

**МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ**



Line

|  |
| --- |
| **Ризик-орієнтоване планування діяльності з внутрішнього аудиту** |
| Методичний посібник |

Line

**Київ**

**2024**

****

****

****

**М**етодичний посібник «Ризик-орієнтоване планування діяльності з внутрішнього аудиту» підготовлено Центральним підрозділом гармонізації з метою надання допомоги працівникам підрозділів внутрішнього аудиту державних органів у здійснення ризик-орієнтованого планування діяльності з внутрішнього аудиту, формуванні плану діяльності з внутрішнього аудиту на підставі результатів оцінки ризиків.

У цьому посібнику представлено підходи до складання та ведення бази даних щодо простору аудиту, організації, проведення та документування ідентифікації й оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту, формування та наповнення плану діяльності з внутрішнього аудиту, внесення до нього змін.

Використані у посібнику підходи базуються на положеннях, закладених у Керівництві «Оцінка ризиків при плануванні аудиту», підготовленому Співтовариством з взаємного вивчення та обміну досвідом в управлінні державними фінансами PEM PAL (квітень 2014 року), а також вітчизняному досвіді та кращих практиках діяльності з внутрішнього аудиту у державному секторі.



**Зміст**

[Перелік скорочень 3](#_top)

[Вступ 5](#_top)

[1. Визначення простору аудиту 7](#_Toc141119578)

[2. Визначення подій та ідентифікація ризиків 12](#_Toc141119579)

[3. Оцінка ризиків за впливом та ймовірністю 22](#_Toc141119580)

[4. Визначення об’єктів аудиту за допомогою факторів відбору 30](#_Toc141119581)

[5. Формування плану діяльності з внутрішнього аудиту (внесення змін до нього) 38](#_Toc141119582)

[6. Визначення у внутрішніх документах аспектів ризик-орієнтованого планування діяльності з внутрішнього аудиту 50](#_Toc141119583)

[Додатки 57](#_Toc141119584)

[*Додаток 1. Приклад формалізації та документування простору аудиту шляхом ведення бази даних*……………………………………………………………………………………...57](#_Toc141119585)

[*Додаток 2. Приклад поетапної процедури проведення та документування результатів ідентифікації й оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту* 74](#_Toc141119592)

[*Додаток 3. Приклад розрахунку потреби у ресурсах для забезпечення виконання плану діяльності з внутрішнього аудиту* 92](#_Toc141119593)

**Перелік скорочень**

****Терміни, використані у цьому Методичному посібнику, мають такі значення:

*база даних щодо простору аудиту* – документ, що складається, наповнюється, ведеться та оновлюється підрозділом внутрішнього аудиту державного органу, територіального органу державного органу та бюджетної установи, що містить інформацію стосовно об’єктів аудиту щодо яких можуть здійснюватися внутрішні аудити таким підрозділом внутрішнього аудиту;

*внутрішній аудитор, працівник підрозділу внутрішнього аудиту* – працівник підрозділу внутрішнього аудиту державного органу, територіального органу державного органу та бюджетної установи;

*зведена база даних щодо простору аудиту* – документ, що складається, наповнюється, ведеться та оновлюється підрозділом внутрішнього аудиту державного органу та включає інформацію стосовно сукупності об’єктів аудиту щодо яких можуть здійснюватися внутрішні аудити підрозділами внутрішнього аудиту системи державного органу(формується у розрізі підрозділу внутрішнього аудиту державного органу та підрозділів внутрішнього аудиту територіальних органів та бюджетних установ);

*зведений план* – план діяльності з внутрішнього аудиту, сформований підрозділом внутрішнього аудиту державного органу та затверджений керівником державного органу, який визначає пріоритети та результати діяльності підрозділів внутрішнього аудиту системи державного органу на наступні три роки, які враховують стратегію (пріоритети) та цілі діяльності державного органу, а також щорічно визначає завдання підрозділів внутрішнього аудиту системи державного органу на наступний календарний рік з урахуванням визначених пріоритетів та результатів роботи таких підрозділів внутрішнього аудиту на відповідний трирічний період (формується у розрізі підрозділу внутрішнього аудиту державного органу та підрозділів внутрішнього аудиту територіальних органів та бюджетних установ);

