www.pwc.com/ua

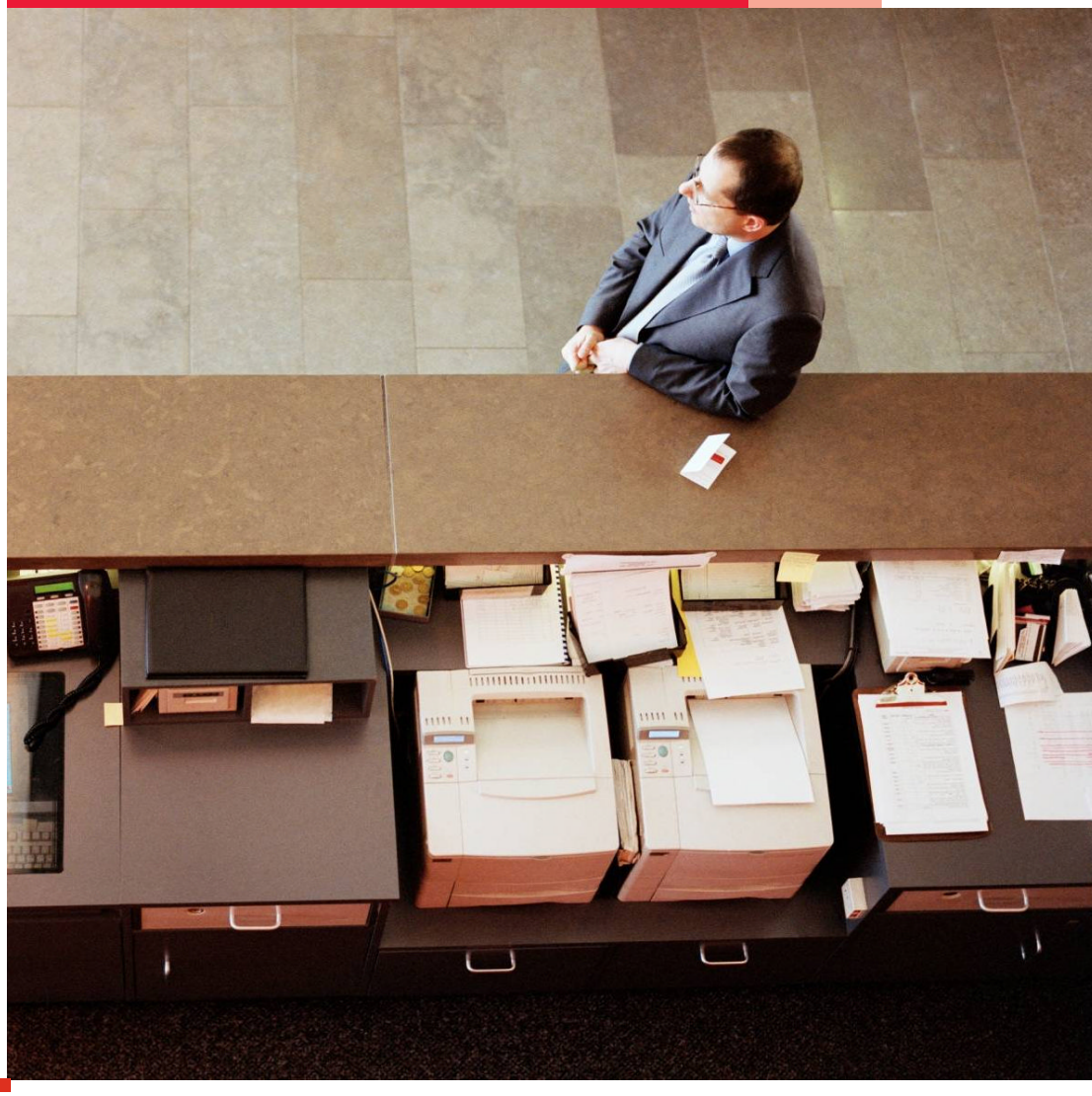
# *Україна*

# *Всесвітній огляд економічних злочинів*

## Кіберзлочини в центрі уваги

*З 877 респондентів із 78 країн поділилися своїми думками щодо економічної злочинності у світі*

*Грудень 2011*



pwc

# Зміст

# Загальна інформація

Економічна злочинність не має меж. Вона впливає на організації у всьому світі, жодна галузь економіки чи організація не може відчувати себе повністю захищеною від небажаних наслідків економічної злочинності. Крім безпосередніх збитків, економічна злочинність може завдати серйозної шкоди іміджу організацій та погіршити їхню репутацію, що в результаті може привести навіть до втрати долі на ринку. На сьогоднішній день суспільство стає все менш толерантним до недотримання етичних норм поведінки, тому організаціям необхідно завоювати довіру суспільства та постійно підтримувати її.

Цього року Всесвітній огляд економічних злочинів робить акцент на зростаючу загрозу кіберзлочинності. У наш час багато людей та організацій використовують різні технології, включаючи Інтернет. Таким чином вони зустрічаються з потенційними ризиками атак шахраїв із будь-якого куточку світу. На фоні таких проблем, як викрадення даних та виток інформації, комп'ютерні віруси та атаки хакерів, особлива увага у нашому огляді приділяється значущості цього виду економічної злочинності та його впливу на організації в усьому світі.

В рамках нашого дослідження проводилося опитування представників різних організацій щодо економічної злочинності. Також в огляд були включені специфічні запитання стосовно кіберзлочинності, які висвітлюють ризики і загрози кіберзлочинності і заходи, що їх вживають організації для реагування на атаки із використанням комп'ютерних технологій.

Цьогорічний звіт складається з двох частин:

1. Кіберзлочинність та її вплив на організації, рівень інформованості про кіберзлочинність та заходи зі зниження ризиків небажаних наслідків.
2. Економічні злочини, шахраї та жертви: види шахрайства, методи виявлення шахрайських дій, ідентифікація порушників та можливі наслідки.

Це вже шостий Всесвітній огляд економічних злочинів. В Україні таке дослідження проводиться вдруге.

Загальна кількість учасників склала майже 4 000 осіб з 78 країн, серед яких 53% – директори та топ-менеджери організацій, 36% учасників представляють організації, зареєстровані на біржах різних країн, та 38% учасників представляють організації з чисельністю персоналу понад 1 000 працівників.

