їх збільшити протягом наступних двох років (у порівнянні з 44% організацій у світі).

На Вашу думку, яку приблизну суму фінансових збитків у доларах США зазнала Ваша організація від найбільш суттєвих економічних злочинів та / або шахрайства протягом останніх двох років ?



* Не враховані відповіді респондентів, які зазначили, що "Суму фінансових збитків оцінити неможливо" та "Важко відповісти".

58%

українських організацій повідомили про погіршення професійної етики та поведінки працівників внаслідок найбільш суттєвих випадків шахрайства

Наслідки від шахрайства – не тільки фінансові

Неважливо чи випадок шахрайства був один, чи організація стала жертвою системного шахрайства – розголошення цього факту громадськості може завдати серйозної шкоди репутації організації.

Це відбувається тому, що в час тотальної прозорості від організацій часто не залежить, коли проблема перетвориться на масштабну кризу. Натомість, це вирішує громадськість.

Українські організації відзначають, що від економічних злочинів та шахрайства найбільше постраждали їхня репутація/бренд (50%), відносини з бізнес-партнерами (42%) та взаємодія з регуляторами (38%).

Проте, це ще не всі негативні наслідки. Коли репутації організації нанесений удар, це в свою чергу негативно впливає на її працівників. 58% українських організацій відмітили погіршення професійної етики та поведінки працівників внаслідок найбільш суттєвих випадків шахрайства.

Оцінка ризиків – це перший крок на шляху протидії шахрайству

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 вчинений:

- Лише 40% опитаних організацій в Україні проводили загальну оцінку ризиків шахрайства протягом останніх двох років.
- Близько третини українських організацій повідомили, що проводили оцінку вразливості до кіберзлочинів.
- Та ж негативна тенденція спостерігається в більш фокусній оцінці ризиків критичних напрямків діяльності організацій: протидії хабарництву та корупції, боротьбі з відмиванням коштів, або застосуванні санкцій та дотриманні вимог експортного контролю. Крім того, лише 27% українських організацій проводили перевірку дотримання законодавства (due diligence) у сфері протидії хабарництву та корупції в процесі придбання / поглинання іншого бізнесу (порівняно з 45% організацій у світі).

- Кожна п'ята організація (17%) взагалі не проводила оцінку ризиків протягом двох років.

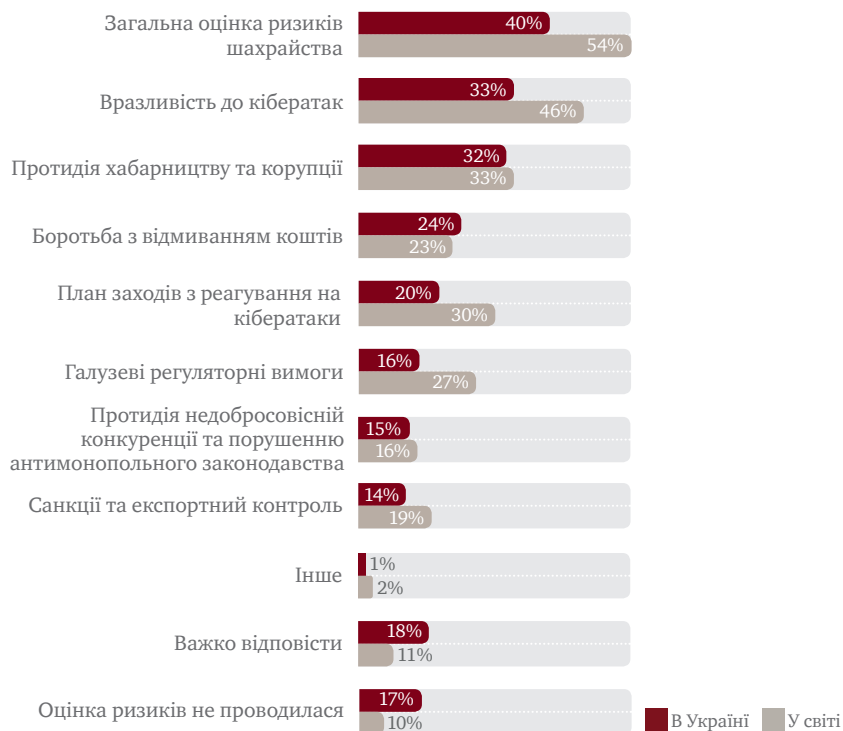
Однак, правила гри кардинально та безповоротно змінюються. Толерантність громадськості до неетичної професійної поведінки як з боку організацій, так і окремих їх співробітників, наближається до нуля.

Це вказує на високий ризик того, що факт економічного злочину чи шахрайства стане надбанням громадськості, тому організаціям нагально необхідно протидіяти шахрайству, поки воно не стало системним. Оцінка ризиків шахрайства може допомогти організаціям у виявленні конкретних шахрайських схем, притаманних для них, на які необхідно звертати увагу.

Що спонукало Вашу організацію до проведення оцінки ризиків?



Протягом останніх двох років, чи проводилась у Вашій організації оцінка ризиків у будь-якому з наступних напрямків?



“Старі друзі” чи “Нові обличчя”: основні види шахрайства

Найпоширенішими видами економічних злочинів в українських організаціях залишаються: хабарництво та корупція, незаконне привласнення майна та шахрайство у сфері закупівель.

