



МІНІСТЕРСТВО  
ФІНАНСІВ  
УКРАЇНИ

# Планування діяльності з внутрішнього аудиту





# ПЛАНУВАННЯ ДІЯЛЬНОСТІ З ВНУТРІШНЬОГО АУДИТУ

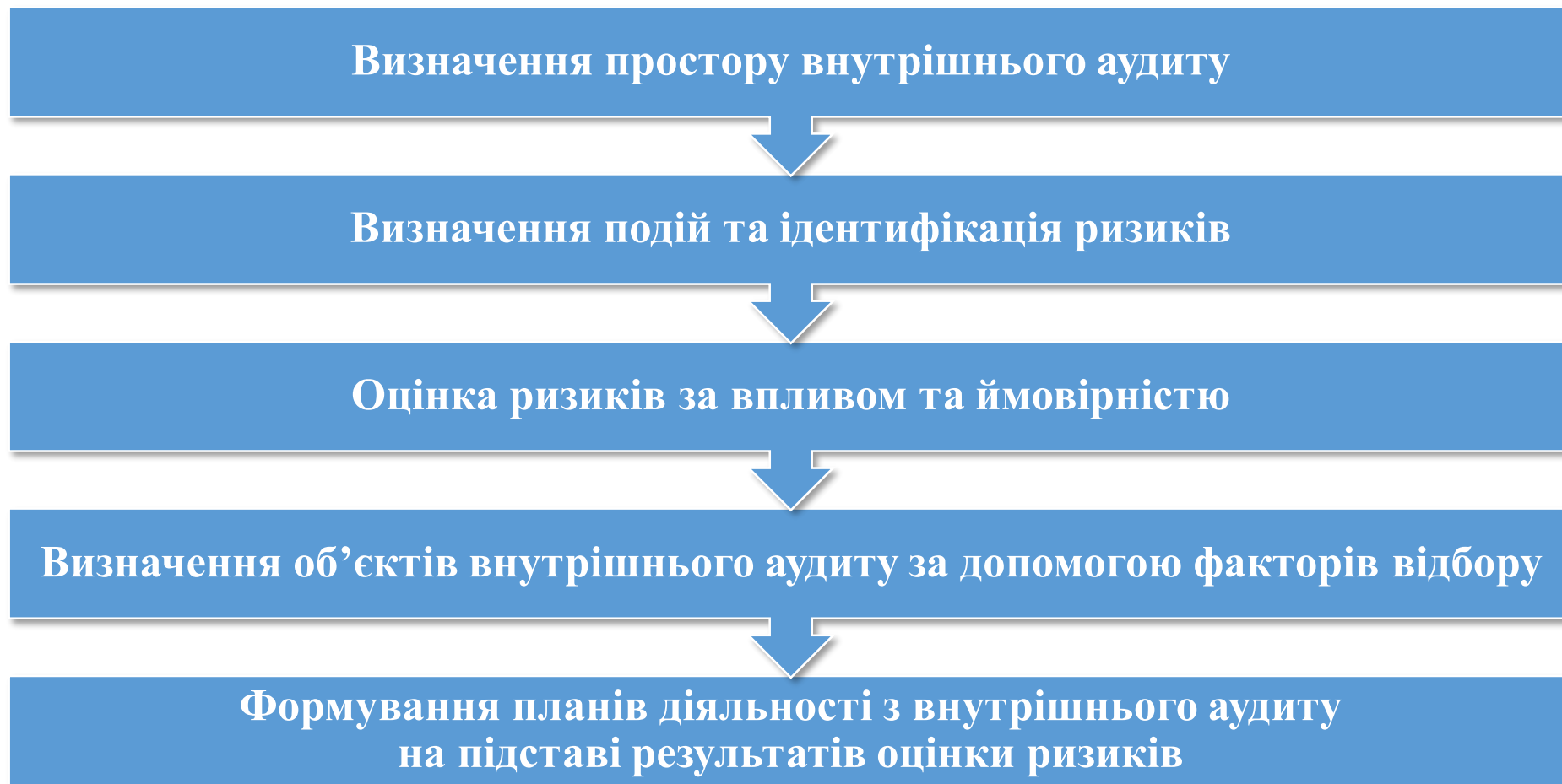
Підрозділ внутрішнього аудиту забезпечує:

- 1. визначення простору внутрішнього аудиту, який має бути формалізований та задокументований шляхом ведення бази даних та її підтримання в актуальному стані
- 2. формування планів на підставі результатів оцінки ризиків з метою визначення пріоритетів роботи підрозділу внутрішнього аудиту, що мають враховувати стратегію (пріоритети) та цілі діяльності державного органу
- 3. проведення оцінки ризиків не рідше одного разу на рік (оформлюється документально)
- 4. розробку внутрішніх документів з питань здійснення внутрішнього аудиту, що врегульовують підходи до складання та ведення бази даних, організації, проведення та документування ідентифікації й оцінки ризиків для планування діяльності з внутрішнього аудиту, визначення факторів відбору для здійснення планових внутрішніх аудитів та частоти їх здійснення щодо кожного об'єкта внутрішнього аудиту

**Стандарт 7 «Планування діяльності з внутрішнього аудиту», пункт 4 Стандарта 1 «Завдання, права та обов'язки»**  
(наказ Мінфіну від 04.10.2011 № 1247)



# ПЛАНУВАННЯ ДІЯЛЬНОСТІ З ВНУТРІШНЬОГО АУДИТУ



*Методичний посібник «Ризик-орієнтоване планування діяльності з внутрішнього аудиту»  
([tof.gov.ua/Діяльність/Розвиток державного внутрішнього фінансового контролю/Методичні посібники щодо ДВФК](http://tof.gov.ua/Діяльність/Розвиток_державного_внутрішнього_фінансового_контролю/Методичні_посібники_щодо_ДВФК))*



# ВИЗНАЧЕННЯ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

*ціль етапу: визначити та описати потенційні об'єкти, які окремо можна дослідити під час здійснення внутрішнього аудиту*



**Простір аудиту** – загальна сфера застосування функції внутрішнього аудиту (сукупність об'єктів внутрішнього аудиту, а також підприємств, установ та організацій, на яких можуть здійснюватися внутрішні аудити)



Об'єктом внутрішнього аудиту є діяльність державного органу, його територіальних органів, підприємств (у тому числі суб'єктів господарювання, державна частка у статутному капіталі яких перевищує 50 відсотків чи становить величину, яка забезпечує державі право вирішального впливу на господарську діяльність таких суб'єктів господарювання), установ та організацій, що належать до сфери його управління, в повному обсязі або з окремих питань (на окремих етапах), та заходи, що здійснюються керівниками таких органів, підприємств, установ та організацій для забезпечення ефективного функціонування системи внутрішнього контролю (дотримання принципів законності та ефективного використання бюджетних коштів та інших активів, досягнення результатів відповідно до встановленої мети, виконання завдань, планів і вимог щодо їх діяльності) (пункт 2 Порядку № 1001)



## ВИЗНАЧЕННЯ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

*ціль етапу: визначити та описати потенційні об'єкти, які окремо можна дослідити під час здійснення внутрішнього аудиту*

Простір внутрішнього аудиту структурується за:

горизонтальний принцип  
розподілу об'єктів внутрішнього  
аудиту

- напрямками (сферами) діяльності державного органу або їх частинами;
- бюджетними програмами;
- адміністративними послугами;
- контрольно-наглядовими функціями;
- функціональними процесами;
- загальними процесами

вертикальний принцип розподілу  
об'єктів внутрішнього аудиту

- структурними підрозділами державного органу;
- територіальними органами;
- підприємствами, установами та організаціями, які належать до сфери управління державного органу



## ВИЗНАЧЕННЯ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

*ціль етапу: визначити та описати потенційні об'єкти, які окремо можна дослідити під час здійснення внутрішнього аудиту*

Для розподілу простору внутрішнього аудиту за горизонтальним та вертикальним принципами використовуються документальні джерела інформації, зокрема:

- законодавчі та нормативно-правові акти, що регулюють діяльність державного органу, а також установ, підприємств, організацій, які належать до сфери його управління
- стратегічні та операційні плани (річні, піврічні, квартальні)
- внутрішні документи установи (організаційна структура, положення про структурні підрозділи, посадові інструкції, відповідні порядки та регламенти)
- паспорти бюджетних програм, фінансові плани державних підприємств, звітність (річна та періодична фінансова, інша нефінансова звітність)
- аудиторські звіти підрозділу внутрішнього аудиту та акти/звіти зовнішніх контролюючих органів



## ВИЗНАЧЕННЯ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

*ціль етапу: визначити та описати потенційні об'єкти, які окремо можна дослідити під час здійснення внутрішнього аудиту*

Проведення консультацій підрозділом внутрішнього аудиту з керівником державного органу та відповідальними за діяльність особами

**В рамках визначення простору внутрішнього аудиту, його актуалізації з'ясовуються:**

- питання щодо достатності/недостатності або надмірного рівня деталізації об'єктів внутрішнього аудиту, визначених підрозділом внутрішнього аудиту;
- питання, які цікавлять керівництво, на які слід звернути увагу підрозділу внутрішнього аудиту;
- ролі структурних підрозділів в досягненні визначених цілей





## ВИЗНАЧЕННЯ ПОДІЙ ТА ІДЕНТИФІКАЦІЯ РИЗИКІВ

*ціль етапу: правильність формування аудиторської думки про ризики, пов'язані з відповідними об'єктами внутрішнього аудиту*

Підходи до ідентифікації підрозділом внутрішнього аудиту ризиків:

1) у разі запровадження у діяльності державного органу системи управління ризиками на послідовній та структурованій основі підрозділ внутрішнього аудиту, зокрема:

досліджує внутрішні документи з питань управління ризиками, своєчасність надання керівництву установи інформації щодо з питань управління ризиками

вивчає реєстри ризиків з метою розуміння визначених ризиків, досліджує повноту виявлення відповідальними за діяльність особами ризиків

з'ясовує прийнятий керівництвом **«ризик-апетит»**, досліджує запроваджені заходи контролю з метою зменшення ризиків, оцінює їх достатність (до якого рівня заходи контролю забезпечують зниження залишкових ризиків та як співвідносяться залишкові ризики та «ризик-апетит»)

**«ризик-апетит»** – рівень ризику, що приймається керівництвом державного органу як несуттєвий;

**невід'ємний ризик** – рівень ризику до вжиття керівництвом та відповідальними за діяльність особами заходів контролю;

**залишковий ризик** – рівень ризику після вжиття керівництвом та відповідальними за діяльність особами заходів контролю





## ВИЗНАЧЕННЯ ПОДІЙ ТА ІДЕНТИФІКАЦІЯ РИЗИКІВ

*ціль етапу: правильність формування аудиторської думки про ризики, пов'язані з відповідними об'єктами внутрішнього аудиту*

Підходи до ідентифікації підрозділом внутрішнього аудиту ризиків:

1) у разі запровадження у діяльності державного органу системи управління ризиками на послідовній та структурованій основі підрозділ внутрішнього аудиту, зокрема:

аналізує обрані відповідальними за діяльність особами способи реагування на ризики, порівнює визначені способи реагування на ризики з судженням внутрішніх аудиторів