Кількість респондентів з України збільшилася на 23% у порівнянні з попереднім опитуванням. В опитуванні взяли участь 84 керівники та представники вищого керівництва організацій, що працюють у 13 галузях економіки.

# Основні висновки

*Кіберзлочинність в Україні*

- Кіберзлочинність стала одним із п'яти найпоширеніших економічних злочинів в Україні.
- Кожен третій респондент (37%) вважає, що ризик кіберзлочинності підвищився за останні 12 місяців.
- Понад 25% організацій не мають відповідних політик та механізмів реагування на кіберзлочини.
- 46% опитаних не проходили навчання в області кібербезпеки протягом останніх 12 місяців.
- 58% респондентів з України заявили, що в їхніх організаціях відсутній процес моніторингу відвідування соціальних мереж.

*Економічна злочинність в Україні*

- 36% організацій зафіксували випадки економічної злочинності за останні 12 місяців.
- Третина організацій не проводять оцінку ризиків шахрайства.
- Незаконне привласнення майна (73%), корупція та хабарництво (60%) залишаються найпоширенішими видами економічної злочинності в Україні.
- Кількість внутрішніх шахрайських операцій суттєво зросла (на 22%) у порівнянні з 2009 роком.
- Більшість українських респондентів, які зафіксували випадки шахрайства оцінюють збитки в розмірі до 5 млн. дол. США.
- 40% злочинів були скоєні вищим керівництвом організацій.
- Кожен п'ятий працівник, який скоїв економічний злочин в організаціях не поніс покарання.

*Відсутність чіткого визначення та опису поняття кіберзлочинності призводить до того, що організації до кінця не усвідомлюють пов'язаних з нею ризиків. Це ускладнює процес виявлення та попередження кіберзлочинів*

# Загроза кіберзлочинності

На думку спеціалістів PwC, існує 5 основних видів кібератак, цілі та методи яких іноді співпадають:

Фінансові злочини і шахрайство. Здійснюються організованими групами осіб, що добре фінансуються і займаються викраденням коштів та інших активів за допомогою сучасних технологій.

Шпіонаж. На сьогодні корпоративна пошта та файли, а також традиційні об'єкти інтелектуальної власності (наукові дослідження та розробки) представляють велику цінність для будь-якої організації. Привласнення інтелектуальної власності – це постійна загроза. Жертви можуть навіть не здогадуватися про те, що трапилося, до моменту раптової появи піратських копій на ринку або реєстрації патенту на результати досліджень та розробок іншими третіми особами.

Воєнні дії. До них відносяться воєнні конфлікти між різними країнами, а також спроби захопити організації приватного сектору, зокрема такі важливі інфраструктурні об'єкти національного масштабу, як енергетична, телекомунікаційна та фінансова системи.

Тероризм. Перекликається із загрозою воєнних дій. Атаки здійснюються терористичними групами (з можливою підтримкою з боку держави) з метою захоплення стратегічно важливих приватних чи державних інфраструктурних об'єктів.

Активізм. За своєю природою нагадує деякі інші категорії, проте атаки здійснюються прихильниками ідеалізму.

Не існує загальноприйнятого визначення кіберзлочинності. Відповідно, відсутність чіткого визначення кіберзлочинності ускладнює процес виявлення та реагування на кіберзлочини, особливо коли організаціям навіть невідомо про існуючу небезпеку. Більше того, неповне розуміння «концепції супротивника» може звести нанівець усі спроби боротьби з кіберзлочинністю.

Виникає питання: кіберзлочинність – це просто інструмент для здійснення незаконних дій чи все ж таки окремий вид економічної злочинності?

Чи повинні організації вживати спеціальних заходів щодо управління цим ризиком на додаток до звичайних механізмів виявлення та попередження шахрайства?

У нашому огляді за 2011 рік ми спробували більш детально розглянути ці та інші питання.

У цьому опитуванні застосовувалося наступне визначення кіберзлочинності: ***«Кіберзлочинність (або «злочин з використанням комп'ютерних технологій»)*** *– це економічний злочин, скоєний із використанням обчислювальної техніки та мережі Інтернет. Приклади кіберзлочинності: розповсюдження вірусів, незаконне завантаження інформації, фішинг та фармінг, а також викрадення особистої інформації (наприклад, реквізитів банківських рахунків). До цієї категорії відносяться тільки ті економічні злочини, в яких основним (а не допоміжним чи супутнім) інструментом скоєння злочину є комп'ютер, Інтернет або електронні носії інформації та пристрої»*[1].

[1] Згідно з визначенням у Всесвітньому огляді економічних злочинності за 2011 рік, який був підготований PwC за сприяння нашого партнера з наукових питань професора Пітера Соммера.

# *Кіберзлочинність – один з п'яти найпоширеніших економічних злочинів в Україні*

Кіберзлочинність – це п'ятий за розмірами вид економічної злочинності в Україні після незаконного привласнення майна, корупції та хабарництва, недобросовістної конкуренції та маніпуляції з фінансовою звітністю (див. Рисунок 1).

За результатами опитування на кіберзлочинність припадає 23% випадків шахрайства у світі, про які повідомили учасники опитування, і 17% в Україні.

Дані огляду в сфері інформаційної безпеки свідчать про те, що кіберзлочини стають більш складними та витонченими, що перешкоджає процесу їх виявлення та попередження. Це може призвести до ще більших збитків та втрат у майбутньому.

## Новий ризик чи реальні випадки шахрайства, обсяги яких неухильно зростають?

Не всі із зазначених вище 5 видів кібератак є типовими для України. Проте абсолютно точно можна стверджувати, що загроза кіберзлочинності – це реальна проблема, яка може негативно вплинути на організації в Україні.

У попередньому Всесвітньому огляді економічних злочинів ми вже ставили запитання стосовно кіберзлочинів. З огляду на незначну кількість зафіксованих випадків кіберзлочинності результати не були виділені окремо в огляді за 2009 рік.