*інша діяльність з внутрішнього аудиту* – робота підрозділу внутрішнього аудиту, спрямована на розробку внутрішніх документів (методології) з питань внутрішнього аудиту; планування діяльності з внутрішнього аудиту; звітування (внутрішнє та зовнішнє) про результати діяльності підрозділу внутрішнього аудиту; моніторинг впровадження рекомендацій за результатами здійснення внутрішніх аудитів; проведення внутрішніх оцінок якості внутрішнього аудиту; підвищення кваліфікації та професійне навчання внутрішніх аудиторів; здійснення консультаційної діяльності;

*Методичні рекомендації з внутрішнього контролю* – Методичні рекомендації з організації внутрішнього контролю розпорядниками бюджетних коштів у своїх закладах та у підвідомчих бюджетних установах, затверджені наказом Мінфіну від 14.09.2012 № 995;

*МСВА* – Міжнародні стандарти професійної практики внутрішнього аудиту (International Professional Practices Framework, IPPF), підготовлені Інститутом внутрішніх аудиторів (The Institute of Internal Auditors, IIA);

*план* – план діяльності з внутрішнього аудиту, сформований підрозділом внутрішнього аудиту державного органу, територіального органу державного органу та бюджетної установи та затверджений керівником державного органу, територіального органу та бюджетної установи, який визначає пріоритети та результати діяльності таких підрозділів внутрішнього аудиту на наступні три роки, які враховують стратегію (пріоритети) та цілі діяльності державного органу, а також щорічно визначає завдання підрозділу внутрішнього аудиту державного органу, територіального органу державного органу та бюджетної установи на наступний календарний рік з урахуванням визначених пріоритетів та результатів роботи такого підрозділу внутрішнього аудиту на відповідний трирічний період;

*Основні засади внутрішнього контролю* – Основні засади здійснення внутрішнього контролю розпорядниками бюджетних коштів, затверджені постановою Кабінету Міністрів України від 12.12.2018 № 1062;

*підпорядковані підприємства/установи* – територіальні органи державних органів, а також державні підприємства, бюджетні установи та організації, які належать до сфери управління державного органу;

*підрозділ внутрішнього аудиту* – підрозділ внутрішнього аудиту або посадова особа, на яку покладено повноваження щодо здійснення внутрішнього аудиту, які утворені та функціонують у державному органі, його територіальних органах та бюджетних установах;

*постанова № 1001* – постанова Кабінету Міністрів України від 28.09.2011 № 1001 «Деякі питання здійснення внутрішнього аудиту та утворення підрозділів внутрішнього аудиту»;

*Порядок № 1001* – Порядок здійснення внутрішнього аудиту та утворення підрозділів внутрішнього аудиту, затверджений постановою Кабінету Міністрів України від 28.09.2011 № 1001;

*простір аудиту* – визначається підрозділом внутрішнього аудиту державного органу, підрозділами внутрішнього аудиту територіальних органів та бюджетних установ, який формалізовано та задокументовано шляхом ведення бази (зведеної бази) даних, її підтримки в актуальному стані, що включає інформацію стосовно сукупності об’єктів аудиту щодо яких можуть проводитися внутрішні аудити підрозділом внутрішнього аудиту державного органу, територіального органу та бюджетної установи;

*система державного органу* – апарат державного органу, територіальні органи державних органів, а також бюджетні установи, які належать до сфери управління державного органу;

*Стандарти* – Стандарти внутрішнього аудиту, затверджені наказом Мінфіну від 04.10.2011 № 1247, зареєстрованого у Мін’юсті 20.10.2011 за № 1219/19957;

*ЦПГ* – Центральний підрозділ гармонізації (Департамент гармонізації державного внутрішнього фінансового контролю Міністерства фінансів України).