аналізує ефективність запроваджених заходів контролю щодо їх впливу на залишкові ризики

виявити неідентифіковані ризики та залишкові ризики, які, незважаючи на запроваджені заходи контролю, можуть залишатися високими

задокументувати виявлені та оцінені підрозділом внутрішнього аудиту ризики, які не було ідентифіковано відповідальними за діяльність особами, та залишкові ризики



## ВИЗНАЧЕННЯ ПОДІЙ ТА ІДЕНТИФІКАЦІЯ РИЗИКІВ

*ціль етапу: правильність формування аудиторської думки про ризики, пов'язані з відповідними об'єктами внутрішнього аудиту*

Підходи до ідентифікації підрозділом внутрішнього аудиту ризиків:

2) у разі відсутності у державному органі формалізованої системи управління ризиками підрозділ внутрішнього аудиту, зокрема:



визначає події, які приводять до виникнення ризиків

ідентифікує та оцінює ризики з точки зору ступеню їх впливу та ймовірності виникнення

враховує думку керівництва та посадових осіб державного органу, які безпосередньо відповідають за функції, процеси, що охоплюються внутрішнім аудитом



## ВИЗНАЧЕННЯ ПОДІЙ ТА ІДЕНТИФІКАЦІЯ РИЗИКІВ

*ціль етапу: правильність формування аудиторської думки про ризики, пов'язані з відповідними об'єктами внутрішнього аудиту*

**Для визначення ризиків підрозділ внутрішнього аудиту аналізує документи, зокрема:**

- інформацію про типові/системні порушення та недоліки, встановлені за результатами попередніх внутрішніх аудитів
- повідомлення про проблемні питання та ризики у діяльності структурних підрозділів державного органу, підприємств, установ та організацій, що належать до сфери його управління
- інформацію зі ЗМІ, звернень народних депутатів, державних органів, правоохоронних органів, зовнішніх контролюючих органів, скарг фізичних та юридичних осіб
- інформацію щодо звітності (наприклад, із фінансової та бюджетної звітності, звітів про виконання паспорту бюджетної програми та фінансових планів)
- нормативно-правові акти, які регулюють діяльність державного органу
- внутрішні документи (наприклад, положення про структурні підрозділи, порядки та регламенти)
- стратегічні плани, річні, піврічні, квартальні плани
- щорічні звіти про діяльність державного органу
- аудиторські звіти за результатами проведення попередніх внутрішніх аудитів
- акти/звіти контрольних заходів, проведених зовнішніми контролюючими органами (Рахунковою палатою, органами державного фінансового контролю тощо)



## ВИЗНАЧЕННЯ ПОДІЙ ТА ІДЕНТИФІКАЦІЯ РИЗИКІВ

*ціль етапу: правильність формування аудиторської думки про ризики, пов'язані з відповідними об'єктами внутрішнього аудиту*

Проведення консультацій підрозділом внутрішнього аудиту з керівником державного органу та відповідальними за діяльність особами

### **В рамках ідентифікації та оцінки ризиків з'ясовуються:**

- проблемні питання та ризики у діяльності структурних підрозділів державного органу, а також підприємств, установ та організацій, що належать до сфери його управління;
- питання щодо ідентифікованих та оцінених підрозділом внутрішнього аудиту ризиків (у разі не запровадження належної системи управління ризиками);
- прийнятий керівництвом рівень ризику («ризик-апетит»);
- правильність судження підрозділу внутрішнього аудиту про невід'ємний рівень ризику;
- питання щодо вжитих керівництвом та відповідальними за діяльність особами заходів щодо системного управління ризиками, їх вплив на рівень залишкового ризику



# ВИЗНАЧЕННЯ ПОДІЙ ТА ІДЕНТИФІКАЦІЯ РИЗИКІВ

*ціль етапу: правильність формування аудиторської думки про ризики, пов'язані з відповідними об'єктами внутрішнього аудиту*

Ризики					
Операційні	ІТ-системи та зв'язок	Законодавчі	Фінансові	Кадрові	Репутаційні
Приклади подій, що створюють ризики					
невиконання функцій, процесів, операцій; відсутність/недостатність контролю за реалізацією процесу, операції; втрата матеріально-технічного обладнання	недоступні або недостовірні дані; вірусні атаки на основне програмне забезпечення; знищення найбільш важливих облікових записів або відсутність до них доступу; несанкціонований виток чутливої інформації	недотримання вимог законодавства; відсутність, суперечність або нечітка регламентація положень законодавства; неналежна претензійна-позовна діяльність; судові позови, порушення контрактів (угод); зупинення важливої діяльності	зменшення фінансування; наявність фактів корупції та шахрайства, нецільового та неефективного використання державних ресурсів; відсутність коштів на здійснення операцій; штрафи, пені; втрата коштів чи активів	втрата кваліфікованих працівників (звільнення, вихід на пенсію); не проведення заходів з підвищення кваліфікації персоналу, тренінгів, семінарів; наявність вакансій впродовж тривалого часу	негативне висвітлення діяльності державного органу у ЗМІ; втрата довіри зі сторони зацікавлених сторін через операційні недоліки; незадоволення працівників (скарги, звернення, у тому числі на гарячі телефонні лінії); негативна інформація від державних органів, правоохоронних органів



## ВИЗНАЧЕННЯ ПОДІЙ ТА ІДЕНТИФІКАЦІЯ РИЗИКІВ

*ціль етапу: правильність формування аудиторської думки про ризики, пов'язані з відповідними об'єктами внутрішнього аудиту*



Для внутрішнього аудитора важливо встановити особу, яка найбільш зацікавлена в управлінні відповідним ризиком («власника ризика»)





## ВИЗНАЧЕННЯ ПОДІЙ ТА ІДЕНТИФІКАЦІЯ РИЗИКІВ

*ціль етапу: правильність формування аудиторської думки про ризики, пов'язані з відповідними об'єктами внутрішнього аудиту*

### Принципи формулювання ризиків



слід уникати визначення ризиків, які не мають впливу на цілі

слід уникати визначення ризиків, які є зворотним формулюванням цілей

не слід визначати ризики як наслідки подій

слід враховувати причину виникнення ризику та можливий його вплив на цілі (причинно-наслідковий зв'язок)



# ВИЗНАЧЕННЯ ПОДІЙ ТА ІДЕНТИФІКАЦІЯ РИЗИКІВ

*ціль етапу: правильність формування аудиторської думки про ризики, пов'язані з відповідними об'єктами внутрішнього аудиту*

Назва процесу: захист інформації в інформаційних системах (ІТ-безпека)

Ціль процесу: забезпечення захисту персональних даних фізичних осіб, розміщених у базі даних

Формулювання ризику		Пояснення
Дані фізичних осіб будуть незахищені	X	Ризик сформульований як зворотний від цілі
Виток персональних даних фізичних осіб	X	Відсутній причинно-наслідковий зв'язок
Виникнення помилок у роботі бази даних	X	Ризик не має впливу на ціль
Розкриття даних третім особам внаслідок несанкціонованого доступу до бази даних, що призведе до витоку персональних даних	✓	Це ризик, який можна зменшити, зокрема шляхом застосування додаткових заходів захисту інформації
Зміна або знищення даних внаслідок хакерських та вірусних атак, що призведе до втрати цілісності персональних даних	✓	Це ризик, яким можна керувати, зокрема шляхом застосування більш досконалих технологій та процедур реагування на загрози, а також навчання персоналу
Неавторизоване управління базою даних внаслідок надання доступу до даних іншим суб'єктам відносин, пов'язаних із персональними даними, що може призвести до втрати конфіденційної інформації	✓	Це ризик, який можна зменшити, зокрема шляхом створення додаткових умов для захисту інформації



# ОЦІНКА РИЗИКІВ ЗА ВПЛИВОМ ТА ЙМОВІРНІСТЮ

*ціль етапу: визначення підрозділом внутрішнього аудиту найбільш ризикових об'єктів внутрішнього аудиту*

## Приклади критеріїв впливу

Рівень (бал)	Фінансовий вплив	Кадровий вплив	Операційний вплив	Репутаційний вплив
Низький (1)	Фінансово-матеріальний вплив нижче 100 тис. грн	Незапланована відсутність (хвороба тощо) деяких ключових працівників у одному підрозділі може призвести до затримки у роботі цього підрозділу	Обмежене або мінімальне зниження спроможностей може заважати продовженню виконання завдань та функцій за одним напрямом діяльності. Швидке відновлення у роботі	Некомпетентність (неналежне управління або суттєве порушення вимог законодавства) можуть призвести до зниження довіри з боку громадськості на місцевому рівні. Період відновлення довіри є коротким
Середній (2)	Фінансово-матеріальний вплив вище 100 тис. грн, але нижче 500 тис. грн	Незапланована відсутність (хвороба тощо) деяких ключових працівників у одному підрозділі може призвести до суттєвих збоїв у роботі цього підрозділу	Суттєве зниження/втрата спроможностей може заважати продовженню виконання завдань та функцій за одним/декількома напрямками діяльності. Швидке відновлення у роботі	Некомпетентність (неналежне управління або несистемні факти шахрайства/корупції у невеликих масштабах) можуть призвести до зниження довіри з боку громадськості на центральному рівні. Період відновлення довіри є коротким або помірним
Високий (3)	Фінансово-матеріальний вплив вище 500 тис. грн, але нижче 1 млн грн	Незапланована відсутність (хвороба тощо) більшості ключових працівників у одному підрозділі може призвести до значних збоїв у роботі цього підрозділу	Значне зниження/втрата спроможностей може заважати продовженню виконання завдань та функцій за двома і більше напрямками діяльності. Повільне відновлення у роботі	Некомпетентність (неналежне управління або системні факти шахрайства/корупції) можуть призвести до різкого зниження довіри з боку громадськості або важливих партнерів на центральному та міжнародному рівні. Період відновлення довіри є помірним
Дуже високий (4)	Значний фінансово-матеріальний вплив вище 1 млн грн	Серйозні травми, загибель працівника	Відсутність можливості продовжувати звично виконувати завдання та функції. Повсюдний збій за всіма напрямками діяльності. Суттєва втрата спроможностей. Повільне відновлення у роботі	Некомпетентність (неналежне управління або існування фактів шахрайства/корупції у великих масштабах) може призвести до втрати довіри з боку громадськості та важливих партнерів на центральному та міжнародному рівні. Період відновлення довіри є тривалим



# ОЦІНКА РИЗИКІВ ЗА ВПЛИВОМ ТА ЙМОВІРНІСТЮ

*ціль етапу: визначення підрозділом внутрішнього аудиту найбільш ризикових об'єктів внутрішнього аудиту*

## Приклади критеріїв ймовірності

Рівень	Критерії ймовірності настання ризику	Бал
Рідко/майже не можливо	Ймовірність виникнення дуже низька (0-24 %)	1
Малоймовірно	Ймовірність виникнення віддалена (25-50 %)	2
Можливо	Ймовірність виникнення ризику впродовж 1-2 років (51-74 %)	3
Часто/очікується	Ризик існує або очікується (75-100 %)	4



# ОЦІНКА РИЗИКІВ ЗА ВПЛИВОМ ТА ЙМОВІРНІСТЮ

*ціль етапу: визначення підрозділом внутрішнього аудиту найбільш ризикових об'єктів внутрішнього аудиту*