Проте, результати цього річного опитування не обійшлися без «новачка». Вперше до п'ятірки найпоширеніших економічних злочинів в українських організаціях увійшло шахрайство у сфері управління персоналом, розділивши третє та четверте місце з шахрайством у сфері закупівель.

Не здають своїх позицій і кіберзлочини, які залишаються у п'ятірці найпоширеніших видів шахрайства в українських організаціях з моменту, коли ми вперше включили такий вид економічного злочину до опитування у 2011 році.

З якими видами економічних злочинів та / або шахрайства стикалася Ваша організація за останні два роки?



Рівень хабарництва та корупції в українських організаціях виріс із 56% у 2016 році до 73% у 2018 році. У світі, лише 25% респондентів відповіли, що їхні організації стикалися з випадками хабарництва та корупції, що майже втричі менше порівняно з українськими організаціями. Також, за результатами нашого дослідження кожний третій український респондент (33%) зазначив, що його організація отримувала пропозицію дати хабаря протягом останніх двох років. Викликає занепокоєння той факт, що 23% українських респондентів очікують, що хабарництво та корупція, з поміж інших видів економічних злочинів та / або шахрайства, буде найбільш суттєвим для їхніх організацій з точки зору фінансових збитків або інших наслідків у наступні два роки.

Показник випадків **незаконного привласнення майна**, беззмінний лідер у цій категорії, навпаки зменшився з 62% у 2016 році до 46% у 2018 році. Падіння показника цього виду економічного злочину може бути наслідком посилення контролів в українських організаціях та збільшення інвестицій у засоби для запобігання йому, які починають демонструвати свою ефективність. З іншого боку, ми вважаємо, що включення двох нових категорій (шахрайство з боку споживачів (17%) та неетична професійна поведінка (17%)) частково призвели до зменшення відповідей респондентів щодо випадків незаконного привласнення майна в їхніх організаціях.

Результати опитування за 2018 рік показали, що 33% організацій в Україні стикалися з **шахрайством у сфері закупівель**, що на 11% більше, ніж в організаціях у світі. Так часто випадки шахрайства у сфері закупівель трапляються в організаціях, які неефективно перевіряють постачальників на доброчесність та відсутність у них конфлікту інтересів, та які не мають механізмів контролю за вибором постачальників, укладанням з ними договорів та процесом оплати за їхні товари та послуги.

Шахрайство у сфері управління персоналом розділило третє та четверте місце серед видів шахрайства в українських організаціях, порівняно з восьмим місцем в організаціях у світі. Крім того, результати нашого дослідження демонструють стрімке зростання частки респондентів, які повідомили про цей вид економічного злочину: 33% у 2018 році порівняно з 4% у 2016 році. Зростання обізнаності про шахрайство у сфері управління персоналом та його сприйняття як справжнього шахрайства, а не як «оптимізацію витрат» – це, безумовно, позитивна тенденція, оскільки цей вид шахрайства може значно погіршити професійну етику та поведінку працівників, а також їх лояльність до організації.

Кількість **кіберзлочинів**, яких зазнають організації неухильно зростає з року в рік і цей вид економічного злочину несе високий ризик як для організацій комерційного, так і державного сектору. Результати опитування за 2018 рік свідчать про зростання числа кіберзлочинів проти організацій в Україні на 7%, порівняно з 2016 роком. Розвиток технологій призвів до виникнення ряду нових загроз для організацій, серед яких: шкідливе програмне забезпечення, фішинг, сканування мережі та атаки методом підбору паролів. А оскільки 16% українських респондентів переконані у вірогідності того, що їхня організація постраждає від кіберзлочинів у наступні два роки, організаціям в Україні слід приділити максимальну увагу цьому виду економічних злочинів.

55%

випадків шахрайства, скоєних співробітниками організації, були вчинені її вищим керівництвом



67%

третіх сторін, що скоюють шахрайства – це наближені до організації фізичні та юридичні особи: агенти, постачальники та клієнти

Так хто ж відповідальний?

У багатьох організаціях функції комплаєнс, етики та управління ризиками закріплені за окремими підрозділами і рідко розглядаються як єдине стратегічне ціле.

Такий підхід може призвести до того, що ті чи інші сфери діяльності організації залишаються неохопленими, тож випадки шахрайства можна дуже легко замовчувати чи вважати проблемою інших підрозділів, попри негативний вплив такого підходу на загальну ефективність заходів із запобігання шахрайству, фінансові результати та відносини з регуляторами.