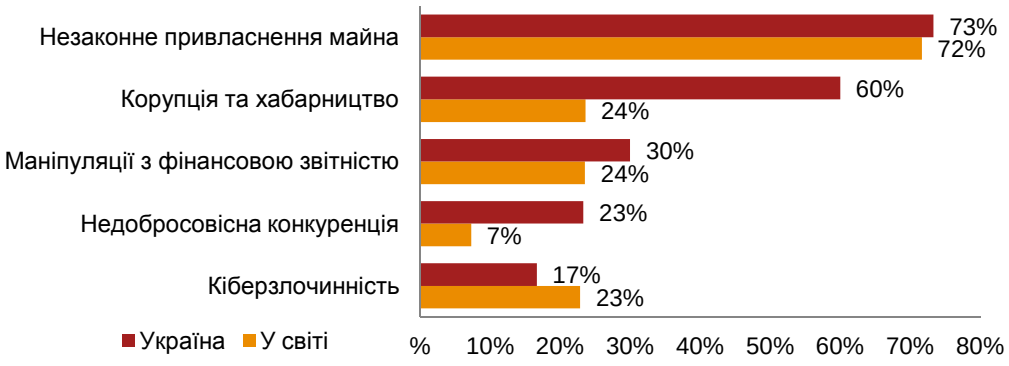
Враховуючи підвищену загрозу кіберзлочинності, в огляді за 2011 рік ми акцентували свою увагу саме на цьому виді шахрайства і знову включили питання, чи стикалися організації з випадками кіберзлочинності за останні 12 місяців.

Більше третини (37%) опитаних в Україні підтверджують, що кількість випадків кіберзлочинності в їхніх організаціях зросла. Близько 4% вказали на зниження цього показника, і 59% відповіли, що ситуація не змінилася.

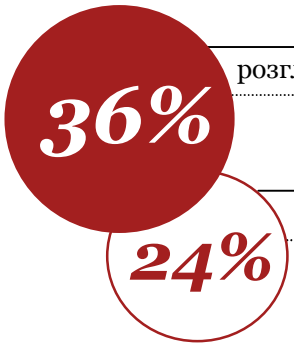
Збільшення ризику кіберзлочинності можна пояснити наступними факторами:

- Регулярні згадування у засобах масової інформації про випадки кібератак викликали підвищену увагу до цього виду шахрайства та змусили організації запровадити додаткові механізми контролю, які і дозволили виявити більшу кількість таких економічних злочинів;
- Неоднозначне визначення поняття кіберзлочинності: багато респондентів перекласифікували деякі традиційні види економічних злочинів як кіберзлочинність, тому що вони були скоєні з використанням комп'ютерів, електронних пристроїв чи мережі Інтернет;
- Підвищена увага з боку регулюючих органів;
- Використання новітніх технологій, які «полегшують» скоєння кіберзлочинів.

**Рис. 1: П'ять найпоширеніших економічних злочинів в Україні та світі у 2011 році**




Респонденти, які зіткнулися з економічною злочинністю за останні 12 місяців




розглядають ризик кіберзлочинів як зовнішню загрозу

розглядають ризик кіберзлочинів як внутрішню загрозу

## Кіберзлочинність – внутрішня чи зовнішня загроза?

36% респондентів в Україні розглядають кіберзлочинність як зовнішню загрозу, 24% – внутрішню загрозу, а 34% вважають, що загроза існує як ззовні, так і всередині організації.

Ці показники дещо відрізняються від результатів Всесвітнього огляду, оскільки 46% респондентів в інших країнах визнають, що ризик кіберзлочинності в основному виникає ззовні. І тільки 13% вважають, що злочини були скоєні працівниками організацій. 29% опитаних розглядають загрозу кіберзлочинності, як внутрішню і зовнішню загрози одночасно.

## Які джерела кіберзлочинності?

Організаціям було запропоновано відповісти на запитання: ризик зовнішньої кіберзлочинності переважно існує всередині чи за межами країни, в якій вони здійснюють свою діяльність?

Більше половини (53%) опитаних в Україні стверджують, що зовнішні загрози кіберзлочинності виникають всередині країни. Основними кібершахраями були визнані клієнти та постачальники. При цьому понад 40% учасників опитування впевнені, що загрози можуть виникати як за межами, так і всередині країни, в якій вони здійснюють свою діяльність.

Серед основних країн походження кіберзлочинності українські респонденти зазначили Гонконг (разом із Китаєм), Росію та США. Представники великої кількості українських організацій вважають, що загроза кіберзлочинності може виникнути у будь-якій країні світу, включаючи Україну.

Статистика Всесвітнього огляду підтверджує результати опитування в Україні. До списку можливих країн походження кіберзлочинності потрапили: Гонконг (разом із Китаєм), Індія, Нігерія, Росія, США та Україна[1].

*На сьогодні кіберзлочинність – це реальна глобальна загроза, яка може походити з будь-якої країни світу і виходити за межі конкретної юрисдикції на відміну від багатьох інших традиційних видів економічних злочинів*

## Які внутрішні джерела кіберзлочинності?

На думку 67% опитаних відділ інформаційних технологій (IT) є найбільш ризиковим підрозділом з точки зору кіберзлочинності як внутрішньої загрози. І це недивно, оскільки вважається, що саме співробітники відділу IT мають необхідні навички та можливості для скоєння злочинів з використанням комп'ютерних технологій (наприклад, надлишкові права доступу до систем із можливістю видалення журналів запису подій, що надалі ускладнює процес виявлення незаконних дій).

Проте варто зазначити ще один цікавий факт: серед інших підрозділів, які наражають організації на ризики кіберзлочинності, респонденти зазначили відділ фінансів (47%), відділ маркетингу та продажів (37%), юридичний відділ (27%), підрозділи вертикалі операційної діяльності (22%), а також представників вищого керівництва (29%). Подібна тенденція спостерігається і в інших країнах.

Найменш ризиковими були визнані відділ інформаційної безпеки та фізичної безпеки (16% опитаних), а також відділ з управління персоналом (10%). При цьому не варто забувати про те, що правопорушниками можуть виявитися співробітники будь-якого відділу.

[1] Країни перераховані в алфавітному порядку

*58% опитаних заявили, що в їхніх організаціях відсутній процес моніторингу соціальних мереж або їм невідомо про його наявність*

## Чи дійсно соціальні мережі настільки небезпечні?

58% опитаних в Україні та 60% у світі заявили, що в їхніх організаціях відсутній процес моніторингу соціальних мереж або їм невідомо про його наявність. Ця статистика насторожує, оскільки ці сайти можуть стати причиною виникнення суттєвих ризиків безпеки у випадку зловживань із боку співробітників.