– за таким умовним позначенням наведено вимоги законодавства у сфері внутрішнього аудиту та внутрішнього контролю, а також окремі поняття, на які слід особливо звертати увагу внутрішньому аудитору.

У цьому Методичному посібнику терміни «відповідальна за діяльність особа», «об’єкти внутрішнього аудиту», «державний орган», «бюджетна установа» / «установа» вживаються у значеннях, що застосовуються у Порядку № 1001 та Стандартах.

**Вступ**

**П**ланування діяльності з внутрішнього аудиту впливає на досягнення мети (місії) та цілей внутрішнього аудиту, виконання підрозділом внутрішнього аудиту завдань та функцій, визначених законодавством у сфері внутрішнього аудиту.

Основними завданнями підрозділу внутрішнього аудиту є надання керівнику установи об’єктивних і незалежних висновків та рекомендацій, які допомагають у підвищенні ефективності та результативності системи внутрішнього контролю, у тому числі процесів управління ризиками, удосконалення системи управління.

Водночас, підрозділ внутрішнього аудиту не повинен ставити за мету здійснення оцінки цілісної системи внутрішнього контролю, оскільки ресурси внутрішнього аудиту є обмеженими та не дозволяють одночасно охопити дослідженнями усі об’єкти аудиту, а тому повинні бути спрямовані на сфери діяльності, які є найбільш важливими та актуальними для ефективного управління державним органом.

Відбір підрозділом внутрішнього аудиту важливих та актуальних об’єктів аудиту та визначення пріоритетності їх дослідження є процесом ризик-орієнтованого планування діяльності з внутрішнього аудиту.

Процес ризик-орієнтованого планування діяльності з внутрішнього аудиту повинен розпочинатися з вивчення діяльності державного органу. Знання стратегії (пріоритетів) та цілей діяльності державного органу необхідно підрозділу внутрішнього аудиту для чіткого розуміння важливих та актуальних сфер (напрямів) діяльності державного органу, правильності формування думки про ризики у діяльності державного органу, визначення необхідних ресурсів на здійснення діяльності з внутрішнього аудиту та загалом вдалого аудиторського підходу для здійснення оцінки відповідних об’єктів аудиту.

В рамках ризик-орієнтованого планування діяльності з внутрішнього аудиту підрозділ внутрішнього аудиту повинен спочатку ідентифікувати та оцінити ризики з усієї сукупності об’єктів аудиту, надалі – визначити потенційні для дослідження об’єкти аудиту, встановити пріоритетність їх дослідження за допомогою факторів відбору та визначити частоту здійснення планових аудитів щодо кожного об’єкту аудиту. Під час ризик-орієнтованого планування з’ясовується та враховується думка керівника установи та проводяться консультації з відповідальними за діяльність особами щодо проблем та ризиків, які впливають на досягнення державним органом визначених цілей.

Застосування ризик-орієнтованого підходу до оцінки об’єкта аудиту під час планування діяльності з внутрішнього аудиту допомагає ефективніше розподіляти обмежені ресурси підрозділу внутрішнього аудиту та вирішує проблему підрозділу внутрішнього аудиту – як при обмежених ресурсах, відібрати об’єкти аудиту, які становлять ризик для досягнення мети та цілей діяльності державного органу. При цьому, ресурси, потреба в яких була визначена, повинні бути достатніми та адекватними, а також повинні ефективно використовуватись під час виконання плану діяльності з внутрішнього аудиту.

Вимоги щодо формування плану діяльності з внутрішнього аудиту на підставі результатів оцінки ризиків передбачено пунктом 6 Порядку № 1001 та Стандартом 7 «Планування діяльності з внутрішнього аудиту». Аналогічні вимоги містяться у МСВА (стандарти 2000 «Управління функцією внутрішнього аудиту», 2010 «Планування», 2020 «Надання інформації та затвердження», 2030 «Управління ресурсами»).