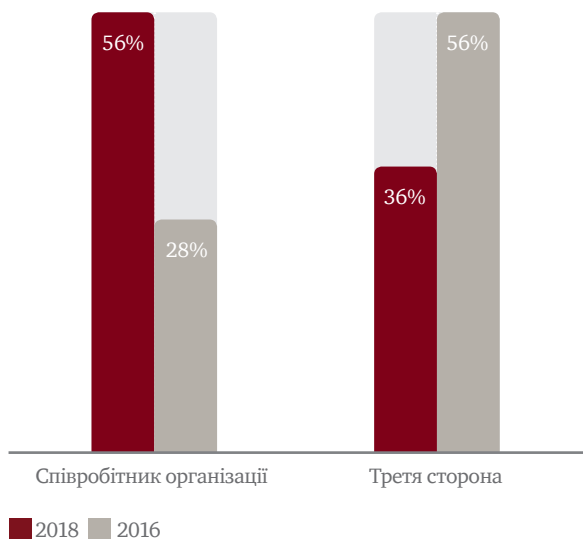
Розробка та впровадження механізму співробітництва та координації різних підрозділів організації, відповідальних за розслідування випадків шахрайства, за управління ризиками шахрайства та за звітування Правлінню або регуляторам, дозволить організації підвищити ефективність оцінки та управління комплаєнс, етикою та ризиками на горизонтальному рівні, а також врахувати їх принципи в процесі прийняття стратегічних рішень. Це важливий крок, який допоможе подолати нескоординованість дій основних підрозділів до чиїх функцій входить протидія шахрайству, та, зрештою, дозволить вивести шахрайство із тіні.

Хто стоїть за шахрайством?

Наше опитування виявило значне збільшення випадків шахрайства в українських організаціях, скоєних співробітниками (з 28% у 2016 році до 56% у 2018 році), з поміж яких частка шахрайства скоєного вищим керівництвом також суттєво зросла (з 27% у 2016 році до 55% у 2018 році). Більше того, протягом останніх двох років шахрайство, скоєне співробітниками організації, майже в два рази більше, ніж шахрайство, скоєне третіми сторонами.

Та попри ці факти, найбільшою «білою плямою» організації під час протидії шахрайству, а одночасно – і однією з найсерйозніших її загроз, часто є не її працівники, а її контрагенти. Це треті сторони, з якими організація має регулярні та прибуткові відносини – агенти, постачальники та клієнти. Іншими словами, це ті фізичні та юридичні особи, від яких організації очікують певну взаємну довіру, але які, натомість, можуть красти в організації. Зважаючи на результати цього річного дослідження, організаціям в Україні варто посилити управління ризиками щодо взаємодії з третіми сторонами (корпоративна розвідка, перевірка доброчесності контрагентів), як основний захід із запобігання випадкам шахрайства.

Хто вчинив найбільш суттєвий економічний злочин та / або шахрайство протягом останніх двох років?



Сучасні технології: вразливість організації чи можливість для неї?

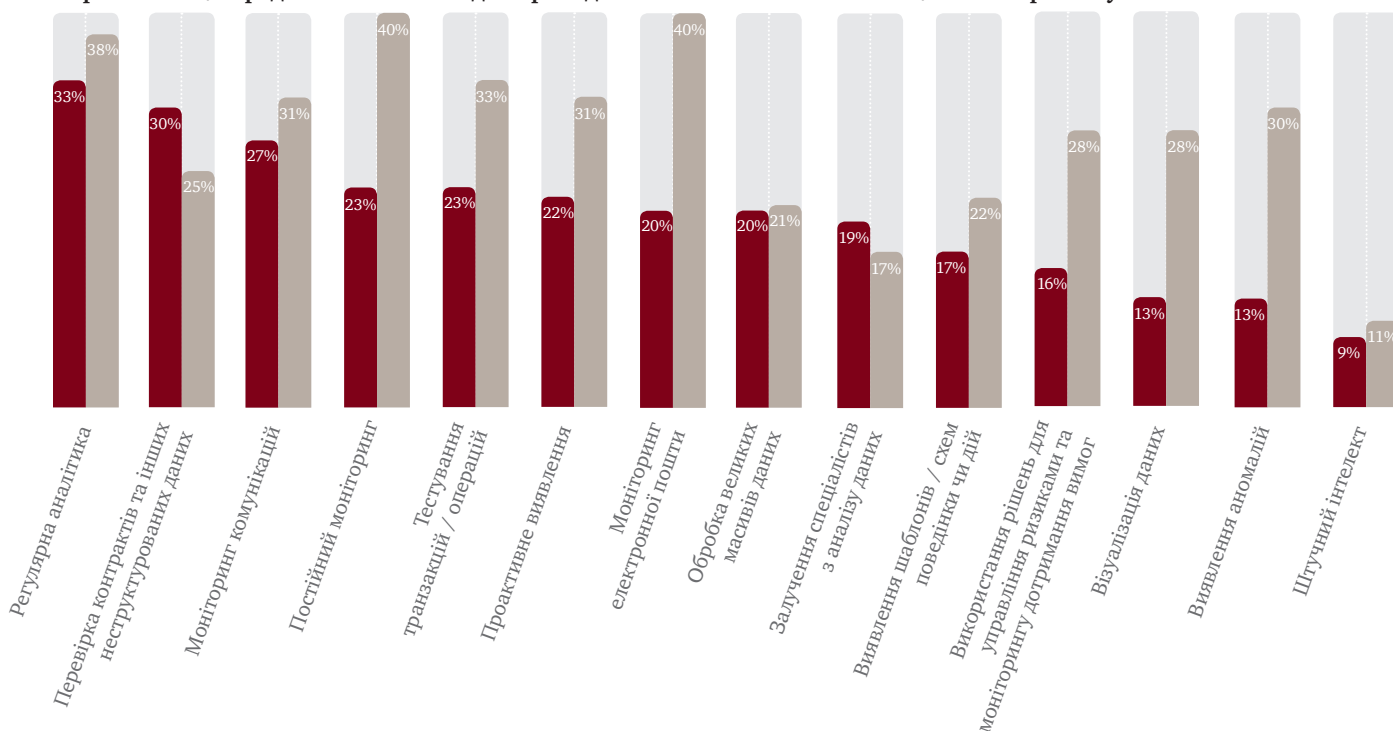
Визначте технології для боротьби з шахрайством, які підходять Вам