Матриця оцінки ризиків						
Рівень (бал)			ЙМОВІРНІСТЬ			
			Рідко/майже не можливо	Малоймовірно	Можливо	Часто/ очікується
			1	2	3	4
ВПЛИВ	Низький	1	Низький (а) (1)	Низький (а) (2)	Низький (а) (3)	Середній (я) (4)
	Середній	2	Низький (а) (2)	Середній (я) (4)	Середній (я) (6)	Високий (а) (8)
	Високий	3	Низький (а) (3)	Середній (я) (6)	Високий (а) (9)	Дуже високий (а) (12)
	Дуже високий	4	Середній (я) (4)	Високий (а) (8)	Дуже високий (а) (12)	Дуже високий (а) (16)

Ідентифікація та оцінка ризиків проводиться у взаємопов'язаний спосіб

За результатами формується **реєстр ідентифікованих та оцінених ризиків**

*(містить інформацію щодо назви ризику, результатів оцінки за впливом та ймовірністю, загальної оцінки ризику)*



## ОЦІНКА РИЗИКІВ ЗА ВПЛИВОМ ТА ЙМОВІРНІСТЮ

*ціль етапу: визначення підрозділом внутрішнього аудиту найбільш ризикових об'єктів внутрішнього аудиту*

Відмінність між процесом управління ризиками у діяльності державного органу та процесом оцінки ризиків підрозділом з внутрішнього аудиту

**Управління ризиками у діяльності державного органу – елемент системи внутрішнього контролю**

Діяльність з управління ризиками належить до повноважень (відповідальності) керівництва державного органу/відповідальних за діяльність осіб

**Оцінка ризиків підрозділом внутрішнього аудиту – етап планування діяльності з внутрішнього аудиту (належить до повноважень підрозділу внутрішнього аудиту)**

Результати оцінки ризиків слугують базою для формування планів





## ОЦІНКА РИЗИКІВ ЗА ВПЛИВОМ ТА ЙМОВІРНІСТЮ

*ціль етапу: визначення підрозділом внутрішнього аудиту найбільш ризикових об'єктів внутрішнього аудиту*

Відмінність між процесом управління ризиками у діяльності державного органу та процесом оцінки ризиків підрозділом внутрішнього аудиту

**Управління ризиками у діяльності державного органу (як елемент системи внутрішнього контролю):**

- ідентифікація та оцінка невід'ємних ризиків керівництвом та відповідальними за діяльність особами;
- визначення способів реагування на ризики;
- розробка та впровадження заходів контролю для впливу на ризики

**Оцінка ризиків підрозділом внутрішнього аудиту (як етап планування діяльності з внутрішнього аудиту):**

- надання керівництву та відповідальним за діяльність особам власної думки щодо повноти визначення ними невід'ємних ризиків, доцільності та дієвості обраних способів реагування на ризики, ефективності розроблених заходів контролю для впливу на ризики;
- виявлення та оцінка ризиків, які не було ідентифіковано відповідальними за діяльність особами, та залишкових ризиків

**Внутрішні аудитори мають дотримуватися принципів незалежності та об'єктивності!!!**



## ОЦІНКА РИЗИКІВ ЗА ВПЛИВОМ ТА ЙМОВІРНІСТЮ

*ціль етапу: визначення підрозділом внутрішнього аудиту найбільш ризикових об'єктів внутрішнього аудиту*

Допомога підрозділу внутрішнього аудиту структурним підрозділам державного органу щодо організації та здійснення діяльності з управління ризиками:

здійснення консультаційної діяльності (надання порад та рекомендацій щодо підвищення ефективності та результативності діючих процесів)

проведення робочих зустрічей та семінарів з відповідальними за діяльність особами з питань управління ризиками

**Внутрішні аудитори мають дотримуватися принципів незалежності та об'єктивності!!!**



## **ВИЗНАЧЕННЯ ОБ'ЄКТІВ ВНУТРІШНЬОГО АУДИТУ ЗА ДОПОМОГОЮ ФАКТОРІВ ВІДБОРУ**

*ціль етапу: визначення пріоритетності об'єктів внутрішнього аудиту та частоти дослідження кожного об'єкту внутрішнього аудиту*

**Оцінка кожного фактору відбору за визначеними критеріями (із використанням  
бальних оцінок та вагових коефіцієнтів)**



**Визначення пріоритетних об'єктів внутрішнього аудиту в просторі внутрішнього  
аудиту**



**Визначення частоти проведення планових внутрішніх аудитів щодо кожного  
об'єкту внутрішнього аудиту**



# ВИЗНАЧЕННЯ ОБ'ЄКТІВ ВНУТРІШНЬОГО АУДИТУ ЗА ДОПОМОГОЮ ФАКТОРІВ ВІДБОРУ

*ціль етапу: визначення пріоритетності об'єктів внутрішнього аудиту та частоти дослідження кожного об'єкту внутрішнього аудиту*

## Фактори відбору для здійснення планових внутрішніх аудитів

<b>А. Фінансова важливість/матеріальність</b>	<i>охоплені внутрішнім аудитом обсяги державних ресурсів</i>
<b>В. Складність діяльності</b>	<i>напрями діяльності, які важче реалізувати належним чином</i>
<b>С. Загальна політика внутрішнього контролю</b>	<i>якість процедур контролю, імplementованих у процес</i>
<b>Д. Репутаційна чутливість</b>	<i>увага з боку Уряду, ЗМІ, громадян тощо</i>
<b>Е. Масштаб змін</b>	<i>зміни основних елементів внутрішнього середовища</i>
<b>Є. Надійність керівництва</b>	<i>довіра до керівництва</i>
<b>Г. Можливість для зловживань</b>	<i>вразливі функції для шахрайства та корупції</i>
<b>Н. Питання, які цікавлять керівництво</b>	<i>функції, які викликають занепокоєння керівництва</i>
<b>І. Час від попереднього аудиту</b>	<i>дисциплінуючий фактор</i>
<b>Ж. Стан впровадження аудиторських рекомендацій</b>	<i>низький рівень усунення проблем/недоліків у системі внутрішнього контролю</i>



# ВИЗНАЧЕННЯ ОБ'ЄКТІВ ВНУТРІШНЬОГО АУДИТУ ЗА ДОПОМОГОЮ ФАКТОРІВ ВІДБОРУ

*ціль етапу: визначення пріоритетності об'єктів внутрішнього аудиту та частоти дослідження кожного об'єкту внутрішнього аудиту*

Фактор відбору	Критерії		Бали	Показник вагомості
А. Фінансова важливість/матеріальність	На об'єкт аудиту (програму, систему, ресурси тощо) припадає	менше 10 % річного бюджету	1	3
		11 – 50 % річного бюджету	2	
		51 – 80 % річного бюджету	3	
		81 % річного бюджету	4	
В. Складність діяльності	Вплив виконання функції (процесу) на досягнення мети та цілей діяльності державного органу / кількість процедур та задіяного персоналу, яка передбачає реалізація функції (процесу)	суттєво не впливає/ невелика	1	3
		має помірний вплив / помірна	2	
		впливає / велика	3	
		відіграє ключову роль / найбільша	4	
С. Загальна політика внутрішнього контролю	Надійні системи внутрішнього контролю та управління ризиками		1	2
	Системи внутрішнього контролю та управління ризиками в цілому налагодженні і працюють, але мають недоліки		2	
	Системи внутрішнього контролю та управління ризиками в цілому є слабкими та ненадійними, мають суттєві недоліки		3	
	Система внутрішнього контролю неефективна, має суттєві проблеми (перебуває на стадії запровадження/формально розроблена, але не функціонує, діяльність з управління ризиками не запроваджена на послідовній та структурованій основі)		4	
D. Репутаційна чутливість	Мінімальний зовнішній інтерес до функції (процесу) або його цілковита відсутність		1	2
	Можливість виникнення непорозумінь із громадськістю, пов'язаних з виконанням функції (процесу)		2	
	Виникали поодинокі випадки непорозумінь із громадськістю, пов'язаних з виконанням функції (процесу)		3	
	Підвищена увага з боку ЗМІ до реалізації відповідної функції (процесу). Виникнення серйозних/системних проблем та/або втрата репутації установи за наявності таких проблем		4	
...	...		...	...



# ВИЗНАЧЕННЯ ОБ'ЄКТІВ ВНУТРІШНЬОГО АУДИТУ ЗА ДОПОМОГОЮ ФАКТОРІВ ВІДБОРУ

*ціль етапу: визначення пріоритетності об'єктів внутрішнього аудиту та частоти дослідження кожного об'єкту внутрішнього аудиту*

Фактор відбору	Показник вагомості
А. Фінансова важливість/матеріальність	Wa
В. Складність діяльності	Wb
С. Загальна політика внутрішнього контролю	Wc
Д. Репутаційна чутливість	Wd
Е. Масштаб змін	We
ґ. Надійність керівництва	Wf
Г. Можливість для зловживань	Wg
Н. Питання, які цікавлять керівництво	Wh
І. Час від попереднього аудиту	Wi
Ј. Стан впровадження аудиторських рекомендацій	Wg





# ВИЗНАЧЕННЯ ОБ'ЄКТІВ ВНУТРІШНЬОГО АУДИТУ ЗА ДОПОМОГОЮ ФАКТОРІВ ВІДБОРУ

*ціль етапу: визначення пріоритетності об'єктів внутрішнього аудиту та частоти дослідження кожного об'єкту внутрішнього аудиту*

## Розрахунок індексу пріоритетності

$$I_p = R_m \times \frac{(A \times Wa) + (B \times Wb) + (C \times Wc) + (D \times Wd) + (E \times We) + (F \times Wf) + (G \times Wg) + (H \times Wh) + (I \times Wi) + (J \times Wj)}{n},$$

де  $I_p$  – індекс пріоритетності;

$R_m$  – загальна оцінка ризику за ймовірністю та впливом;

$A-J$  – бал, присвоєний за фактором відбору;

$Wa-Wj$  – показник вагомості фактору відбору;

$n$  – загальна кількість застосованих факторів відбору

## Визначення пріоритетності об'єктів внутрішнього аудиту

Ступень пріоритету	Індекс пріоритетності
дуже високий	від 100 та більше
високий	від 61 до 99
середній	від 41 до 60
низький	до 40

## Визначення частоти здійснення планових внутрішніх аудитів щодо кожного об'єкта внутрішнього аудиту

Ступень пріоритету	Частота внутрішнього аудиту	Індекс пріоритетності
дуже високий	4 рази на 5 років	від 100 та більше
високий	3 рази на 5 років	від 61 до 99
середній	2 рази на 5 років	від 41 до 60
низький	1 раз на 5 років	до 40