Молоде покоління активно відвідує соціальні мережі переважно через нав'язану суспільством необхідність ділитися інформацією з іншими. Таким чином, відсутність моніторингу сайтів соціальних мереж може створити певні проблеми для організацій пов'язані з кіберзлочинністю.

При цьому варто визнати той факт, що сучасне покоління виросло разом із цими сайтами, і практика обміну особистою інформацією вже давно стала нормою для всього покоління.

Організації повинні усвідомлювати, що молоді спеціалісти можуть мати абсолютно інше бачення щодо ризиків, на які ці сайти потенційно наражають організації, і для них необхідно організовувати та проводити відповідні тренінги.

## Як знизити ризики?

Враховуючи визнану у всьому світі зростаючу тенденцію кіберзлочинності, той факт, що за останні 12 місяців 46% опитаних в Україні (42% у світі) не проходили жодних тренінгів із кібербезпеки, викликає занепокоєння. Це може свідчити лише про те, що їм невідомо про ризики, на які наражає їхні організації кіберзлочинність.

## Наскільки ефективні тренінги у процесі запобігання кіберзлочинам?

Ми задали запитання щодо того, які тренінги по боротьбі з кіберзлочинністю проводились в організаціях. Лише одна шоста опитаних, які пройшли тренінг, заявили, що відповідне навчання проводилося у форматі семінарів чи практичних занять. 62% проходили тренінги у віддаленому режимі, за допомогою електронних тренінгів і т.д.

Невелика кількість тренінгів у форматі семінарів і практичних занять пояснюється значними часовими та фінансовими витратами на їх проведення.

Проте 56% опитаних заявили, що саме такі тренінги є найбільш ефективними для підвищення рівня інформованості про кіберзлочинність.

## Що робити якщо злочин вже відбувся?

Нижче зазначені три найпоширеніші варіанти реагування українськими організаціями на кіберзлочини:

- залучення власних досвідчених працівників для вирішення проблеми;
- звернення за допомогою до незалежних експертів;
- інформування правоохоронних органів.

При виявлені шахрайства, скоєного третіми сторонами, організації, як правило, сповіщали про це правоохоронні органи та інші компетентні органи нагляду, а також подавали цивільні позови з вимогами про відшкодування збитків чи припинення ділових відносин.

Співробітників, причетних до шахрайських дій, у 73% випадках звільняли з посад.

Соціальні мережі можуть і не становити загрози кіберзлочинності, проте вони можуть бути використані для підвищення ефективності засобів соціальної інженерії, які спрямовані на скоєння злочинів із використанням комп'ютерних технологій або сприяють фішингу. Наприклад, використання соціальних мереж для збору інформації про конкретну особу (так звана техніка «цілеспрямованого фішингу») чи для встановлення шкідливих програм на комп'ютер користувача з метою полегшення подальшого скоєння кіберзлочинів.

# *Керівництво організацій приходить до розуміння того, що безпека у першу чергу стратегічно важливе питання бізнесу, ніж IT*

## Які заходи реагування вживають організації?

Як сказано вище, близько половини опитаних, які зіткнулися з економічними злочинами за останні 12 місяців, заявили, що ризик кіберзлочинності зростає.

Згідно з опитуванням, кіберзлочинність – це один з п'яти найпоширеніших видів шахрайства. З метою зниження ризику шахрайства багато українських організацій (50%) запроваджують додаткові технічні засоби та наймають кваліфіковані кадри для попередження та виявлення кіберзлочинів, а також для проведення службових розслідувань.

Як правило, зовнішніх консультантів залучають за фактом виникнення інциденту (57%). І лише 21% організацій в Україні звертається до зовнішніх експертів у попереджувальних цілях.

**Таблиця 1: Механізми реагування українськими організаціями на кіберзлочини в 2011 році**

| | |
|---|---|
| Використання внутрішніх ресурсів для попередження та виявлення злочинів | 51% |
| Використання внутрішніх ресурсів для проведення службових розслідувань | 50% |
| Залучення форензік-експертів | 45% |
| Медійні та PR плани менеджменту | 38% |

% від загальної кількості учасників опитування

## Як захистити свою організацію?

1. Отримати підтримку топ-менеджменту – правління та генерального директора необхідно інформувати про загрозу кіберзлочинності. Необхідно, щоб вище керівництво мало у розпорядженні повну інформацію про ризики, пов'язані з комп'ютерними злочинами.

2. Переглянути роботу служби безпеки – на відміну від традиційних економічних злочинів, кіберзлочинність динамічно змінюється, постійно виникають нові ризики, і як наслідок, організаціям необхідно постійно адаптувати свої процедури з урахуванням цих ризиків.

3. Інформованість – організаціям необхідна вся інформація про своє поточне та майбутнє комп'ютерне середовище. Якщо організація належним чином поінформована, вона може приймати інформовані рішення та вживати на їх основі пріоритезовані заходи.

4. Створити групу оперативного реагування на кіберзлочини. Добре підготована група оперативного реагування забезпечить виявлення інциденту на будь-якій ділянці бізнесу, оцінку ризику та доведення його до відома керівництва.

5. Навчання всіх співробітників – організації необхідна культура «інформованості про кіберзлочинність». Для цього потрібно передбачити у штаті персонал із відповідними знаннями, який зможе забезпечити навчання всіх співробітників для створення достатньої інформованості про ризик кіберзлочинності в організації.

6. Активна та прозора позиція організації стосовно злочинів з використанням комп'ютерних технологій – організація повинна активно переслідувати порушників та інформувати спільноту про загрози, факти порушень та заходи, які вживаються організацією.

## Кіберзлочинність – це не лише проблема IT

Зазвичай кіберзлочинність відносять до сфери IT, що викликає взаємне непорозуміння між співробітниками бізнес-підрозділів та спеціалістів із інформаційної безпеки.

Дані Всесвітнього огляду стану інформаційної безпеки у 2011 році, підготованого PwC, свідчать про те, що забезпечення кібербезпеки – це не лише питання технічного характеру, але й один із обов'язків бізнес-підрозділів.

На запитання про те, хто має нести загальну відповідальність за усунення загроз кібербезпеки, більше половини опитаних (67%) вказали директора з IT або директора по технологіях, і лише 13% назвали генерального директора або членів правління організації. Це значить, що незалежно від того, чи входить директор з IT до складу правління організації, чи ні, він не поділяє відповідальність з генеральним директором або правлінням в цілому.