Цифрові технології активно розвиваються, проте набувають подвійного значення – вони водночас є і загрозою для організації, і засобом її захисту. У сучасних реаліях цифрові технології охопили усі аспекти діяльності організації, у той самий час вони використовуються для скоєння економічних злочинів та шахрайства. Через це, усі ми спостерігаємо ефект замкненого кола: рік за роком технології стають дедалі прогресивнішими, що, у свою чергу, створює простір для збільшення випадків шахрайських дій. Тож організаціям не залишається іншого виходу: вони змушені бути готовими реагувати на дедалі складніші типи шахрайських схем.

Якщо сучасні технології використовувати оптимально, вони можуть стати цінним інструментом для захисту організації. 49% українських респондентів відповіли, що технології дозволяють їхнім організаціям забезпечувати постійний моніторинг у режимі реального часу, а 51% переконані, що технології надають їхнім організаціям інформацію, яка дозволяє вживати оперативних заходів для протидії економічним злочинам та / або шахрайству.

Хід прогресу зупинити неможливо, тож сьогодні організаціям доступний величезний вибір з поміж інноваційних та надсучасних технологій для захисту від шахрайства. Проте, коли йдеться про застосування новітніх інструментів та методів, українські організації відстають від решти світу.

Якою мірою Ваша організація використовує або розглядає можливість використання з метою контролю наступних альтернативних / передових технологій для протидії економічним злочинам та / або шахрайству?



■ В Україні ■ У світі

*Відповіді респондентів, які вказали, що їхня організація «Використовує і вважає ефективними» альтернативні / передові технології для протидії економічним злочинам та / або шахрайству

Шахрайство дедалі більше мігрує у цифровий простір

Обсяги ділової активності в Інтернеті зростають з кожним днем. Як споживачі, так і організації дедалі сильніше залежать від ІТ. Поширення Інтернету та поява у повсякденному житті новітніх електронних засобів зробили шахрайство більш витонченим та оригінальним.

«Індустрія 4.0» («Четверта промислова революція», «Індустріальний Інтернет» або «Фабрика цифрових технологій») спрямована на повномасштабне переведення усіх фізичних активів і процесів на цифрові технології та їх інтеграцію у цифрові екосистеми з партнерами у ланцюжку створення доданої вартості. Це змінило спосіб ведення бізнесу та функціонування організацій – ми постійно дізнаємося про нові розумні пристрої: смартфони, смарт-телевізори, смарт-автомобілі тощо. Інноваційні рішення дозволяють машинам спілкуватися та приймати рішення, а технології штучного інтелекту, робототехніки, дронів та 3D-друку трансформують способи виробництва продукції та виконання повсякденних робочих завдань людиною. ІТ рішення вже стали базовим інструментарієм для функціонування організацій, в той самий час як ІТ організації виходять і на інші ринки: роздрібна торгівля, фінансовий сектор, ринок виробництва та збуту автомобілів. Та це ще не все: ІТ рішення створюють нові ринки та послуги, замінюючи собою роботу, яку раніше виконувала людина. Змінюються і принципи взаємодії: на ринку B2C (бізнес-споживач) поширюються інтернет-платформи та електронні сервіси, на ринку B2B (бізнес-бізнес) – смарт-контракти, на ринку B2G (бізнес-уряд) – технології електронного урядування.

Та разом з тим «Індустрія 4.0» створює для організацій нові загрози, серед яких: кібератаки, корпоративне шпигунство та багато інших. У цьому контексті інформаційна безпека стає невід'ємним компонентом успішного функціонування організації.

Наведемо деякі характеристики та виклики сучасного цифрового шахрайства:

- *Нові цифрові продукти створюють простір для нових видів атак.*

Раніше для того, щоб вивести продукцію на ринок, організації діяли за схемою B2B, тобто: співпрацювали з торговельними посередниками, дистриб'юторами та роздрібними мережами. Сьогодні ж організації активно використовують цифрові платформи B2C, які поєднують їх безпосередньо із споживачами та створюють можливість для істотно різноманітніших видів атак, а отже, і шахрайства. Тож не дивно, що багато споживачів й досі не довіряють інтернет-магазинам та платформам, адже в них є причини хвилюватися за безпеку своїх персональних даних чи недовіряти оплаті через Інтернет.

- *Треті сторони використовують дедалі складніші технічні засоби.*

Цифрове шахрайство стає дедалі складнішим, продуманим та руйнівним. Лише один з багатьох прикладів - це кібератака на магістральну електромережу України. Хакери змогли успішно проникнути до інформаційних систем трьох енергориночних компаній в Україні та тимчасово припинити постачання електроенергії кінцевим споживачам. Внаслідок цієї атаки близько 230 тисяч громадян залишилися без електроенергії протягом 1-6 годин.