Процес формування плану діяльності з внутрішнього аудиту на підставі результатів оцінки ризиків включає п’ять послідовних етапів:

* визначення простору аудиту (усієї сукупності об’єктів аудиту), забезпечення розподілу об’єктів аудиту у просторі аудиту за горизонтальним та вертикальним принципами (описано у розділі 1). Приклад формалізації та документування простору аудиту шляхом ведення бази даних наведено у [***додатку 1***](#_Додаток_1._Приклад);
* ідентифікація ризиків щодо кожного об’єкта аудиту, включеного до бази даних щодо простору аудиту (включаючи підходи до ідентифікації ризиків якщо у діяльності установи забезпечено здійснення управління ризиками та визначено підходи щодо документування управління ризиками, а також якщо управління ризиками в установі не запроваджене) (описано у розділі 2);
* проведення оцінки ризиків за визначеними критеріями впливу/критеріями ймовірності та шкалою оцінювання ризиків, узагальнення результатів ідентифікації та оцінки ризиків (описано у розділі 3). Приклад проведення та документування процедури ідентифікації й оцінки ризиків наведено у [***додатку 2***](#_Додаток_8._Приклад);
* визначення пріоритетних об’єктів аудиту з метою включення до плану діяльності з внутрішнього аудиту (із застосуванням набору факторів відбору, оцінки кожного фактору за допомогою бальних оцінок та вагових коефіцієнтів, визначення ступеня пріоритету об’єктів аудиту та частоти здійснення планових внутрішніх аудитів щодо кожного об’єкта аудиту на підставі розрахунку індексу пріоритетності, визначення загального періоду внутрішнього аудиту (описано у розділі 4)). Приклад проведення та документування процедури ідентифікації й оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту наведено у [***додатку 2***](#_Додаток_8._Приклад);
* формування та затвердження плану діяльності з внутрішнього аудиту на підставі результатів оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту (з урахуванням визначення підрозділом внутрішнього аудиту потреб/обмежень у ресурсах для забезпечення виконання запланованої діяльності), внесення змін до плану (включаючи підходи до актуалізації оцінки ризиків) (описано у розділі 5). Форми плану діяльності з внутрішнього аудиту (плану із змінами), зведеного плану діяльності з внутрішнього аудиту (зведеного плану із змінами) та рекомендації щодо складання таких планів розміщено на офіційному вебсайті Мінфіну у рубриці «Зразки документів з внутрішнього контролю та внутрішнього аудиту» розділу «Державний внутрішній фінансового контроль» глави «Діяльність». Приклад розрахунку підрозділом внутрішнього аудиту потреб у ресурсах для забезпечення виконання плану діяльності з внутрішнього аудиту наведено у [***додатку 3***](#_Додаток_3._Форма).

Підходи до складання та ведення бази даних щодо простору аудиту, організації, проведення та документування ідентифікації й оцінки ризиків, визначення факторів відбору для здійснення планових внутрішніх аудитів та частоти їх здійснення щодо кожного об’єкта аудиту повинні визначатися у внутрішніх документах з питань здійснення внутрішнього аудиту в частині планування (питання, які мають бути врегульовано у внутрішніх документах описано у розділі 6).

**1. Визначення простору аудиту**

**В**изначення простору аудиту є відправною точкою для розробки плану діяльності з внутрішнього аудиту. Ціль етапу – визначити та описати потенційні об’єкти, які окремо можна дослідити під час здійснення внутрішнього аудиту.

Поняття простору аудиту, вимоги щодо визначення підрозділом внутрішнього аудиту простору аудиту, його формалізації та документування шляхом ведення бази даних та її підтримки в актуальному стані передбачено пунктом 3 розділу І Стандартів та пунктом 1 Стандарту 7 «Планування діяльності з внутрішнього аудиту».

***П****ростір внутрішнього аудиту – сукупність об’єктів внутрішнього аудиту, а також підприємств, установ та організацій, що належать до сфери управління державного органу, щодо діяльності яких можуть проводитись внутрішні аудити (вимоги пункту 3 розділу І Стандартів).*

***П****ідрозділ внутрішнього аудиту забезпечує визначення простору внутрішнього аудиту.*

***П****ростір внутрішнього аудиту має бути формалізований та задокументований шляхом ведення бази даних та її підтримання в актуальному стані (вимоги пункту 1 Стандарту 7 «Планування діяльності з внутрішнього аудиту»)*

Простір аудиту – це простий спосіб визначення всього, чи сукупності всього, що можливо окремо дослідити під час здійснення внутрішнього аудиту.