# ПРИКЛАД ФОРМАЛІЗАЦІЇ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

## ІНФОРМАЦІЯ ПРО ОБ'ЄКТИ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	Спрямовування внутрішнього аудиту	Результати оцінки ризиків, пов'язаних з об'єктом внутрішнього аудиту			Фактори відбору об'єктів внутрішнього аудиту										Ступінь пріоритету об'єктів внутрішнього аудиту	Частота здійснення планових внутрішніх аудитів
			Ризики високого рівня	Ризики середнього рівня	Ризики низького рівня	Фінансова важливість/ матеріальність	Складність діяльності	Загальна політика внутрішнього контролю	Репутаційна чутливість	Масштаб змін	Надійність керівництва	Можливість для зловживань	Питання, які цікавлять керівництво	Час від попереднього аудиту	Стан впровадження аудиторських рекомендацій		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	Оцінка ефективності існуючих механізмів ІТ-безпеки (ІТ-аудит)	Застосування нових способів віддаленої роботи, зберігання та передача даних за допомогою мобільних пристроїв та хмарних технологій може призвести до зниження рівня захисту інформації	Низький рівень обізнаності працівників щодо можливих загроз через відсутність навчальних заходів з питань ІТ-безпеки може призвести до збільшення випадків порушення цілісності, конфіденційності та доступності інформації	Використання неліцензійного програмного забезпечення може призвести до несанкціонованого доступу до конфіденційної інформації	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	ВИСОКИЙ	3 рази на 5 років
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)	Оцінка ефективності діяльності ІТ-підрозділу (ІТ-аудит)	Невчасне вирішення проблем, пов'язаних з роботою ІТ-систем через відсутність необхідної кваліфікації та навичок працівників ІТ-підрозділу може призвести до зниження ефективності діяльності органу	Неналежний контроль за виконанням ІТ-процесів та процедур може знизити ефективність роботи ІТ-підрозділу	Відсутність моніторингу розподілу та використання ІТ-ресурсів може призвести до неефективного їх використання	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	СЕРЕДНИЙ	2 рази на 5 років
Інформаційні системи і технології	Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)	Оцінка ефективності розробки та реалізації ІТ-стратегії та її відповідності цілям установи (ІТ-аудит)	Зменшення обсягів фінансування може призвести до невиконання ІТ-проектів, які мають бути здійснені в рамках реалізації ІТ-стратегії	Розробка ІТ-стратегії протягом тривалого часу може призвести до втрати актуальності окремих її аспектів	Невідповідність придбаних програмних продуктів цілям органу внаслідок невідкої ІТ-стратегії може призвести до зниження результативних показників діяльності	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	НИЗЬКИЙ	1 раз на 5 років

Приклад наповнення головної таблиці «Інформація про об'єкти простору внутрішнього аудиту» бази даних щодо простору аудиту (колонки 1-18)



# ПРИКЛАД ФОРМАЛІЗАЦІЇ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

Структурні підрозділи державного органу	Підприємства, установи та організації, які належать до сфери управління державного органу	Структурні підрозділи територіального органу/бюджетної установи державного органу (де створені підрозділи внутрішнього аудиту)	Підрозділ внутрішнього аудиту	Інформація щодо здійснення попередніх внутрішніх аудитів						Інформація щодо проведення контрольних заходів (ревізій, перевірок, державних фінансових аудитів тощо) зовнішніми контролюючими органами (Рахунковою палатою, органами державного фінансового контролю тощо)					
				Тема внутрішнього аудиту	Коротка інформація щодо виявлених проблем та недоліків	Дата здійснення внутрішнього аудиту	Період, за який здійснювався внутрішній аудит	Структурний підрозділ державного органу, підпорядковані підприємства, установи та організації, де здійснювався внутрішній аудит	Інформація про стан реагування на висновки та рекомендації за результатами здійснення внутрішнього аудиту	Тема контрольного заходу	Коротка інформація щодо виявлених проблем та порушень/недоліків	Дата проведення контрольного заходу	Період, за який проводився контрольний захід	Структурний підрозділ державного органу, підпорядковані підприємства, установи та організації, де проводились контрольні заходи	Інформація про стан виконання обов'язкових вимог/реагування на висновки та рекомендації за результатами проведення контрольних заходів
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
Підрозділ інформаційних технологій	Підприємство А	Підрозділ інформаційних технологій територіального органу/бюджетної установи А	Підрозділ внутрішнього аудиту державного органу	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —
	Підприємство Б			2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —
	—			—	—	—	—	—	—	—	—	—	—	—	—
	Установа А			п	п	п	п	п	п	п	п	п	п	п	п
—	Установа Б	Підрозділ інформаційних технологій територіального органу/бюджетної установи Б	Підрозділ внутрішнього аудиту територіального органу/бюджетної установи А	п	п	п	п	п	п	п	п	п	п	п	п
	Організація А														
	Організація Б														
	—														
Підрозділ інформаційних технологій	Підприємство А	Підрозділ інформаційних технологій територіального органу/бюджетної установи А	Підрозділ внутрішнього аудиту державного органу	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —
	Підприємство Б			2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —
	—			—	—	—	—	—	—	—	—	—	—	—	—
	Установа А			п	п	п	п	п	п	п	п	п	п	п	п
—	Установа Б	Підрозділ інформаційних технологій територіального органу/бюджетної установи Б	Підрозділ внутрішнього аудиту територіального органу/бюджетної установи А	п	п	п	п	п	п	п	п	п	п	п	п
	Організація А														
	Організація Б														
	—														
Підрозділ інформаційних технологій			Підрозділ внутрішнього аудиту державного органу	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —	1) —
				2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —	2) —
				—	—	—	—	—	—	—	—	—	—	—	—
				п	п	п	п	п	п	п	п	п	п	п	п

Продовження головної таблиці «Інформація про об'єкти простору внутрішнього аудиту» бази даних щодо простору аудиту (колонки 19-34)





# ПРИКЛАД ФОРМАЛІЗАЦІЇ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	Спрямування внутрішнього аудиту	Структурні підрозділи державного органу	Підприємства, установи та організації, які належать до сфери управління державного органу	Структурні підрозділи територіального органу/бюджетної установи державного органу (де створені підрозділи внутрішнього аудиту)	Підрозділ внутрішнього аудиту
1	2	3	19	20	21	22
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	Оцінка ефективності існуючих механізмів ІТ-безпеки	Підрозділ інформаційних технологій	Підприємство А Підприємство Б ... Установа А Установа Б ... Організація А Організація Б ...	Підрозділ інформаційних технологій територіального органу/бюджетної установи А  Підрозділ інформаційних технологій територіального органу/бюджетної установи Б ...	Підрозділ внутрішнього аудиту державного органу  Підрозділ внутрішнього аудиту територіального органу/бюджетної установи А  Підрозділ внутрішнього аудиту територіального органу/бюджетної установи Б ...
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)	Оцінка ефективності діяльності ІТ-підрозділу	Підрозділ інформаційних технологій	Підприємство А Підприємство Б ... Установа А Установа Б ... Організація А Організація Б ...	Підрозділ інформаційних технологій територіального органу/бюджетної установи А  Підрозділ інформаційних технологій територіального органу/бюджетної установи Б ...	Підрозділ внутрішнього аудиту державного органу  Підрозділ внутрішнього аудиту територіального органу/бюджетної установи А  Підрозділ внутрішнього аудиту територіального органу/бюджетної установи Б ...
Інформаційні системи і технології	Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)	Оцінка реалізації ІТ-стратегії та її відповідності цілям діяльності установи	Підрозділ інформаційних технологій			Підрозділ внутрішнього аудиту державного органу

Приклад визначення у зведеній базі даних об'єктів аудиту в розрізі підрозділу внутрішнього аудиту апарату державного органу та підрозділів внутрішнього аудиту територіальних органів та/або бюджетних установ



# ПРИКЛАД ФОРМАЛІЗАЦІЇ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

Оцінка впливу									
Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	№ з/п	Назва ризику	Фінансовий вплив	Кадровий вплив	Операційний вплив	Репутаційний вплив	Бал	Рівень впливу
1	2	3	4	5	6	7	8	9	10
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	1	Використання неліцензійного програмного забезпечення може призвести до несанкціонованого доступу до конфіденційної інформації	Значний фінансово-матеріальний вплив (вище 1 млн грн) (4)	не застосовується	Відсутність можливості продовжувати значно виконувати завдання та функції. Повсюдний збій за всіма напрямками діяльності. Суттєва втрата спроможностей (4)	Некомпетентність (неналежне управління або ігнорування фактів шахрайства/корупції) у великих масштабах) може призвести до втрати довіри з боку громадськості та важливих партнерів на центральному та міжнародному рівні. Період відновлення довіри є тривалим (4)	4 {(4+4+4)/3}	дуже високий
		2	Застосування нових способів віддаленої роботи, зберігання та передача даних за допомогою мобільних пристроїв та хмарних технологій може призвести до зниження рівня захисту інформації	Значний фінансово-матеріальний вплив (вище 1 млн грн) (4)	не застосовується	Відсутність можливості продовжувати значно виконувати завдання та функції. Повсюдний збій за всіма напрямками діяльності. Суттєва втрата спроможностей (4)	Некомпетентність (неналежне управління або системні факти шахрайства/корупції) можуть призвести до різкого зникнення довіри з боку громадськості або важливих партнерів на центральному та міжнародному рівні. Період відновлення довіри є тривалим (3)	4 {(4+4+3)/3}	дуже високий
			Низький рівень обізнаності працівників щодо можливих загроз через відсутність	Значний фінансово-матеріальний вплив (вище 1 млн грн) (4)	Незапланована відсутність (хвороба тощо) деяких ключових працівників у	Відсутність можливості продовжувати значно виконувати завдання та функції. Повсюдний	Некомпетентність (неналежне управління або ігнорування фактів шахрайства/корупції) у великих	4 {(4+1+4+4)/4}	дуже високий

Оцінка ймовірності								
Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	№ з/п	Назва ризику	Ймовірність виникнення ризику низька (0-24 %)	Ймовірність виникнення ризику віддалена (25-50 %)	Ймовірність виникнення ризику впродовж 1-2 років (51-74 %)	Ризик існує або очікується (75-100 %)	Рівень ймовірності
1	2	3	4	5	6	7	8	9
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	1	Використання неліцензійного програмного забезпечення може призвести до несанкціонованого доступу до конфіденційної інформації	1				рідко/майже не можливо
		2	Застосування нових способів віддаленої роботи, зберігання та передача даних за допомогою мобільних пристроїв та хмарних технологій може призвести до зниження рівня захисту інформації			3		можливо
		3	Низький рівень обізнаності працівників щодо можливих загроз через відсутність навчальних заходів з питань ІТ-безпеки може призвести до збільшення випадків порушення цілісності, конфіденційності та доступності інформації		2			малоймовірно
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних	4	Відсутність моніторингу розподілу та використання ІТ-ресурсів може призвести до неефективного їх використання		2			малоймовірно
		5	Неадекватний контроль за виконанням ІТ-процесів та процедур може знизити			3		можливо

ПРОСТІР	Відбір об'єктів	Оцінка впливу	Оцінка ймовірності	Заг.оцінка риз./реєстр риз.:	Оцінка факторів відбору	...	+	←	→
---------	-----------------	---------------	--------------------	------------------------------	-------------------------	-----	---	---	---