- *Політично мотивовані кібератаки виходять на арену.*

За останні роки кібератаки стали доволі поширеним явищем. Та сьогодні організації та державні органи у всьому світі потерпають від нового гравця – кібератак, профінансованих державами, здійснених хакерами з політичних чи ідеологічних мотивів, та, вчинених терористичними організаціями. Для цих зловмисників кібератака – це засіб не збагачення, а досягнення тих чи інших геополітичних цілей: порушення діяльності держав, викрадення персональних даних та інтелектуальної власності, збір інформації про структуру інформаційних систем та програмного забезпечення, отримання даних для віддаленого доступу до критично важливої інфраструктури.

31%

організацій в Україні
постраждали від
кіберзлочинів

Підготуйтеся до інцидентів кібератак, поки ще не пізно

За даними нашого дослідження кіберзлочини один із найпоширеніших видів економічних злочинів: від них постраждали 31% організацій в Україні.

Кібератаки вражають все на своєму шляху: неважливо, чи це приватна компанія, чи державна установа, чи розташована вона в Україні, чи в іншій частині світу.

Організації в Україні з побоюванням ставляться до кіберзлочинів: 16% українських респондентів не лише очікують кібератаки на їхні організації у наступні два роки, а й переконані, що кібератаки будуть найбільш значимими для їхніх організацій з точки зору фінансових збитків або інших наслідків.

Та попри це, більшість організацій в Україні не лише недостатньо підготовлені до кібератак, а й не розуміють до кінця ризики, на які наражаються. Так, **лише кожна третя організація в Україні (31%) має повністю функціонуючу програму кібербезпеки** для захисту від кібератак. Така програма має включати наявні та потенційні ризики для організації і включати перевірений план заходів з реагування на інциденти кібербезпеки.

Стандартна практика для організацій, що постраждали від кіберзлочинів, це повідомити державні чи правоохоронні органи про інциденти кібератак. Проте, **28% організацій в Україні відповіли, що вони мало ймовірно або й навряд чи будуть повідомляти про такі факти державним або правоохоронним органам** (порівняно з 12% респондентів у світі). Більше половини (54%) цих респондентів стверджують, що не впевнені у тому, що у правоохоронних органів є необхідна кваліфікація у цій сфері, а інші 41% – не довіряють правоохоронним органам.

Більше третини українських організацій, що зазнали кібератак, постраждали від наслідків шкідливого програмного забезпечення.

Внаслідок кібератак були **порушені не тільки бізнес-процеси організацій** (на думку 51% українських респондентів), **а й завдані істотні збитки організаціям: 38%** українських респондентів зазначили, що їхні організації постраждали від вимагання через враження програмним забезпеченням типу ransomware.

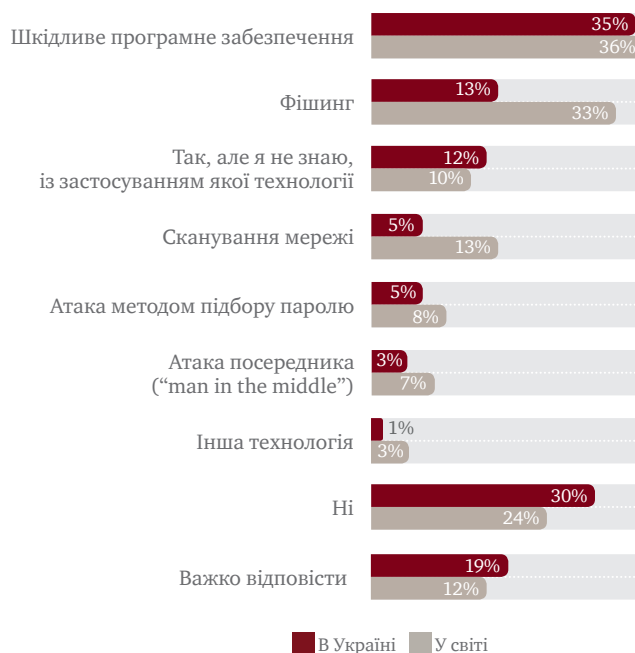
Нещодавні масштабні кібератаки з використанням програмного забезпечення типу ransomware були спрямовані на великі приватні компанії, підприємців та державні установи в Україні та світі. Тож, у небезпеці буквально кожний.