Лише 20% респондентів заявили, що генеральний директор та члени правління обговорюють оцінку таких ризиків принаймні один раз на рік. 32% опитаних відповіли, що це обговорення проводиться за необхідності, у той час як 25% зазначили, що оцінка цих ризиків в організації взагалі не проводиться.

Ми очікуємо, що у майбутньому генеральні директори та члени правлінь організацій регулярно розглядатимуть питання, пов'язані з ризиком кіберзлочинності.

*36% організацій в Україні зіткнулися з економічними злочинами за останні 12 місяців*

# Огляд економічних злочинів в Україні

36% із 84 респондентів в Україні повідомили про те, що за останній рік вони зіткнулися принаймні з одним випадком економічного злочину. Цей показник є вищим, ніж у світі (34%), але нижчим порівняно з даними за 2009 рік (45%).

Ми можемо припустити, що на результати огляду за 2009 рік вплинула економічна рецесія, наслідком якої стало зростання кількості шахрайських дій.

Ми вважаємо, що зниження рівня шахрайства у 2011 році за даними українських організацій пояснюється неефективністю його виявлення, а не фактичним скороченням кількості таких випадків.

У контексті цього ми порівняли кількість випадків шахрайства, про які повідомили організації, які регулярно проводять оцінку ризиків, з даними організацій, які не проводять такої оцінки.

У результаті організації, які регулярно проводять оцінку ризиків, заявляють про більшу кількість зловживань та більшу частоту таких випадків.

Однак, ми очікуємо, що топ-менеджмент повинен бути інформований про економічні злочини. Так, у 2011 році топ-менеджмент виявився більше поінформованим про випадки зловживань у своїх організаціях порівняно з 2009 роком: лише 10% респондентів, які є представниками топ-менеджменту, повідомили про те, що не знали про випадки шахрайства у своїх організаціях (55% у 2009 році).

Для забезпечення ефективності діяльності організаціям необхідно приділяти більше уваги процедурам попередження шахрайства та управління ризиками шахрайства.

Організації, які проводять оцінку ризиків, відзначають більшу кількість випадків шахрайства і вищу їх частоту

### Статистика шахрайства за видами організацій

Більшість учасників огляду в Україні – це представники приватних (69%) та публічних організацій (24%).

Представники урядових, державних та неприбуткових організацій, які становлять 7% учасників огляду, відповіли, що не стикались із випадками зловживань за останній рік або їм невідомо про такі випадки.

Однак приватні компанії зіштовхуються із випадками економічних злочинів майже втричі частіше, ніж публічні організації. Найбільш поширеними видами зловживань у приватних компаніях є:

- незаконне привласнення майна (31%);
- корупція та хабарництво (29%);
- маніпуляції з фінансовою звітністю (14%).

Статистика для публічних компаній:

- незаконне привласнення майна (37%);
- корупція та хабарництво (21%);
- кіберзлочинність (16%).

**Рис. 2: Види шахрайства в Україні у 2009 та 2011 роках**


% респондентів, що зіткнулися з економічною злочинністю у 2009 та 2011 рр.

## З якими видами економічних злочинів стикаються організації в Україні?

Існує багато видів економічних злочинів, причому деякі з них більше поширені та зустрічаються систематично. У 2011 році найбільш поширеним видом економічних злочинів в Україні було незаконне присвоєння майна (73%), на другому місці – хабарництво та корупція (60%), на третьому – маніпуляції з фінансовою звітністю (30%).

Результати опитування свідчать про те, що українські компанії набагато більше страждають від хабарництва і корупції та недобросовісної конкуренції, ніж інші країни у Центральній та Східній Європі та світі (див. Таблицю 2).

Значна кількість інцидентів зловживань, про які повідомляють наші респонденти, також означає, що ці види зловживань не лише найбільш поширені, але й можуть бути виявлені легше, ніж інші види економічних злочинів.

Кількість випадків незаконного присвоєння майна та недобросовісної конкуренції зросла майже на 15% у порівнянні з 2009 роком. При цьому хабарництво і корупція та маніпуляції з фінансовою звітністю залишилися на тому ж рівні.

Це спонукає шахраїв розробляти все витонченіші схеми шахрайства, які можуть залишитися невиявленими. У наші дні шахраї мають широкий арсенал прийомів, у той час як спеціалісти з внутрішніх розслідувань лише починають розробляти механізми попередження та виявлення зловживань. Економічна рецесія призвела до того, що організації з небажанням інвестують у такі послуги, як внутрішній аудит або внутрішні фінансові розслідування.

## Чи має значення розмір організації?

Цього року результати опитування показують, що всі українські організації (незалежно від їх розміру) рівною мірою страждають від економічних злочинів.

**Таблиця 2: Види зловживань в Україні, за якими спостерігається значна відмінність від країн Центральної та Східної Європи та світу в 2011 році**

| | Хабарництво та корупція | Недобросовісна конкуренції |
|---|---|---|
| Україна | 60% | 23% |
| Центр.-Східна. Європа | 36% | 12% |
| Світ | 24% | 7% |

% від загальної кількості респондентів, які зіткнулися з випадками економічних злочинів за останні 12 місяців

**Таблиця 3: Зловживання в Україні в 2011 році з розбивкою за розміром організацій**

| | |
|---|---|
| До 200 співробітників | 27% |
| 201 –1 000 співробітників | 30% |
| 1 001 – 5 000 співробітників | 23% |
| Понад 5 000 співробітників | 20% |

% від загальної кількості респондентів, які зіткнулися з випадками економічних злочинів за останні 12 місяців

* У 2009 цей варіант відповіді не пропонувався

*Понад 40% респондентів очікують випадки корупції та хабарництва в Україні у наступні 12 місяців*

## Які галузі найбільше страждають від економічної злочинності?

Цього року в опитуванні представлені погляди представників понад 13 різних галузей. Фінансові послуги, роздрібна торгівля, виробництво споживчих товарів, промислове виробництво та професійні послуги представляють понад половину (63%) від загальної кількості учасників в Україні та світі.

Кожен другий респондент, що працює у секторі фінансових послуг, енергетики та гірничо-видобувної промисловості за останні 12 місяців зіштовхнувся із випадками економічних злочинів (див. Рисунок 3).