Готово Циклічні пошування

</

Приклад ризик-орієнтованого відбору об'єктів аудиту





# ПРИКЛАД ФОРМАЛІЗАЦІЇ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

Загальна оцінка ризиків/реєстр ризиків								
Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	№ з/п	Назва ризику	Оцінка ймовірності	Оцінка впливу	Оцінка ризику за ймовірністю та впливом		Загальна оцінка ризику за ймовірністю та впливом
1	2	3	4	5	6	7	8	9
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	1	Використання неадаптивного програмного забезпечення може призвести до несанкціонованого доступу до конфіденційної інформації	1	4	6 (1 x 4)	середній	8 (4+12+8)/3
		2	Застосування нових способів віддаленої роботи, зберігання та передачі даних та допоміжних мобільних пристроїв та хмарних технологій може призвести до зникнення рівня захисту інформації	3	4	12 (3 x 4)	високий	
		3	Невнесений рівень обсяжності працівників щодо можливих загроз через відсутність навчальних заходів з питань ІТ-безпеки може призвести до збільшення випадків порушення цілісності, конфіденційності та доступності інформації	2	4	8 (2 x 4)	високий	
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)	4	Відсутність моніторингу розподілу та використання ІТ-ресурсів може призвести до неадекватного їх використання	2	2	4 (2 x 2)	середній	8 (4+8+12)/3
		5	Невчасний контроль за виконанням ІТ-процесів та процедур може знизити ефективність роботи ІТ-підрозділу	3	3	9 (3 x 3)	високий	
		6	Невчасне вирішення проблем, пов'язаних з роботою ІТ-систем через відсутність необхідної кваліфікації та навичок працівників ІТ-підрозділу може призвести до зменшення ефективності діяльності органу	3	4	12 (3 x 4)	високий	
Інформаційні	Стратегія розвитку		Розробка ІТ-стратегії протягом тривалого часу			8		

Оцінка факторів відбору								
Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	Факторна важкість/матеріальність [Бал] показник важкості - 1	Складність діяльності [Бал] показник важкості - 1	Лаяльна робота внутрішнього контролю [Бал] показник важкості - 2	Результативність [Бал] показник важкості - 2	Масштаб змін [Бал] показник важкості - 2	Надійність керівництва [Бал] показник важкості - 3	Можливість для виконання факти заходів та корупції [Бал] показник важкості - 4
1	2	3	4	5	6	7	8	9
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	На об'єкт аудиту (програму, систему, ресурси тощо) припадає 11 - 30 % річного бюджету [1]	Виконання функцій (процесів) відіграє ключову роль у досягненні мети та цій діяльності (установки, реалізації функцій (процесів) передбачає надбавку кількості процедур та заданого персоналу [4])	Системи внутрішнього контролю та управління розроблені в цілому з слабкими та неадекватними, мають суттєві недоліки [3]	Виконання функцій (процесів) неадекватно, пов'язане з виконанням функцій (процесів) [1]	За останній рік відбулося від 30 до 30 % змін змін та змін у процедурах в рамках реалізації функцій (процесів) [2]	Особи, відповідальні за реалізацію відповідних функцій (процесів), мають досвід від 1 до 2 років з відповідного напрямку діяльності у державному секторі [3]	існують подвійні факти заходів та корупції [3]
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)	На об'єкт аудиту (програму, систему, ресурси тощо) припадає менше 10 % річного бюджету [1]	Виконання функцій (процесів) виконує не достатньою мірою, виконання функцій (процесів) передбачає велику кількість процедур та заданого персоналу [3]	Системи внутрішнього контролю та управління розроблені в цілому з слабкими та неадекватними, мають суттєві недоліки [3]	Можливість виконання неадекватно, пов'язане з виконанням функцій (процесів) [2]	За останній рік відбулося від 30 до 30 % змін змін та змін у процедурах в рамках реалізації функцій (процесів) [2]	Особи, відповідальні за реалізацію відповідних функцій (процесів), мають досвід від 1 до 2 років з відповідного напрямку діяльності у державному секторі [3]	Можливість виконання неадекватно, пов'язане з виконанням функцій (процесів) та корупції [2]
Інформаційні системи і технології	Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)	На об'єкт аудиту (програму, систему, ресурси тощо) припадає менше 10 % річного бюджету [1]	Виконання функцій (процесів) виконує неадекватно, пов'язане з виконанням функцій (процесів) передбачає велику кількість процедур та заданого персоналу [2]	Системи внутрішнього контролю та управління розроблені в цілому з слабкими та неадекватними, мають суттєві недоліки [3]	Можливість виконання неадекватно, пов'язане з виконанням функцій (процесів) [2]	За останній рік відбулося від 30 до 30 % змін змін та змін у процедурах в рамках реалізації функцій (процесів) [2]	Висока корпоративна культура та висока реалізація функцій (процесів), мають досвід від 5 років та практичну участь у реалізації функцій (процесів) у державному секторі [1]	Можливість виконання неадекватно, пов'язане з виконанням функцій (процесів) та корупції [3]

Визначення пріоритетних об'єктів внутрішнього аудиту для включення до стратегічного та операційного планів діяльності з внутрішнього аудиту на 2019 - 2021 роки														
Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	Фактор відбору	Фінансова важкість/матеріальність	Складність діяльності	Загальна важкість внутрішнього контролю	Результативна чутливість	Масштаб змін	Надійність керівництва	Можливість для запровадження	Питання, які викликають керівництво	Час від попереднього аудиту	Стан запровадження аудиторських рекомендацій	ВІДРЕГІСТРОВАНІСТЬ	СТУПІНЬ ПРІОРИТЕТУ ОБ'ЄКТУ ВНУТРІШНЬОГО АУДИТУ
		Показник важкості фактору відбору	1	2	3	4	5	6	7	8	9			
Бали, присвоєні за критеріями оцінки фактору відбору														
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	8	2	4	3	3	2	3	3	3	4	3	61	Високий
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)	8	1	3	3	2	2	3	2	2	3	3	46	Середній
Інформаційні системи і технології	Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)	8	1	2	2	1	2	1	1	2	3	3	34	Низький

Приклад ризик-орієнтованого відбору об'єктів аудиту (продовження)





# ПРИКЛАД ФОРМАЛІЗАЦІЇ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

№ з/п	Назва підприємства, установи та організації	Код за ЄДРПОУ	Місцезнаходження	ПІБ керівника	Контактні дані	Примітка
1	Підприємство А	32855961	м. Київ, вул. ...	Петров О.В.	тел... e-mail...	
2	Підприємство Б	32866961	м. Житомир, вул. ...	Василенко А.П.	тел... e-mail...	
3	Підприємство В	...	...	...	...	
...	...	...	...	...	...	

Приклад ведення довідника підприємств, установ та організацій, які належать до сфери управління державного органу

№ з/п	Назва структурного підрозділу	ПІБ керівника	Контактні дані
1	Служба управління персоналом	...	тел... e-mail...
2	Підрозділ інформаційних технологій	...	тел... e-mail...
3	Підрозділ правового забезпечення	...	...
...	...	...	...

Приклад ведення довідника структурних підрозділів державного органу



# ПРИКЛАД ФОРМАЛІЗАЦІЇ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

ІНФОРМАЦІЯ ПРО ОБ'ЄКТИ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ														
Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	Спрямовування внутрішнього аудиту	Результати оцінки ризиків, пов'язаних з об'єктом внутрішнього аудиту			Фактори відбору об'єктів внутрішнього								Час від попереднього
			Ризики високого рівня	Ризики середнього рівня	Ризики низького рівня	Фінансова важливість	матеріальність	критичність діяльності	Загальна політика внутрішнього контролю	здатність чутливості	Масштаб змін	Дійсність нерівноваж	Можливість для зловживань	Питання, які цікавлять керівництво
1	2	3	4	5	6	7	8	9	10	11	12	13	14	
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ безпека)	Оцінка ефективності існуючих механізмів ІТ безпеки (ІТ аудит)	Застосування нових способів віддаленої роботи, зберігання та передачі даних за допомогою мобільних пристроїв та хмарних технологій може призвести до зникнення рівня захисту інформації	Низький рівень обізнаності працівників щодо можливих загроз через відсутність навчальних заходів з питань ІТ безпеки може призвести до збільшення випадків порушення цілісності, конфіденційності та доступності інформації	Використання неліцензійного програмного забезпечення може призвести до несанкціонованого доступу до конфіденційної інформації	☑	☑	☑	☑	☑	☑	☑	☑	
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних технологій (ІТ підрозділу)	Оцінка ефективності діяльності ІТ підрозділу (ІТ аудит)	Невчасне вирішення проблем, пов'язаних з роботою ІТ систем через відсутність необхідної кваліфікації та наявності працівників ІТ підрозділу може призвести до зникнення ефективності діяльності органу	Незалежний контроль за виконанням ІТ процесів та процедур може знизити ефективність роботи ІТ підрозділу	Відсутність моніторингу розподілу та використання ІТ-ресурсів може призвести до неефективного їх використання	☑	☑	☑	☑	☑	☑	☑	☑	
Інформаційні системи і технології	Стратегія розвитку інформаційних систем державного органу (ІТ стратегія)	Оцінка ефективності розробки та реалізації ІТ стратегії та її відповідності цілям установи	Зменшення обсягів фінансування може призвести до не виконання ІТ проєктів, які мають бути здійснені в рамках реалізації ІТ стратегії	Розробка ІТ стратегії протягом тривалого часу може призвести до втрати актуальності окремих її аспектів	Використання неліцензійного програмного коду, застосування нових способів віддаленої роботи високого рівня обізнаності працівників щодо ІТ безпеки, контроль за виконанням ІТ-проєктів, наявність виражених проблем, пов'язаних з розробкою ІТ-стратегії протягом тривалого часу, неадекватність пріоритетів програмних проєктів	☑	☑	☑	☑	☑	☑	☑	☑	

Приклад вибору ризику із розкривного списку



# ПРИКЛАД ФОРМАЛІЗАЦІЇ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

ІНФОРМАЦІЯ ПРО ОБ'ЄКТИ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ					
Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	Спрямовання внутрішнього аудиту	Частота здійснення внутрішнього аудиту	Структурні підрозділи державного органу	Підприємства, установи та організації, які належать до сфери управління державного органу
1	2	3	18	19	20
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	Оцінка ефективності існуючих механізмів ІТ-безпеки	3 рази на 5 років	Підрозділ інформаційних технологій	

Приклад застосування довідника при виборі  
структурного підрозділу державного органу

ІНФОРМАЦІЯ ПРО ОБ'ЄКТИ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ					
Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	Спрямовання внутрішнього аудиту	Частота здійснення внутрішнього аудиту	Структурні підрозділи державного органу	Підприємства, установи та організації, які належать до сфери управління державного органу
1	2	3	18	19	20
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	Оцінка ефективності існуючих механізмів ІТ-безпеки	3 рази на 5 років	Підрозділ інформаційних технологій	

Приклад застосування довідника при виборі  
підприємства



## Приклад фільтрування об'єктів аудиту за ступенем пріоритету





# ПРИКЛАД ФОРМАЛІЗАЦІЇ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

ІНФОРМАЦІЯ ПРО ОБ'ЄКТИ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ							
Вибір об'єктів за підрозділом внутрішнього аудиту							
Підрозділ ВА державного органу							
Підрозділ ВА державного органу, Підрозділ ВА територіального органу А							
Підрозділ ВА державного органу, Підрозділ ВА територіального органу А, Підрозділ ВА територіального органу Б							
Підрозділ ВА територіального органу Б							
(поро)							
Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	Структурні підрозділи державного органу	Підприємства, установи та організації, які належать до сфери управління державного органу	Структурні підрозділи територіального органу/бюджетної установи державного органу (де створені підрозділи внутрішнього аудиту)	Підрозділ внутрішнього аудиту	Інформація	
						Тема внутрішнього аудиту	Коротка інформація щодо виявлених проблем та недоліків
1	2	19	20	21	22	23	24
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	Підрозділ інформаційних технологій	Підприємство А Підприємство Б	Підрозділ інформаційних технологій територіального органу А	Підрозділ ВА державного органу, Підрозділ ВА територіального органу А	1) ... 2) ... ...	1) ... 2) ... ...
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)	Підрозділ інформаційних технологій	Підприємство А Підприємство Б	Підрозділ інформаційних технологій територіального органу А Підрозділ інформаційних технологій територіального органу Б	Підрозділ ВА державного органу, Підрозділ ВА територіального органу А, Підрозділ ВА територіального органу Б	1) ... 2) ... ...	1) ... 2) ... ...