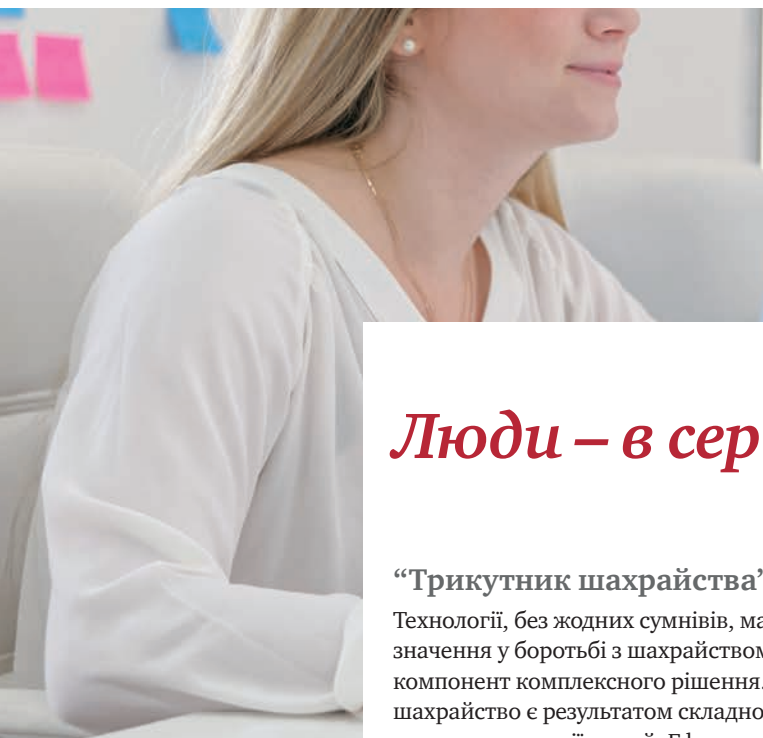
«Чи готова наша організація до кібератаки?» – це запитання, яке ми маємо поставити собі.

Від яких із зазначених видів економічних злочинів та /або шахрайства постраждала Ваша організація внаслідок кібератак?



Протягом останніх двох років, чи постраждала Ваша організація від кібератаки із застосуванням однієї із наступних технологій?





Люди – в серці будь-якої організації

“Трикутник шахрайства”

Технології, без жодних сумнівів, мають критичне значення у боротьбі з шахрайством, але лише як компонент комплексного рішення. Це тому, що шахрайство є результатом складного поєднання умов та мотивації людей. Ефективним засобом для розуміння та запобігання трьом основним факторам, що призводять до шахрайства з боку співробітників організації, – є трикутник шахрайства.

На верхівці “трикутника шахрайства” – стимул або тиск всередині організації, що схиляє до вчинення шахрайства, у підніжжя трикутника – можливість вчинення шахрайських дій внаслідок слабких механізмів контролю в організації та внутрішнє виправдання таких дій працівником організації. Оскільки, для скоєння працівником шахрайських дій потрібні усі ці три фактори, щоб запобігти шахрайству, необхідно впливати на кожен з факторів окремо, шляхом: заохочення культури відкритості на всіх рівнях організації, впровадження ефективних механізмів контролю та розвитку позитивної корпоративної культури.



Прозорість організації – попередження стимулу до вчинення шахрайства

Випадки шахрайства в організаціях приватного сектору, як правило, пов'язані з тиском всередині організації щодо досягнення бізнес-цілей, і цей тиск може виникати на будь-якому рівні організації. Згідно з результатами нашого опитування, 17% організацій в Україні постраждали від шахрайства, пов'язаного з неетичною професійною поведінкою (зловживання для досягнення заохочувальної винагороди).

Аналізуючи причини, що змушують співробітників чинити шахрайства, важливо не переоцінювати значення суто фінансових стимулів. Настільки ж важливими є страх та відчуття сорому за зроблену помилку.

Крім того, ситуативні персоналізовані механізми контролю допоможуть відповісти на запитання, чи не призводять надто агресивні плани з продажів до шахрайських дій. Також, ефективна система попередження потенційних проблем в організації може бути реалізована шляхом «політики відкритих дверей» та «гарячої лінії», про які відомо широкому загалу співробітників.

Якою мірою кожен із наведених факторів сприяв вчиненню співробітником (шахраєм) економічного злочину та / або шахрайства?

* (% українських респондентів, що назвали один із наведених факторів основним чинником вчинення співробітником шахрайства)

Частка організацій в Україні, які відповіли, що мають офіційну програму професійної етики та комплаєнс, зменшилась з

75%
до
59%

Механізми контролю – запобігання можливостям для вчинення шахрайства

31% опитаних респондентів в Україні вживають заходів із підвищення ефективності бізнес-процесів, зокрема, механізмів внутрішнього контролю. Аналогічні заходи внутрішнього контролю організації застосовують для протидії стимулу до вчинення шахрайських дій та виправданню таких дій: як зазначили 31% та 30% українських респондентів, відповідно.

Проте, організаціям слід приділяти більшу увагу та зосередити зусилля, спрямовані на боротьбу з шахрайством, для мінімізації саме можливостей для скоєння шахрайських дій.

В організаціях поширене переконання, що механізми внутрішнього контролю, які використовують технології, здатні самостійно виявити усі факти шахрайства, та що керівництво завжди діє етично. Насправді ж досвід свідчить про те, що майже усі значні випадки шахрайства з боку співробітників організації стали наслідком того, що керівництво організації має можливість обійти ці механізми внутрішнього контролю чи звести нанівець їхню ефективність. Результати нашого дослідження демонструють, що з-поміж випадків шахрайства, скоєного співробітниками організації, частка шахрайства вчиненого її вищим керівництвом різко зросла з 27% у 2016 році до 55% у 2018 році. Для подолання цієї системної проблеми організаціям необхідно розробити механізми контролю, які врахують можливість того, що керівництво зможе їх обійти, або вступити у змову в тому чи іншому напрямку.