Ми порівняли факти економічної злочинності за галузями та відзначили зростання кількості таких випадків у 2011 році у галузі роздрібної торгівлі та виробництві споживчих товарів на 6%, а у секторі фінансових послуг – на 5%.

## Майбутні очікування

Незважаючи на зменшення за даними опитування рівня хабарництва та корупції на 9%, понад 40% респондентів з України очікують зіштовхнутись із ними протягом наступних 12 місяців. Крім того, провідні позиції в опитуванні серед очікуваних видів зловживань посідають порушення прав інтелектуальної власності (36%) та незаконне привласнення майна (35%).

За даним глобального опитування, організації очікують зростання випадків незаконного привласнення майна (34%), кіберзлочинності (26%) і хабарництва та корупції (23%).

**Таблиця 4: Види шахрайства, які очікують українські організації у майбутньому**

| | |
|---|---|
| Хабарництво та корупція | 42% |
| Порушення прав інтелектуальної власності | 36% |
| Незаконне привласнення майна | 35% |
| Маніпуляції з фінансовою звітністю | 25% |
| Кіберзлочинність | 25% |
| Недобросовісна конкуренція | 24% |
| Відмивання грошей | 17% |
| Податкове шахрайство | 14% |
| Торгівля інсайдерською інформацією | 12% |
| Промислове шпигунство | 10% |

% від загальної кількості респондентів

**Рис. 3: Зловживання за галузями економіки в Україні у 2011 році**


% респондентів, які зіткнулися з економічною злочинністю за останні 12 місяців

# *40% злочинів в Україні здійснює вище керівництво*

Найбільш типовий шахрай у всьому світі – це так званий «білий комірець».

Типовий суб'єкт економічних злочинів – це чоловік за тридцять років із вищою освітою, стійкою психікою та стабільною родиною.

## Портрет шахрая

Цього року організації у рівній мірі страждають від зловживань, скоєних як власними співробітниками, так і зовнішніми шахраями, при цьому з 2009 року число серйозних економічних злочинів, скоєних співробітниками, зросло на 22%.

**Таблиця 5: Суб'єкти зловживань**

| | 2011р. | 2009р. |
|---|---|---|
| Співробітники | 50% | 28% |
| Зовнішні особи | 47% | 72% |
| Невідомо | 3% | 0% |

% від загальної кількості респондентів, які зіткнулися з випадками економічних злочинів

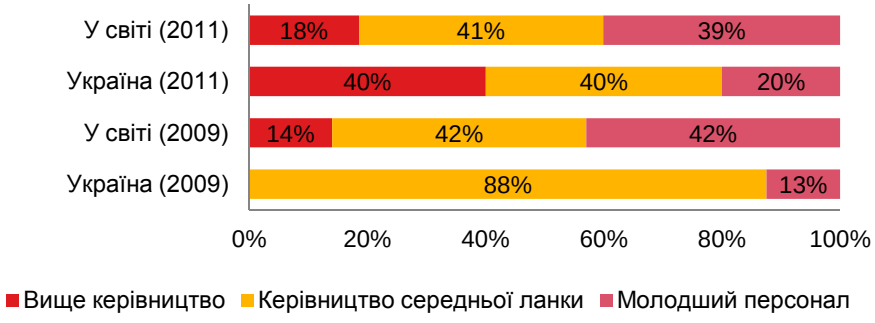
Більшість посадових шахраїв в Україні – представники вищої (40%) та середньої (40%) керівної ланки. У світі 60% внутрішніх злочинів скоює керівництво середньої ланки та звичайні співробітники.

Типовий суб'єкт економічних злочинів в Україні – це чоловік із вищою освітою у віці 31-50 років, який працює в організації 3-10 років.

Як в Україні, так і у світі основний суб'єкт зловживань – це клієнт (43% в Україні та 35% у світі). Крім того, поширені зовнішні винуватці зловживань – це агенти та посередники (14%) та постачальники (14%).

Один з найважливіших інструментів попередження шахрайства є підхід «знати з ким ви маєте ділові стосунки». Тому важливим елементом програм із мінімізації ризиків стає аналіз клієнтів, постачальників та агентів.

**Рис. 4: Основні суб'єкти посадових злочинів в Україні та світі**




% респондентів, які зіткнулися з економічною злочинністю у 2009 та 2011 роках

# *Збитки більшості організацій України, які зіткнулися з економічною злочинністю за останні 12 місяців, склали в середньому до 5 млн. доларів США*

## Скільки організаціям коштує шахрайство?

Більшість респондентів, які зіткнулися з економічною злочинністю за останні 12 місяців, оцінюють збитки до 5 млн. доларів США. Найдорожчими для організацій виявилися три найпоширеніших види зловживань, а саме, незаконне присвоєння майна, хабарництво та корупція і маніпуляції з фінансовою звітністю. У 2011 році помічене суттєве збільшення частоти цих видів зловживань та збитків від них порівняно з 2009 роком.

Випадки шахрайства, які скоюють співробітники, зазвичай призводять до більших збитків, ніж при зловживаннях зовнішніх сторін, наприклад, клієнтів, постачальників або агентів.

Вартість злочину зростає з віком шахрая. Так, найдорожчі злочини (5-100 млн. дол. США) були скоєні особами, віком понад 50 років.

## Вартість супутнього збитку

Фінансові збитки – лише один з аспектів збитків, які несуть організації від шахрайської діяльності, і часто – далеко не найвагоміший. Супутній збиток та його негативний вплив на репутацію та бренд, вартість акцій, настрої у колективі, стосунки з партнерами призводять до значних збитків у багатьох видах бізнесу.

Із тих організацій, які зіткнулись з економічними злочинами цього року, 23% повідомляють про погіршення настроїв у колективі, 17% – про шкоду для бренду організації та 13% – про шкоду для ділових стосунків та стосунків із регуляторами.

Хоча ці цифри відповідають результатам у світі, у 2011 році супутні збитки значно нижчі порівняно з 2009 роком. У 2009 році про погіршення настроїв у колективі повідомило 34% респондентів, про погіршення відносин з регулятором – 34%, з бізнес-партнерами – 28%, та про шкоду для бренду – 14%.