Приклад фільтрування об'єктів аудиту в розрізі відповідних підрозділів внутрішнього аудиту



# ПРИКЛАД ФОРМАЛІЗАЦІЇ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ

ІНФОРМАЦІЯ ПРО ОБ'ЄКТИ ПРОСТОРУ ВНУТРІШНЬОГО АУДИТУ							Інформація щодо здійсненн		
Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	Структурні підрозділи державного органу	Підприємства, установи та організації, які належать до сфери управління державного органу	Структурні підрозділи територіального органу/бюджетної установи державного органу (де створені підрозділи внутрішнього аудиту)	Підрозділ внутрішнього аудиту	Тема внутрішнього аудиту	Коротка інформація щодо виявлених проблем та недоліків	Дата здійснення внутрішнього аудиту	
1	2	19	20	21				25	
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	Підрозділ інформаційних технологій	Підприємство А Підприємство Б	Підрозділ інформаційних техно територіального органу А				1) ... 2) ...	
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)	Підрозділ інформаційних технологій	Підприємство А Підприємство Б	Підрозділ інформаційних техно територіального органу А Підрозділ інформаційних техно територіального органу Б				1) ... 2) ...	
Інформаційні системи і технології	Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)	Підрозділ інформаційних	Підприємство А Підприємство Б						

Користувачий автофільтр

Показати лише ті рядки, значення яких:

Підрозділ внутрішнього аудиту, до компетенції яког...

містить Територіального органу А

☒ І ☐ ДБО

Знак питання "?" позначає один будь-який символ

Символ "\*" позначає послідовність будь-яких символів

OK Скасувати

Сортування від А до Я

Сортування від Я до А

Сортування за кольором

Віддалити фільтр із "Підрозділ внутріш..."

Фільтрування за кольором

Текстові фільтри

Пошук

☐ (Виділити все)

☐ Підрозділ ВА державного органу

☐ Підрозділ ВА державного органу, Підрозділ ВА територіального органу А

☐ Підрозділ ВА державного органу, Підрозділ ВА територіального органу А, Під

☐ (Пусті)

Дорівнює...

Не дорівнює...

Починається з...

Закінчується...

Містить...

Не містить...

Користувачий фільтр...

OK Скасувати

Приклад іншого способу фільтрування об'єктів аудиту в розрізі відповідних підрозділів внутрішнього аудиту





# ПРИКЛАД ПРОВЕДЕННЯ ОЦІНКИ РИЗИКІВ ТА ЗДІЙСНЕННЯ РИЗИК-ОРІЄНТОВАНОГО ВІДБОРУ ОБ'ЄКТІВ АУДИТУ

Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	№ з/п	Назва ризику
<b>Інформаційні системи і технології</b>	<b>Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)</b>	1	Використання неліцензійного програмного забезпечення може призвести до несанкціонованого доступу до конфіденційної інформації
		2	Застосування нових способів віддаленої роботи, зберігання та передача даних за допомогою мобільних пристроїв та хмарних технологій може призвести до зниження рівня захисту інформації
		3	Низький рівень обізнаності працівників щодо можливих загроз через відсутність навчальних заходів з питань ІТ-безпеки може призвести до збільшення випадків порушення цілісності, конфіденційності та доступності інформації
<b>Інформаційні системи і технології</b>	<b>Організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)</b>	4	Відсутність моніторингу розподілу та використання ІТ-ресурсів може призвести до неефективного їх використання
		5	Неналежний контроль за виконанням ІТ-процесів та процедур може знизити ефективність роботи ІТ-підрозділу
		6	Невчасне вирішення проблем, пов'язаних з роботою ІТ-систем через відсутність необхідної кваліфікації та навичок працівників ІТ-підрозділу може призвести до зниження ефективності діяльності органу
<b>Інформаційні системи і технології</b>	<b>Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)</b>	7	Розробка ІТ-стратегії протягом тривалого часу може призвести до втрати актуальності окремих її аспектів
		8	Невідповідність придбаних програмних продуктів цілям органу внаслідок невдалої ІТ-стратегії може призвести до зниження результативних показників діяльності
		9	Зменшення обсягів фінансування може призвести до не виконання ІТ-проектів, які мають бути здійснені в рамках реалізації ІТ-стратегії



# ПРИКЛАД ПРОВЕДЕННЯ ОЦІНКИ РИЗИКІВ ТА ЗДІЙСНЕННЯ РИЗИК-ОРІЄНТОВАНОГО ВІДБОРУ ОБ'ЄКТІВ АУДИТУ

## Оцінка впливу

Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	№ з/п	Назва ризику	Фінансовий вплив	Кадровий вплив	Операційний вплив	Репутаційний вплив	Бал	Рівень впливу
1	2	3	4	5	6	7	8	9	10
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	1	Використання неліцензійного програмного забезпечення може призвести до несанкціонованого доступу до конфіденційної інформації	Значний фінансово-матеріальний вплив вище 1 млн грн (4)	не застосовується	Відсутність можливості продовжувати звично виконувати завдання та функції. Повсюдний збій за всіма напрямками діяльності. Суттєва втрата спроможностей (4)	Некомпетентність (неналежне управління або існування фактів шахрайства/корупції у великих масштабах) може призвести до втрати довіри з боку громадськості та важливих партнерів на центральному та міжнародному рівні. Період відновлення довіри є тривалим (4)	4 ((4+4+4)/3)	дуже високий
		2	Застосування нових способів віддаленої роботи, зберігання та передача даних за допомогою мобільних пристроїв та хмарних технологій може призвести до зниження рівня захисту інформації	Значний фінансово-матеріальний вплив вище 1 млн грн (4)	не застосовується	Відсутність можливості продовжувати звично виконувати завдання та функції. Повсюдний збій за всіма напрямками діяльності. Суттєва втрата спроможностей (4)	Некомпетентність (неналежне управління або системні факти шахрайства/корупції) можуть призвести до різкого зниження довіри з боку громадськості або важливих партнерів на центральному та міжнародному рівні. Період відновлення довіри є помірним (3)	4 ((4+4+3)/3)	дуже високий
		3	Низький рівень обізнаності працівників щодо можливих загроз через відсутність навчальних заходів з питань ІТ-безпеки може призвести до збільшення випадків порушення цілісності, конфіденційності та доступності інформації	Значний фінансово-матеріальний вплив вище 1 млн грн (4)	Незапланована відсутність (хвороба тощо) деяких ключових працівників у одному підрозділі може призвести до затримки у роботі цього підрозділу (2)	Відсутність можливості продовжувати звично виконувати завдання та функції. Повсюдний збій за всіма напрямками діяльності. Суттєва втрата спроможностей (4)	Некомпетентність (неналежне управління або існування фактів шахрайства/корупції у великих масштабах) може призвести до втрати довіри з боку громадськості та важливих партнерів на центральному та міжнародному рівні. Період відновлення довіри є тривалим (4)	4 ((4+2+4+4)/4)	дуже високий



# ПРИКЛАД ПРОВЕДЕННЯ ОЦІНКИ РИЗИКІВ ТА ЗДІЙСНЕННЯ РИЗИК-ОРІЄНТОВАНОГО ВІДБОРУ ОБ'ЄКТІВ АУДИТУ

## Оцінка ймовірності

Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	№ з/п	Назва ризику	Ймовірність виникнення ризику низька (0-24 %)	Ймовірність виникнення ризику віддалена (25-50 %)	Ймовірність виникнення ризику впродовж 1-2 років (51-74 %)	Ризик існує або очікується (75-100 %)	Рівень ймовірності
1	2	3	4	5	6	7	8	9
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	1	Використання неліцензійного програмного забезпечення може призвести до несанкціонованого доступу до конфіденційної інформації	1				рідко/майже не можливо
		2	Застосування нових способів віддаленої роботи, зберігання та передача даних за допомогою мобільних пристроїв та хмарних технологій може призвести до зниження рівня захисту інформації			3		можливо
		3	Низький рівень обізнаності працівників щодо можливих загроз через відсутність навчальних заходів з питань ІТ-безпеки може призвести до збільшення випадків порушення цілісності, конфіденційності та доступності інформації		2			малоймовірно
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних систем	4	Відсутність моніторингу розподілу та використання ІТ-ресурсів може призвести до неефективного їх використання		2			малоймовірно
		5	Неналежний контроль за виконанням ІТ-процесів та процедур може знизити ефективність роботи ІТ-підрозділу			3		можливо
		6	Невчасне вирішення проблем, пов'язаних з роботою ІТ-систем через відсутність необхідної кваліфікації та навичок працівників ІТ-підрозділу може призвести до зниження ефективності діяльності органу			3		можливо
Інформаційні системи і технології	Стратегія розвитку інформаційних систем державного	7	Розробка ІТ-стратегії протягом тривалого часу може призвести до втрати актуальності окремих її аспектів			3		можливо
		8	Невідповідність придбаних програмних продуктів цілям органу внаслідок невдалої ІТ-стратегії може призвести до зниження результативних показників діяльності		2			малоймовірно
		9	Зменшення обсягів фінансування може призвести до не виконання ІТ-проектів, які мають бути здійснені в рамках реалізації ІТ-стратегії				4	часто/очікується