Шахрайство є результатом перетину особистого вибору людини із порушенням роботи систем та контролів організації, тож вкрай важливо пам'ятати, що відчуття захищеності часто буває оманливим.

Корпоративна культура – боротьба із виправданням шахрайства

Коли працівники скоюють шахрайство, вони вважають, що це економічний злочин без потерпілих та не можуть собі уявити іншу особу, яка безпосередньо постраждає від їхніх дій.

Тож, у першу чергу, щоб боротися із тим, що працівники виправдовують для себе вчинене ними шахрайство, слід зосередити зусилля на середовищі, яке впливає на їхню поведінку, а саме: корпоративній культурі. Проведення опитувань, створення фокус-груп та поглиблені інтерв'ю із працівниками можуть використовуватись як засоби для оцінки сильних та слабких сторін корпоративної культури всієї організації. Безперервне навчання та розвиток компетенцій є, також, дуже важливими. Коли працівники чітко розуміють, що саме є неприйнятним і чому, - їм буде значно складніше виправдати для себе шахрайські дії.

Наше дослідження виявило, що організації в Україні скорочують свої інвестиції в розвиток етики та комплаєнс. Частка українських респондентів, які відповіли, що мають офіційну програму професійної етики та комплаєнс, зменшилась з 75% у 2016 році до 59% у 2018 році. При цьому лише 40% організацій в Україні, в яких впроваджена така програма, відповіли, що вона включає відповідні політики для протидії шахрайству в цілому.



А саме:

Моніторинг підозрілих дій	14%
Корпоративна безпека	8%
Внутрішній аудит (плановий)	6%
Управління ризиками шахрайства	6%
Аналітика даних	3%
Ротація персоналу	3%

А саме:

Випадково	14%
Від правоохоронних органів	8%
Журналістські розслідування	8%

А саме:

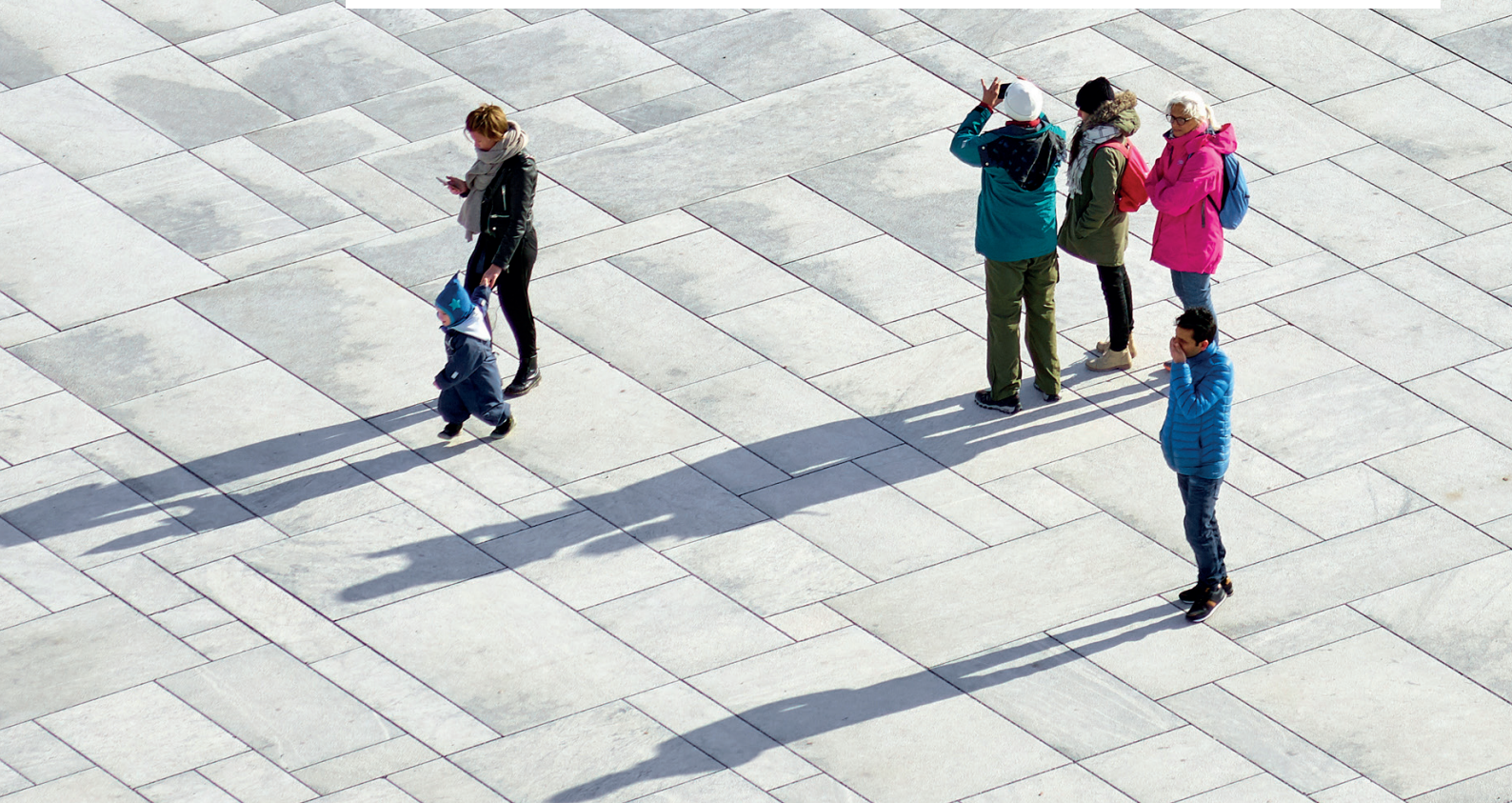
Неофіційні внутрішні канали	14%
Неофіційні зовнішні канали	6%
Офіційний канал («гаряча лінія»)	3%