Під поняттям **«простір аудиту»** розуміється загальна сфера застосування функції внутрішнього аудиту, **сукупність об’єктів аудиту** щодо яких можуть здійснюватися внутрішні аудити.

Простір аудиту повинен визначати та описувати об’єкти аудиту, які окремо можна дослідити під час здійснення внутрішнього аудиту (напрями (сфери) діяльності установи або їх частини – бюджетні програми, адміністративні послуги, контрольно-наглядові функції, загальні та функціональні процеси).

Крім того, простір аудиту передбачає включення інформації щодо структурних підрозділів установи, а також підприємств, установ та організацій, які належать до сфери управління державного органу, які відповідають за реалізацію відповідних програм / послуг / функцій / процесів.

Під час визначення простору аудиту слід врахувати, що об’єкти аудиту повинні мати такий масштаб, щоб проведення внутрішнього аудиту щодо такого об’єкта було 1) доцільним та 2) якісним і результативним (тобто об’єкт аудита не повинен бути занадто великим та занадто малим). Наприклад, окремими підрозділами внутрішнього аудиту в просторі аудиту зазначається в якості об’єкта аудиту «система внутрішнього контролю» або «організація системи внутрішнього контролю» чи «функціонування системи внутрішнього контролю». Водночас, з огляду на законодавче визначення «системи внутрішнього контролю», здійснення внутрішнього аудиту по відношенню до такого об’єкта аудиту буде для підрозділу внутрішнього аудиту занадто затратним – за часовими та трудовими витратами та загалом може не дати результатів, які очікуються від підрозділу внутрішнього аудиту.

***С****истема внутрішнього контролю – впроваджені керівником установи політики, правила і заходи, які забезпечують функціонування, взаємозв’язок та підтримку всіх елементів внутрішнього контролю і спрямовані на досягнення визначених мети (місії), стратегічних та інших цілей, завдань, планів і вимог щодо діяльності установи (вимоги абзацу четвертого пункту 2 Основних засад з внутрішнього контролю)*

Приклади формулювання об’єктів аудиту наведено у [***додатку 1***](#_Додаток_1._Приклад).

Розподіл об’єктів аудиту у просторі аудиту доцільно здійснювати відповідно до функціонального аспекту діяльності державного органу **(горизонтальний розподіл)**, а також організаційної структури та підпорядкування – центральний, обласний чи районний рівні (зверху-вниз) **(вертикальний розподіл)**.

Наразі більшість підрозділів внутрішнього аудиту під час визначення простору аудиту широко використовує вертикальний розподіл. Такий підхід до визначення простору аудиту завжди є найзручнішим, проте він може виявитися не самим ефективним способом для визначення об’єктів аудиту.

Тому важливо розділяти простір аудиту також за горизонтальним принципом, який базується на визначених законодавством напрямах (сферах) діяльності установи. Наприклад, системи управління чи обліку мають вплив на діяльність усіх структурних підрозділів державного органу, а також підприємств, установ та організацій, які належать до сфери управління державного органу. Такі об’єкти аудиту можуть представляти найбільший ризик для декількох функцій (програм, послуг, процесів), тому повинні досліджуватися за горизонтальним підходом.

Керівник підрозділу внутрішнього аудиту самостійно вирішує якою буде структура простору аудиту. Водночас, слід враховувати специфіку діяльності державного органу, розмір та структуру підрозділів внутрішнього аудиту, складність об’єктів аудиту.