# ПРИКЛАД ПРОВЕДЕННЯ ОЦІНКИ РИЗИКІВ ТА ЗДІЙСНЕННЯ РИЗИК-ОРІЄНТОВАНОГО ВІДБОРУ ОБ'ЄКТІВ АУДИТУ

## Загальна оцінка ризиків/реєстр ризиків

Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	№ з/п	Назва ризику	Оцінка ймовірності	Оцінка впливу	Оцінка ризику за ймовірністю та впливом		Загальна оцінка ризиків за ймовірністю та впливом	
						Бал	Рівень	Бал	Рівень
1	2	3	4	5	6	7	8	9	10
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	1	Використання неліцензійного програмного забезпечення може призвести до несанкціонованого доступу до конфіденційної інформації	1	4	4 (1 x 4)	середній	8 ((4+12+8)/3)	високий
		2	Застосування нових способів віддаленої роботи, зберігання та передача даних за допомогою мобільних пристроїв та хмарних технологій може призвести до зниження рівня захисту інформації	3	4	12 (3 x 4)	високий		
		3	Низький рівень обізнаності працівників щодо можливих загроз через відсутність навчальних заходів з питань ІТ-безпеки може призвести до збільшення випадків порушення цілісності, конфіденційності та доступності інформації	2	4	8 (2 x 4)	високий		
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)	4	Відсутність моніторингу розподілу та використання ІТ-ресурсів може призвести до неефективного їх використання	2	2	4 (2 x 2)	середній	8 ((4+9+12)/3))	високий
		5	Неналежний контроль за виконанням ІТ-процесів та процедур може знизити ефективність роботи ІТ-підрозділу	3	3	9 (3 x 3)	високий		
		6	Невчасне вирішення проблем, пов'язаних з роботою ІТ-систем через відсутність необхідної кваліфікації та навичок працівників ІТ-підрозділу може призвести до зниження ефективності діяльності органу	3	4	12 (3 x 4)	високий		
Інформаційні системи і технології	Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)	7	Розробка ІТ-стратегії протягом тривалого часу може призвести до втрати актуальності окремих її аспектів	3	3	9 (3 x 3)	високий	8 ((9+4+12)/3))	високий
		8	Невідповідність придбаних програмних продуктів цілям органу внаслідок невдалої ІТ-стратегії може призвести до зниження результативних показників діяльності	2	2	4 (2 x 2)	середній		
		9	Зменшення обсягів фінансування може призвести до не виконання ІТ-проектів, які мають бути здійснені в рамках реалізації ІТ-стратегії	4	3	12 (4 x 3)	високий		



# ПРИКЛАД ПРОВЕДЕННЯ ОЦІНКИ РИЗИКІВ ТА ЗДІЙСНЕННЯ РИЗИК-ОРІЄНТОВАНОГО ВІДБОРУ ОБ'ЄКТІВ АУДИТУ

Матриця оцінки ризиків						
Рівень (бал)			ЙМОВІРНІСТЬ			
			Рідко/майже не можливо	Малоймовірно	Можливо	Часто/ очікується
			1	2	3	4
ВПЛИВ	Низький	1	Низький (а) (1)	Низький (а) (2)	Низький (а) (3)	Середній (я) (4)
	Середній	2	Низький (а) (2)	Середній (я) (4)	Середній (я) (6)	Високий (а) (8)
	Високий	3	Низький (а) (3)	Середній (я) (6)	Високий (а) (9)	Дуже високий (а) (12)
	Дуже високий	4	Середній (я) (4)	Високий (а) (8)	Дуже високий (а) (12)	Дуже високий (а) (16)



# ПРИКЛАД ПРОВЕДЕННЯ ОЦІНКИ РИЗИКІВ ТА ЗДІЙСНЕННЯ РИЗИК-ОРІЄНТОВАНОГО ВІДБОРУ ОБ'ЄКТІВ АУДИТУ

Сфера внутрішнього аудиту: інформаційні системи і технології.

Об'єкти аудиту: забезпечення захисту інформації в інформаційних системах (ІТ-безпека);  
організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу);  
стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)

Фактор відбору		Показник вагомості
A.	Фінансова важливість/матеріальність	3
B.	Складність діяльності	3
C.	Загальна політика внутрішнього контролю	2
D.	Репутаційна чутливість	2
E.	Масштаб змін	2
F.	Надійність керівництва	2
G.	Можливість для зловживань	4
H.	Питання, які цікавлять керівництво	5
I.	Час від попереднього внутрішнього аудиту	2
J.	Стан впровадження аудиторських рекомендацій, наданих за результатами здійснення попередніх внутрішніх аудитів	1





# ПРИКЛАД ПРОВЕДЕННЯ ОЦІНКИ РИЗИКІВ ТА ЗДІЙСНЕННЯ РИЗИК-ОРІЄНТОВАНОГО ВІДБОРУ ОБ'ЄКТІВ АУДИТУ

## Оцінка кожного фактору відбору за визначеними критеріями із використанням бальних оцінок та вагових коефіцієнтів

Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	Фактори відбору									
		Фінансова важливість/матеріальність (бал) показник вагомості - 3	Складність діяльності (бал) показник вагомості - 3	Загальна політика внутрішнього контролю (бал) показник вагомості - 2	Репутаційна чутливість (бал) показник вагомості - 2	Масштаб змін (бал) показник вагомості - 2	Надійність керівництва (бал) показник вагомості - 2	Можливість для зловживань (бал) показник вагомості - 4	Питання, які цікавлять керівництво (бал) показник вагомості - 5	Час від попереднього аудиту (бал) показник вагомості - 2	Стан впровадження аудиторських рекомендацій (бал) показник вагомості - 1
1	2	3	4	5	6	7	8	9	10	11	12
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	На об'єкт аудиту (програму, системи, ресурси тощо) припадає 11 – 50 % річного бюджету (2)	Виконання функції (процесу) відіграє ключову роль у досягненні мети та цілей діяльності установи; реалізація функції (процесу) передбачає найбільшу кількість процедур та задіяного персоналу (4)	Системи внутрішнього контролю та управління ризиками в цілому є слабкими та ненадійними, мають суттєві недоліки (3)	Виникали поодинокі випадки непорозумінь із громадськістю, пов'язаних з виконанням функції (процесу) (3)	За останній рік відбулося від 10 до 30 % кадрових змін та змін у процедурах в рамках реалізації функції (процесу) (2)	Особи, відповідальні за реалізацію відповідної функції (процесу), мають досвід від 1 до 2 років з відповідного напрямку діяльності у державному секторі (3)	Існують поодинокі факти шахрайства та корупції (3)	Висока увага з боку вищого керівництва установи, суттєві або повторювані проблеми, які вийшли на рівень вищого керівництва у минулому (3)	За останні 5 років внутрішній аудит не проводився (4)	Повністю виконано аудиторські рекомендації або внутрішній аудит не здійснювався (1)
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)	На об'єкт аудиту (програму, систему, ресурси тощо) припадає менше 10 % річного бюджету (1)	Виконання функції (процесу) впливає на досягнення мети та цілей діяльності установи; реалізація функції (процесу) передбачає велику кількість процедур та задіяного персоналу (3)	Системи внутрішнього контролю та управління ризиками в цілому є слабкими та ненадійними, мають суттєві недоліки (3)	Можливість виникнення непорозумінь із громадськістю, пов'язаних з виконанням функції (процесу) (2)	За останній рік відбулося від 10 до 30 % кадрових змін та змін у процедурах в рамках реалізації функції (процесу) (2)	Особи, відповідальні за реалізацію відповідної функції (процесу), мають досвід від 1 до 2 років з відповідного напрямку діяльності у державному секторі (3)	Можливість виникнення зловживань, однак фактів шахрайства та корупції ще не виникали (2)	Вище керівництво установи приділяє помірну увагу, наявність проблем, які вийшли на рівень вищого керівництва у минулому (2)	Проведено більше 3 років, але менше 5 років тому (3)	Повністю виконано аудиторські рекомендації або внутрішній аудит не здійснювався (1)
Інформаційні системи і технології	Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)	На об'єкт аудиту (програму, систему, ресурси тощо) припадає менше 10 % річного бюджету (1)	Виконання функції (процесу) має помірний вплив на досягнення мети та цілей діяльності установи; реалізація функції (процесу) передбачає помірну кількість процедур та задіяного персоналу (2)	Системи внутрішнього контролю та управління ризиками в цілому налагоджені і працюють, але мають недоліки (2)	Мінімальний зовнішній інтерес до функції (процесу) або його цілковита відсутність (1)	За останній рік відбулося від 10 до 30 % змін – змін у законодавчих та нормативно-правових актах, які регулюють виконання відповідної функції (процесу), кадрових змін, змін у процедурах в рамках реалізації функції (процесу) (2)	Вище керівництво установи та особи, відповідальні за реалізацію відповідної функції (процесу), мають досвід більше 3 років та практику успішної реалізації проєктів/програм з відповідного напрямку діяльності у державному секторі (1)	Мінімальна можливість для виникнення фактів шахрайства та корупції (1)	Вище керівництво установи приділяє помірну увагу, наявність проблем, які вийшли на рівень вищого керівництва у минулому (2)	Проведено більше 3 років, але менше 5 років тому (3)	Повністю виконано аудиторські рекомендації або внутрішній аудит не здійснювався (1)



# ПРИКЛАД ПРОВЕДЕННЯ ОЦІНКИ РИЗИКІВ ТА ЗДІЙСНЕННЯ РИЗИК-ОРІЄНТОВАНОГО ВІДБОРУ ОБ'ЄКТІВ АУДИТУ

## Розрахунок індексу пріоритетності

об'єкт аудиту: забезпечення захисту інформації в інформаційних системах (ІТ-безпека)

$$61 = 8 \times \left( \frac{(2 \times 3) + (4 \times 3) + (3 \times 2) + (3 \times 2) + (2 \times 2) + (3 \times 2) + (3 \times 4) + (3 \times 5) + (4 \times 2) + (1 \times 1)}{10} \right)$$

об'єкт аудиту: організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)

$$46 = 8 \times \left( \frac{(1 \times 3) + (3 \times 3) + (3 \times 2) + (2 \times 2) + (2 \times 2) + (3 \times 2) + (2 \times 4) + (2 \times 5) + (3 \times 2) + (1 \times 1)}{10} \right)$$

об'єкт аудиту: стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)

$$34 = 8 \times \left( \frac{(1 \times 3) + (2 \times 3) + (2 \times 2) + (1 \times 2) + (2 \times 2) + (1 \times 2) + (1 \times 4) + (2 \times 5) + (3 \times 2) + (1 \times 1)}{10} \right)$$

Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	Фактор відбору	Фінансова важливість/матеріальність	Складність діяльності	Загальна політика внутрішнього контролю	Репутаційна чутливість	Масштаб змін	Надійність керівництва	Можливість для зловживань	Питання, які цікавлять керівництво	Час від попереднього аудиту	Стан впровадження аудиторських рекомендацій	ІНДЕКС ПРІОРИТЕТНОСТІ
		Показник вагомості фактору відбору	3	3	2	2	2	2	4	5	2	1	
		Загальна оцінка ризиків за ймовірністю та впливом	Бали, присвоєні за критеріями оцінки фактору відбору										
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	8	2	4	3	3	2	3	3	3	4	1	61
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)	8	1	3	3	2	2	3	2	2	3	1	46
Інформаційні системи і технології	Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)	8	1	2	2	1	2	1	1	2	3	1	34



# ПРИКЛАД ПРОВЕДЕННЯ ОЦІНКИ РИЗИКІВ ТА ЗДІЙСНЕННЯ РИЗИК-ОРІЄНТОВАНОГО ВІДБОРУ ОБ'ЄКТІВ АУДИТУ

Визначення ступеню пріоритету об'єктів аудиту та частоти здійснення планових внутрішніх аудитів щодо кожного пріоритетного об'єкта аудиту

Сфера внутрішнього аудиту	Об'єкт внутрішнього аудиту	ІНДЕКС ПРІОРИТЕТНОСТІ	СТУПІНЬ ПРІОРИТЕТУ ОБ'ЄКТУ ВНУТРІШНЬОГО АУДИТУ	ЧАСТОТА ЗДІЙСНЕННЯ ПЛАНОВИХ ВНУТРІШНІХ АУДИТІВ
Інформаційні системи і технології	Забезпечення захисту інформації в інформаційних системах (ІТ-безпека)	61	Високий	3 рази на 5 років
Інформаційні системи і технології	Організація та діяльність підрозділу інформаційних технологій (ІТ-підрозділу)	46	Середній	2 рази на 5 років
Інформаційні системи і технології	Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)	34	Низький	1 раз на 5 років