Яким чином був виявлений випадок економічного злочину та / або шахрайства, який був найбільш суттєвими для Вашої організації з точки зору фінансових збитків або інших наслідків протягом останніх двох років?

Висновки

Наше дослідження демонструє, що досі багато організацій не готові до зіткнення із шахрайством, як з боку співробітників організації, так і з боку третіх сторін. Виявлення та попередження економічних злочинів чи шахрайства – це, поза всіляким сумнівом, комплексне та складне для організації завдання, яке передбачає пошук збалансованого комплексу заходів, які включають технології та людські ресурси, і побудовані на чіткому розумінні стимулів до шахрайських дій та обставин за яких ці дії вчинені.

Організаціям вкрай важливо відійти від переконання, що технології є єдиним рішенням або що, до певних меж, шахрайство можна вважати просто частиною операційних витрат організації. Натомість, лише створення корпоративної культури чесності та відкритості в організації за принципом «згори вниз», дозволить побудувати та просувати прозору підзвітність – а це, в свою чергу, дозволить вивести шахрайство з тіні.



Запитання, над якими варто замислитися вже сьогодні:

- Чи знаєте Ви, які напрямки Вашої організації найбільш вразливі до шахрайства і як їх захистити?
- Чи Ваші підрозділи комплаєнс, внутрішнього аудиту, інформаційної безпеки та управління ризиками координують свої дії між собою та працюють як єдина та цілісна функція?
- Якщо Ваші працівники крадуть у Вашої організації гроші, майно чи інтелектуальну власність, чи дізнаєтесь Ви про це?
- Чи маєте Ви чітке розуміння того, з якими третіми сторонами співпрацює Ваша організація? Ви впевнені у доброчесності та бездоганній діловій репутації Ваших контрагентів?
- Чи проводите Ви оцінку ризиків Вашої організації як річну чи стандартну процедуру або лише у кризовій ситуації?
- Чи знаєте Ви про сприйняття бренду Вашої організації та що може йому зашкодити?
- Як Ви забезпечуєте безпеку конфіденційної інформації, яку обробляють, зберігають чи передають зовнішні постачальники?
- Чи отримали Ваші працівники достатнє навчання і підготовку для виявлення та уникнення кібер-загроз?
- Чи знаєте Ви наскільки захищеними є Ваші критичні системи даних?
- Чи намагаєтесь Ви знайти збалансований підхід до інвестування у технології та людські ресурси?
- Як саме Ви заохочуєте Ваших працівників повідомляти про неетичну професійну поведінку? Чи є у Вашій організації офіційний канал («гаряча лінія») для анонімного інформування про зловживання чи шахрайство?
- Чи має Ваша організація комплексну програму професійної етики та комплаєнс, яка включає процедури з протидії шахрайству, хабарництву та корупції?

Контакти

Хочете дізнатися більше про те, що Ви можете зробити у боротьбі з шахрайством?
Зв'яжіться з одним із наших експертів



Марчін Клімчак
Партнер, Керівник практики
Форензик – PwC Польща,
Україна, країни Балтії
marcin.klimczak@pwc.com



Геннадій Чуприков
Директор, Форензик послуги,
PwC Україна
gennadiy.chuprykov@pwc.com



Рафаль Турчин
Директор, Форензик послуги,
PwC Україна
rafal.turczyn@pwc.com

PwC допомагає організаціям і приватним особам досягати поставлених цілей. Мережа PwC працює в 158 країнах, де більш ніж 236 000 фахівців надають аудиторські, податкові та консалтингові послуги найвищої якості. Ви можете висловити свої побажання та отримати більш детальну інформацію про діяльність фірм мережі PwC на сайті www.pwc.com.

Цей документ підготовлений виключно для отримання загальної уяви про питання, що в ньому обговорюються, і не є професійною консультацією. Не слід вживати будь-яких дій на підставі інформації, яка міститься у цьому документі, без попереднього звернення до професійних консультантів. Жодні заяви чи гарантії (явні чи неявні) не надаються щодо точності чи повноти інформації, яка міститься у цій публікації, і тією мірою, якою це передбачено законодавством, PwC не бере на себе жодної професійної, матеріальної або будь-якої іншої відповідальності за наслідки ваших або будь-чиїх дій чи бездіяльності, виходячи з достовірності інформації, яка міститься у цій публікації, і за будь-яке рішення, прийняте на її основі.

© 2018 Всі права захищено. PwC - це фірма-учасник мережі PwC. Кожна фірма мережі є самостійною юридичною особою. Більш детальну інформацію можна знайти на веб-сторінці www.pwc.com/structure.