Простір внутрішнього аудиту доцільно структурувати за такими категоріями:

**напрямами (сферами) діяльності державного органу або їх частинами (горизонтальний принцип розподілу об’єктів аудиту)**:

* бюджетними програми, реалізацію яких здійснює державний орган відповідно до покладених на нього функцій;
* адміністративними послугами, які надаються державним органом відповідно до вимог законодавства;
* контрольно-наглядовими функціями, які здійснюються державним органом відповідно до вимог законодавства;
* загальними процесами (стандартні процеси, притаманні діяльності кожного державного органу). Наприклад, стратегічне (річне) планування діяльності, управління об’єктами державної власності, фінансово-господарська діяльність, державні закупівлі, управління інформаційними потоками та інформаційна безпека, міжнародна діяльність, правова робота, управління персоналом, взаємодія з медіа та громадськістю, діяльність з запобігання та виявлення корупції, цивільний захист та охорона праці;
* функціональними процесами (специфічні процеси, характерні для відповідних державних органів). На відміну від загальних процесів, функціональні процеси можуть не покривати діяльність усіх структурних підрозділів державного органу, підприємств, установ та організацій, які належать до сфери його управління, а реалізовуватись в окремих з них;

**організаційною структурою та місцем розташування (вертикальний принцип розподілу об’єктів аудиту)**:

* структурними підрозділами державного органу (директорати, департаменти, управління, відділи, сектори, окремі посадові особи, які функціонують у структурі державного органу);
* територіальними органами державного органу та підприємствами, установами та організаціями, які належать до сфери його управління (функціонують на центральному, обласному чи районному рівнях).

З метою розподілу простору аудиту за категоріями використовуються такі документальні джерела інформації, зокрема:

* законодавчі та нормативно-правові акти, що регулюють діяльність державних органів, а також установ, підприємств, організацій, які належать до сфери його управління. В таких документах визначено завдання та функції, права та обов’язки, правовий статус та підпорядкування;
* стратегічні та операційні плани (річні, піврічні, квартальні), в яких описуються мета (місія) та стратегічні цілі (пріоритети) діяльності державного органу, завдання та заходи з їх реалізації, кінцеві результати (індикатори) виконання завдань, визначаються відповідальні виконавці (співвиконавці);
* внутрішні документи установи (організаційна структура, положення про структурні підрозділи, посадові інструкції, відповідні порядки та регламенти). В таких документах міститься перелік структурних підрозділів, визначено повноваження та відповідальність (підзвітність) керівництва та працівників, розподіл повноважень та відповідальності (підзвітності), їх закріплення за виконавцями (співвиконавцями), встановлено порядок складання та подання звітності про результати діяльності, включаючи результативні показники щодо досягнення поставлених завдань, рівні, форми та терміни звітування, визначено порядки планування, організації, здійснення окремих процесів;
* паспорти бюджетних програм, фінансові плани державних підприємств, звітність (річна та періодична фінансова, інша нефінансова звітність), які містять показники діяльності бюджетних установ/державних підприємств;
* аудиторські звіти підрозділу внутрішнього аудиту та акти/звіти зовнішніх контролюючих органів, в яких міститься інформація щодо недоліків системи внутрішнього контролю та фактів порушень, а також наданих висновків та рекомендацій/обов’язкових вимог.

Вивчення документів сприяє належному розумінню діяльності державного органу, встановленню зв’язку між програми/послугами/функціями/процесами та структурними підрозділами державного органу/підпорядкованими підприємствами/установами, відповідальними за реалізацію відповідних програм/послуг/функцій/процесів, а також впливає на правильне визначення об’єктів аудиту. За допомогою аналізу документів підрозділ внутрішнього аудиту може виявити зміни у просторі аудиту та провести комплексну оцінку та актуалізацію всіх об’єктів аудиту, включених до простору аудиту.

У рамках визначення простору аудиту підрозділу внутрішнього аудиту доцільно проводити консультації з вищим керівництвом установи та відповідальними за діяльність особами (керівниками структурних підрозділів установи та підпорядкованих підприємств/установ, які відповідають за програми/послуги/функції/процеси, що можуть бути потенційними об’єктами аудиту для підрозділу внутрішнього аудиту).