Ступінь пріоритету	Індекс пріоритетності
дуже високий	від 100 та більше
високий	від 61 до 99
середній	від 41 до 60
низький	до 40

Ступінь пріоритету	Частота здійснення планових внутрішніх аудитів щодо кожного пріоритетного об'єкта аудиту	Індекс пріоритетності
дуже високий	4 рази на 5 років	від 100 та більше
високий	3 рази на 5 років	від 61 до 99
середній	2 рази на 5 років	від 41 до 60
низький	1 раз на 5 років	до 40



## ФОРМУВАННЯ ПЛАНУ ДІЯЛЬНОСТІ З ВНУТРІШНЬОГО АУДИТУ (ВНЕСЕННЯ ДО НЬОГО ЗМІН)

*ціль етапу: визначення переліку пріоритетних об'єктів внутрішнього аудиту на підставі оцінки потреб внутрішнього аудиту*

визначення потреб у ресурсах для виконання запланованої діяльності з внутрішнього аудиту



формування стратегічного та операційного планів на підставі результатів оцінки ризиків та ризик-орієнтованого відбору об'єктів внутрішнього аудиту



затвердження керівником державного органу стратегічного та операційного планів не пізніше початку планового періоду



внесення змін до стратегічного та операційного планів не пізніше завершення планового періоду (у разі необхідності)



оприлюднення затверджених планів на офіційному вебсайті державного органу, направлення копій затверджених планів Мінфіну протягом 10 робочих днів з дати їх затвердження



## ФОРМУВАННЯ ПЛАНУ ДІЯЛЬНОСТІ З ВНУТРІШНЬОГО АУДИТУ (ВНЕСЕННЯ ДО НЬОГО ЗМІН)

*ціль етапу: визначення переліку пріоритетних об'єктів внутрішнього аудиту на підставі оцінки потреб внутрішнього аудиту*

**Визначення потреб у ресурсах на здійснення внутрішніх аудитів проводиться з урахуванням усіх етапів проведення внутрішнього аудиту, а саме:**

- організації внутрішнього аудиту та планування аудиторського завдання;
- виконання аудиторського завдання;
- документування перебігу та результатів внутрішнього аудиту

**Потреби у ресурсах на виконання заходів з іншої діяльності з внутрішнього аудиту визначаються, зокрема, на:**

- здійснення методологічної роботи;
- здійснення ризик-орієнтованого планування діяльності з внутрішнього аудиту;
- здійснення моніторингу врахування рекомендацій за результатами проведених внутрішніх аудитів;
- звітування (внутрішнє та зовнішнє) про діяльність підрозділу внутрішнього аудиту;
- проведення внутрішніх оцінок якості внутрішнього аудиту
- професійний розвиток працівників підрозділу внутрішнього аудиту;
- здійснення роз'яснювальної та консультаційної роботи



## ФОРМУВАННЯ ПЛАНУ ДІЯЛЬНОСТІ З ВНУТРІШНЬОГО АУДИТУ (ВНЕСЕННЯ ДО НЬОГО ЗМІН)

*ціль етапу: визначення переліку пріоритетних об'єктів внутрішнього аудиту на підставі оцінки потреб внутрішнього аудиту*

За результатами визначення потреб у ресурсах керівник підрозділу  
внутрішнього аудиту забезпечує:

до початку виконання запланованої діяльності  
визначення обсягів робочого часу на здійснення внутрішніх аудитів та виконання заходів з іншої діяльності з внутрішнього аудиту (пункт 6 Стандарту 7)

під час подання керівнику державного органу на затвердження плану  
подання/інформування щодо потреб/обмежень, у тому числі про вплив та наслідки обмеження у ресурсах внутрішнього аудиту з наданням відповідних пропозицій щодо шляхів вирішення цього питання (пункт 6 Стандарту 7)

під час щорічного письмового звітування керівнику державного органу (внутрішнє)  
інформування у звіті про результати діяльності підрозділу внутрішнього аудиту, зокрема, про рівень забезпечення ресурсами для провадження діяльності з внутрішнього аудиту (пункт 2 Стандарту 13)





# ФОРМУВАННЯ ПЛАНУ ДІЯЛЬНОСТІ З ВНУТРІШНЬОГО АУДИТУ (ВНЕСЕННЯ ДО НЬОГО ЗМІН)

*ціль етапу: визначення переліку пріоритетних об'єктів внутрішнього аудиту на підставі оцінки потреб внутрішнього аудиту*

## Розрахунок потреби в ресурсах для забезпечення виконання плану діяльності з внутрішнього аудиту

*(назва підрозділу внутрішнього аудиту  
державного органу/бюджетної установи)*

*(зазначається плановий період)*

№ з/п	Потреба в ресурсах (фінансових, людських, ІТ-ресурсів тощо)	Перелік потреби	Розрахунок витрат	Сума витрат (грн)	Примітка
1.	Відрядження для здійснення 6 планових внутрішніх аудитів	Добові	5 чол. x 18 днів x 60 грн	5400,00	
		Квитки	5 чол. x 800 грн x 6 разів	24000,00	
		Проживання у готелі	1000 грн x 18 днів	18000,00	
2.	Забезпечення комп'ютерним обладнанням	Ноутбук	3 шт.	-	
3.	Забезпечення канцелярським приладдям	Папір	2 пачки	600,00	
4.	Відкриття доступу до внутрішньої інформаційної бази даних	Реєстр витрат та доходів підприємств, які належать до сфери управління державного органу	1 реєстр	-	Період відкриття доступу – до завершення здійснення внутрішнього аудиту
5.	Залучення профільних спеціалістів для проведення 3 планових внутрішніх аудитів	Спеціаліст з питань капітального будівництва (Відділ капітального та поточного ремонтів)	1 чол.	-	Для здійснення 1 аудиту
		Спеціаліст з ІТ (Відділ технічного забезпечення та захисту інформації)	2 чол.	-	Для здійснення 2 аудитів
...					
Всього:		х	х	48000,00	х

*(посада керівника підрозділу  
внутрішнього аудиту)*

*(підпис)*



## ФОРМУВАННЯ ПЛАНУ ДІЯЛЬНОСТІ З ВНУТРІШНЬОГО АУДИТУ (ВНЕСЕННЯ ДО НЬОГО ЗМІН)

*ціль етапу: визначення переліку пріоритетних об'єктів внутрішнього аудиту на підставі оцінки потреб внутрішнього аудиту*

План діяльності з внутрішнього аудиту формується на підставі результатів оцінки ризиків

План повинен визначати пріоритети та результати діяльності підрозділу внутрішнього аудиту на наступні три роки, які враховують стратегію (пріоритети) та цілі діяльності державного органу

План щорічно визначаються завдання підрозділу внутрішнього аудиту на наступний календарний рік з урахуванням визначених пріоритетів та результатів діяльності підрозділу внутрішнього аудиту на відповідний трирічний період

*пункт 6 Порядку здійснення внутрішнього аудиту та утворення підрозділів  
внутрішнього аудиту (постанова Кабінету Міністрів України від 28.09.2011 № 1001),  
Стандарт 7*



## ФОРМУВАННЯ ПЛАНУ ДІЯЛЬНОСТІ З ВНУТРІШНЬОГО АУДИТУ (ВНЕСЕННЯ ДО НЬОГО ЗМІН)

*ціль етапу: визначення переліку пріоритетних об'єктів внутрішнього аудиту на підставі оцінки потреб внутрішнього аудиту*

Для складання реалістичних планів необхідно враховувати, зокрема:

можливість залучення та перерозподілу трудових ресурсів у плановому періоді, ротацію кадрів, наявні трудові ресурси

організаційні, географічні та часові обмеження

законодавче обмеження щодо не включення внутрішніх аудитів на підприємствах, установах та організаціях, на яких з тих самих питань і за той самий період підрозділом внутрішнього аудиту здійснено внутрішні аудити менше ніж один календарний рік тому (не поширюється на повторні аудити, що здійснюються підрозділом внутрішнього аудиту для дослідження фактів, викладених у скарзі на дії внутрішніх аудиторів, що надійшла до установи)

резервування обсягу робочого часу на проведення позапланових внутрішніх

План підписує керівник підрозділу внутрішнього аудиту, подає його на розгляд та затвердження керівнику установи не пізніше початку планового періоду



## ФОРМУВАННЯ ПЛАНУ ДІЯЛЬНОСТІ З ВНУТРІШНЬОГО АУДИТУ (ВНЕСЕННЯ ДО НЬОГО ЗМІН)

*ціль етапу: визначення переліку пріоритетних об'єктів внутрішнього аудиту на підставі оцінки потреб внутрішнього аудиту*

Зміни до планів вносяться:



у разі зміни стратегії (пріоритетів) та цілей діяльності державного органу

за результатами проведення оцінки ризиків

з інших обґрунтованих підстав

*(пункт 5 Стандарту 7)*

Внесення змін до плану письмово обґрунтовується керівнику державного органу  
*(пункт 5 Стандарту 7)*



## ФОРМУВАННЯ ПЛАНУ ДІЯЛЬНОСТІ З ВНУТРІШНЬОГО АУДИТУ (ВНЕСЕННЯ ДО НЬОГО ЗМІН)

*ціль етапу: визначення переліку пріоритетних об'єктів внутрішнього аудиту на підставі оцінки потреб внутрішнього аудиту*

Підрозділ внутрішнього аудиту щорічно забезпечує проведення (актуалізацію) оцінки ризиків:

здійснюється перегляд та уточнення застосованих критеріїв ймовірності та критеріїв впливу, присвоєних ризикам балів, забезпечується формування оновленого реєстру ризиків

здійснюється перегляд та уточнення застосованих факторів відбору

враховуються результати проведених внутрішніх аудитів за попередні роки

Результати проведення (актуалізації) оцінки ризиків оформлюються документально  
(пункт 3 Стандарту 7 «Планування діяльності з внутрішнього аудиту»)





## ПЛАНУВАННЯ ДІЯЛЬНОСТІ З ВНУТРІШНЬОГО АУДИТУ

Міністерство фінансів України аналізує плани, зокрема, на предмет:

дотримання вимог законодавства щодо ключових підходів до формування планів

дотримання вимог законодавства щодо забезпечення функціональної незалежності підрозділу внутрішнього аудиту

включення внутрішніх аудитів, спрямованих на оцінку ефективності, результативності та якості виконання завдань та функцій, визначених актами законодавства (планування внутрішніх аудитів з оцінки ефективності)

забезпечення належного рівня завантаженості внутрішніх аудиторів безпосередньо здійсненням внутрішніх аудитів

Рекомендації Мінфіну щодо забезпечення дотримання вимог законодавства під час формування планів, а також повноти та якості складання планів, їх інформаційного наповнення (зокрема, листи 23.08.2019 № 33040-06-5/21485, від 14.05.2020 № 33040-06-5/14303, від 26.05.2021 № 33040-06-5/16518, від 26.09.2021 № 33040-06-5/29483 та від 12.07.2022 № 33040-06-5/14881)