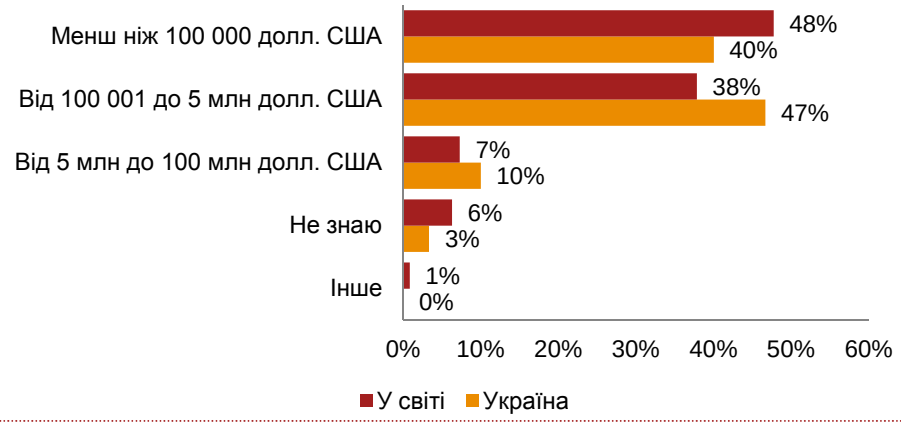
**Таблиця 6: Порівняння супутніх збитків в Україні у 2009 та 2011 роках**

| | 2011р. | 2009 р. |
|---|---|---|
| Стосунки з регуляторами | 13% | 34% |
| Настрої у колективі | 23% | 34% |
| Стосунки з бізнес-партнерами | 13% | 28% |
| Репутація/бренд | 17% | 14% |
| Ціна акцій | 7% | 0% |

% від загальної кількості респондентів, які зіткнулися з випадками економічних злочинів

Низькі показники супутніх збитків у 2011 році виявилися неочікуваними. Зловживання розглядаються як невід'ємна складова бізнесу в Україні, що призводить до формування замкнутого кола: організації виправдовують потенційні зловживання і таким чином підвищують їх ймовірність.

**Рис. 5: Фінансові збитки від економічних злочинів в Україні та у світі у 2011 році**




% респондентів, які зіткнулися з економічною злочинністю за останні 12 місяців

## Як організації виявляють шахрайство?

Виявлення шахрайства передбачає усі методи, які використовуються організацією для встановлення факту економічного злочину. У 2011 році українські респонденти повідомили про такі найефективніші способи виявлення шахрайства.

В Україні більшість злочинів виявляє Служба корпоративної безпеки організації, і лише 6% зловживань виявляє Служба внутрішнього аудиту. Результати всесвітнього огляду свідчать про цілком іншу ситуацію.

Також слід зазначити, що 27% респондентів не знали про методи виявлення шахрайства порівняно з 10% респондентів у світі. Це значить, що організації в інших країнах підтримують високий рівень поінформованості про програми протидії шахрайству.

Більше половини учасників опитування (54%) не використовують систему анонімного інформування. Однак 82% респондентів, які використовують таку систему, вважають її ефективною.

## Які заходи вживають організації проти шахраїв?

73% співробітників, які скоїли шахрайство, були звільнені


проти них були подані цивільні позови, включаючи вимогу про відшкодування заподіяної шкоди. Слід зазначити, що організації не вжили жодних заходів проти шахраїв у 20% випадків. У 2009 році цей показник склав лише 3%, і ця статистика викликає занепокоєння.

Так, в деяких організаціях спостерігається відсутність занепокоєння або бажання активно протидіяти шахрайству. Виникає запитання, чи варто утримувати шахрая в організації та наражатися на ризик повторних зловживань? Ми вважаємо, що організації мають непримиренно ставитися до випадків зловживань та вживати жорстких заходів проти шахраїв із залученням офіційних органів.

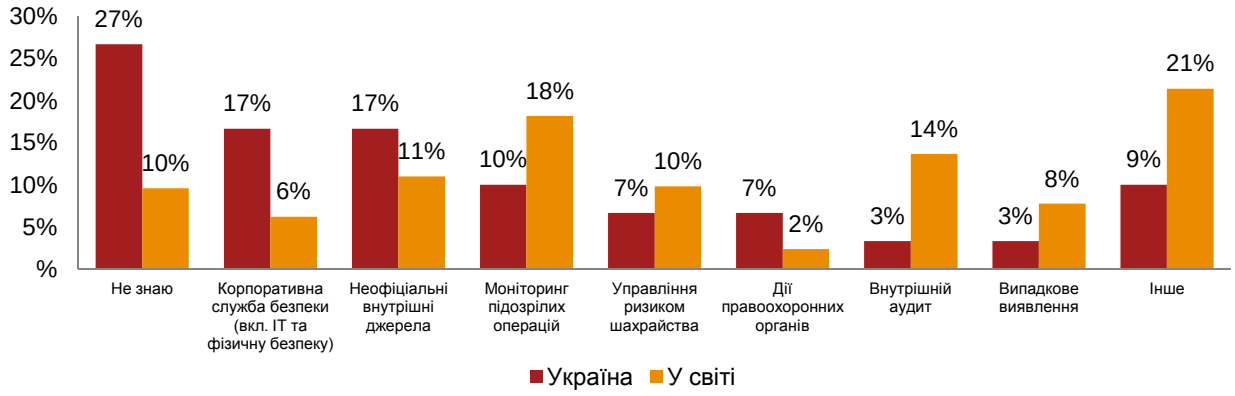
Українськими організаціями було вжито таких заходів проти зовнішніх шахраїв:

- інформування правоохоронних органів (71%);
- подача цивільних позовів, включаючи вимоги про відшкодування збитків (64%);
- припинення ділових стосунків (57%);
- інформування відповідних органів нагляду (43%).

Ці показники відповідають світовій статистиці, а також результатам огляду за 2009 рік.

Насторожує факт, що 43% респондентів заявили про те, що їх організації продовжують підтримувати ділові стосунки з контрагентами, які скоїли шахрайство. Цей факт піднімає фундаментальні питання з приводу корпоративної культури таких організацій.