Під час проведення таких консультацій доцільно обговорити визначені підрозділом внутрішнього аудиту об’єкти аудиту, а також питання, пов’язані з організацією та здійсненням внутрішнього контролю в установі (включаючи діючі заходи контролю), зокрема:

* основні цілі та ролі структурних підрозділів у досягненні цілей діяльності установи;
* питання, що цікавлять керівництво установи, на які слід звернути увагу підрозділу внутрішнього аудиту (зокрема, щодо ефективності та результативності діяльності структурних підрозділів установи, досягнення цілей діяльності установи);
* з’ясувати думку відповідальних за діяльність осіб щодо повноти визначених підрозділом внутрішнього аудиту об’єктів аудиту, їх важливості та актуальності, достатності/недостатності або надмірного рівня деталізації об’єктів аудиту;
* результати контрольних заходів (державних фінансових аудитів, ревізій, перевірок тощо), проведених протягом року зовнішніми контролюючими органами (Рахунковою палатою, органами державного фінансового контролю тощо) у системі державного органу.

Документування результатів консультацій підрозділом внутрішнього аудиту з вищим керівництвом установи та відповідальними за діяльність особами з питань формування та оновлення інформації у базі даних щодо простору аудиту здійснюється за аналогічними процедурами, передбаченими для проведення та документування результатів консультацій з питань проведення оцінки ризиків з метою планування діяльності з внутрішнього аудиту (описано у розділі 2 «Визначення подій та ідентифікація ризиків»).

Консультації з питань формування та оновлення інформації у базі даних щодо простору аудиту можуть проводиться одночасно з консультаціями з питань проведення оцінки ризиків, оскільки за результатами проведення консультацій з питань оцінки ризиків може виникнути потреба в актуалізації (уточненні) інформації у базі даних щодо раніше визначених об’єктів аудитів.

Актуалізацію (уточнення) простору аудиту доцільно здійснювати не рідше одного разу на рік – до початку формування плану діяльності з внутрішнього аудиту на наступні планові періоди (рекомендовано до 30 листопада).

Вимоги щодо забезпечення ведення зведеної бази даних щодо простору аудиту підрозділом внутрішнього аудиту державного органу у разі утворення підрозділів внутрішнього аудиту у територіальних органах та бюджетних установах передбачено абзацом третім пункту 1 Стандарту 7 «Планування діяльності з внутрішнього аудиту».

***У*** *разі утворення підрозділів внутрішнього аудиту у територіальних органах та бюджетних установах підрозділ внутрішнього аудиту державного органу забезпечує ведення зведеної бази даних щодо простору внутрішнього аудиту (вимоги абзацу третього пункту 1 Стандарту 7 «Планування діяльності з внутрішнього аудиту»)*

До зведеної бази даних щодо простору аудиту заноситься інформація щодо об’єктів аудиту у розрізі підрозділу внутрішнього аудиту державного органу та підрозділів внутрішнього аудиту територіальних органів та бюджетних установ. Зведена база даних формується та ведеться за аналогічними процедурами, визначеним для складання та ведення бази даних щодо простору аудиту.

Ведення бази (зведеної бази) даних рекомендується здійснювати в електронному вигляді з використанням програми MS Office Excel.

Приклад формалізації та документування простору аудиту шляхом ведення бази даних з використанням можливостей Microsoft Excel проілюстровано у [***додатку 1***,](#_Додаток_1._Приклад)а також розміщено на офіційному вебсайті Мінфіну у рубриці «Зразки документів з внутрішнього контролю та внутрішнього аудиту» розділу «Державний внутрішній фінансового контроль» глави «Діяльність».

**2. Визначення подій та ідентифікація ризиків**

**Н**аступним кроком після визначення простору аудиту є **ідентифікація ризиків**. Ціль етапу – досягнення внутрішніми аудиторами глибокого розуміння ризиків у діяльності установи з метою правильного формування аудиторської думки про ризики, пов’язані з об’єктами аудиту.

Вимоги щодо формування плану діяльності з внутрішнього аудиту на підставі результатів оцінки ризиків, яка має бути документально оформлена, та проводиться не рідше одного разу на рік передбачено абзацом третім пункту 6 Порядку № 1001 та пунктами 2, 3 Стандарту 7 «Планування діяльності з внутрішнього аудиту».