**Рис. 6: Методи виявлення шахрайства, які застосовувалися в Україні та світі у 2011 році**




% респондентів, які зіткнулися з економічною злочинністю за останні 12 місяців

# Термінологія

Враховуючи різноманітність видів економічних злочинів, передбачених законодавством різних країн, для того щоб допомогти респондентам у заповненні анкети, у межах цього огляду ми визначили такі їх категорії

### *Відмивання грошей*

Дії, націлені на узаконювання доходів від злочинної діяльності з приховуванням справжнього джерела їх походження.

### *Економічний злочин або шахрайство*

Навмисний обман з метою розкрадання грошових коштів, майна або законних прав.

### *Забезпечення стійкого розвитку*

Діяльність із торгівлі квотами на викид вуглецю (купівля або продаж квот), участь у проектах, в межах яких здійснюється взаємне зарахування квот на викид вуглецю.

### *Корупція та хабарництво (включаючи рекетирство та вимагання)*

Незаконне використання службового становища з метою отримання особистої вигоди з порушенням посадових обов'язків, включаючи обіцянку економічних пільг або надання іншої підтримки, використання загроз та шантажу. Також стосується приймання таких заохочень.

### *Маніпуляції з фінансовою звітністю*

Фінансова звітність та інша документація викривляється або представлена таким чином, що не відображає справжню вартість або фактичні фінансові результати організації, включаючи маніпуляції з обліковими записами, зловживання з позичковими коштами/залученням фінансування, незаконне проведення кредитних та несанкціонованих операцій, нестандартних торгових операцій.

### *Механізм реагування на злочини з використанням комп'ютерних технологій*

Зазвичай, до цієї категорії відносяться розроблені організацією засоби попередження, виявлення та розслідування злочинів з використанням комп'ютерних технологій, співробітництво з експертами з фінансових розслідувань, медійні та PR плани.

### *Недобросовісна конкуренція*

Це методи, які перешкоджають або підривають конкуренцію на ринку, включаючи картельні угоди зі змовою з конкурентами (наприклад, ціноутворення, шахрайство в ході торгів та розподіл ринку) та зловживання монопольним становищем.

### *Незаконне присвоєння майна (включаючи розтрати/ розкрадання з боку співробітників)*

Крадіжка майна (включаючи грошові кошти або ТМЦ та обладнання) керівництвом, іншими довіреними особами або співробітниками в особистих корисливих цілях.

### *Оцінка ризику шахрайства*

Оцінка ризику шахрайства використовується для перевірки чи організація проаналізувала такі аспекти:

(i) Ризики шахрайства, з якими вона зіштовхується;

(ii) Оцінка найсуттєвіших ризиків (тобто оцінка ризиків на предмет важливості та ймовірності виникнення);

(iii) Ідентифікація та оцінка механізмів контролю, які функціонують (за наявності), що використовуються для мінімізації ключових ризиків;

(iv) Оцінка загальних програм та механізмів контролю для попередження шахрайства в організації;

(v) Заходи з усунення прогалин у системі контролю.

### *Порушення прав інтелектуальної власності (включаючи торгові марки, патенти, контрафактні товари та послуги)*

До цієї категорії входить підробка та розповсюдження підроблених товарів шляхом порушення патентів або авторського права, а також створення фальшивих купюр та монет із наміром їх використання у якості справжніх.

### *Топ-менеджер*

Топ-менеджер (наприклад, Генеральний директор, Керуючий директор або Виконавчий директор) – це особа, відповідальна за прийняття рішень в організації.

### *Торгівля інсайдерською інформацією*

Торгівля інсайдерською інформацією зазвичай стосується придбання або продажу цінних паперів шляхом порушення фідуціарних обов'язків та інших довірчих стосунків внаслідок наявності суттєвої непублічної інформації про цінні папери. Такі порушення можуть також включати навмисне розкриття такої інформації, торгівлю цінними паперами особою, яка має секретну інформацію, та торгівлю цінними паперами особами, які незаконно заволоділи такою інформацією.

### *Шахрайство, пов'язане зі стійким розвитком*

Шахрайство, пов'язане зі стійким розвитком (див. забезпечення стійкого розвитку), включаючи ринки торгівлі квотами на викиди вуглецю, екологічні позови або офіційні заяви.

### *Шпигунство*

Шпигунство – це дія або практика використання шпигунів для отримання секретної інформації або використання технологій для того, щоби діяти від імені організації.

# Контакти

**PwC** допомагає організаціям і приватним особам досягати поставлених цілей. Міжнародна мережа фірм PwC працює у 158 країнах, де 169 000 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.

### Форензік – фінансові розслідування

Найбільша у світі практика з надання послуг в області фінансових розслідувань (форензік), яка нараховує 1 400 професіональних консультантів у 63 країнах, дозволяє PwC використовувати їхні експертні знання та величезний практичний досвід для вирішення складних ситуацій, в яких опинилися компанії, що здійснюють свою діяльність у різних галузях у численних юрисдикціях.

Наша практика з надання послуг в області фінансових розслідувань у Центральній та Східній Європі, яка динамічно розвивається, нараховує понад 70 професійних консультантів, включаючи бухгалтерів, економістів і спеціалістів у сфері інформаційних технологій.

Ми надаємо наступні послуги:

- Корпоративні розслідування
- Управління ризиками шахрайства
- Підтримка у ході господарських спорів
- Міжнародний арбітраж
- Спори з акціонерами та у зв'язку з угодами злиття та поглинання, а також пов'язані з цим розслідування
- Технологічні рішення для проведення фінансових розслідувань
- Послуги з виявлення шахрайства в області інтелектуальної власності
- Консультаційні послуги в області управління ліцензуванням
- Консультаційні послуги у зв'язку зі страховими позовами
- Протидія легалізації доходів, отриманих незаконним шляхом
- Консультації в рамках інвестиційних проектів
- Підтримка під час розслідувань, які проводяться регулюючими органами США, і в судових розглядах щодо цінних паперів

### Експерти PwC в області форензік-послуг


**Борис Краснянський**

Керуючий партнер

boris.krasnyansky@ua.pwc.com

**Джон Вілкінсон**

Партнер

Лідер форензік-послуг у Центральній та Східній Європі, Російській Федерації та СНД

john.wilkinson@ru.pwc.com

**Геннадій Чуприков**

Старший менеджер

Керівник групи форензік-послуг в Україні

gennadiy.chuprykov@ua.pwc.com

**Вікторія Цицак**

Менеджер

Форензік-послуги в Україні

victoriya.tsytsak@ua.pwc.com