***П****лан формується підрозділом на підставі результатів оцінки ризиків… (вимоги абзацу третього пункту 6 Порядку № 1001).*

***К****ерівник підрозділу внутрішнього аудиту забезпечує формування плану на підставі результатів оцінки ризиків… (вимоги пункту 2 Стандарту 7 «Планування діяльності з внутрішнього аудиту»).*

***П****лан формується підрозділом внутрішнього аудиту на підставі документально оформленої оцінки ризиків, яка проводиться не рідше одного разу на рік (вимоги пункту 3 Стандарту 7 «Планування діяльності з внутрішнього аудиту»)*

Під час планування діяльності з внутрішнього аудиту підрозділ внутрішнього аудиту повинен врахувати запроваджені в установі підходи до управління ризиками.

Відповідно до вимог Основних засад внутрішнього контролю питання управління ризиками включають здійснення ідентифікації ризиків; оцінювання ідентифікованих ризиків за ймовірністю їх виникнення та суттєвістю впливу; обрання способів реагування на ідентифіковані та оцінені ризики (зменшення, прийняття, розділення чи уникнення); інформування керівництва установи про проведену оцінку ризиків, ризикові сфери діяльності установи для прийняття рішення щодо вжиття заходів контролю; здійснення перегляду ідентифікованих та оцінених ризиків для виявлення нових та таких, що зазнали змін; визначення відповідальних посадових осіб за здійснення координації управління ризиками; визначення підходів щодо документування управління ризиками.

***У****правління ризиками – діяльність керівництва та працівників установи з ідентифікації ризиків, проведення їх оцінки, визначення способів реагування на ідентифіковані та оцінені ризики, здійснення перегляду ідентифікованих та оцінених ризиків для виявлення нових та таких, що зазнали змін (вимоги абзацу третього пункту 5 Основних засад внутрішнього контролю)*

У тих випадках, коли у діяльності установи забезпечено здійснення управління ризиками та визначено підходи щодо документування управління ризиками, підрозділ внутрішнього аудиту повинен:

* дослідити внутрішні документи, що стосуються питань управління ризиками, та виконання вимог цих документів керівництвом та працівниками установи, а також своєчасність надання керівництву та працівникам установи інформації з питань управління ризиками;
* проаналізувати ідентифіковані відповідальними за діяльність особами ризики з метою розуміння подій, які призвели до виникнення ризиків, а також визначити повноту виявлення ризиків відповідальними за діяльність особами;
* проаналізувати ідентифіковані ризики, які було оцінено відповідальними за діяльність особами, та обрані ними способи реагування на ризики, оцінити обрані відповідальними за діяльність особами способи реагування на ризики та порівняти їх з судженням працівників підрозділу внутрішнього аудиту;
* дослідити заходи контролю, які було запроваджено відповідальними за діяльність особами з метою зменшення ризиків, оцінити їх достатність (на думку внутрішніх аудиторів) – до якого рівня заходи контролю забезпечують зниження залишкових ризиків та як співвідносяться залишкові ризики та прийнятний рівень ризику. Під час ризик-орієнтованого планування підрозділ внутрішнього аудиту, в першу чергу, цікавить рівень залишкового ризику. В окремих випадках залишковий ризик може дорівнювати невід’ємному ризику. Наприклад, коли новостворена установа та/або відсутня інформація про ефективність заходів контролю;

***П****рийнятний ризик (або «ризик-апетит», «апетит на ризик») – рівень ризику, що приймається керівництвом установи як несуттєвий. Водночас, застосування ефективних заходів контролю дозволяє знижувати рівень ризику до прийнятного рівня (наприклад, у добре контрольованих системах внутрішнього контролю та управління ризиками).*

***З****алишковий ризик – рівень ризику після (або без аналізу інформації про) вжиття керівництвом установи та відповідальними за діяльність особами заходів контролю щодо зменшення ризику.*

***Н****евід’ємний ризик – рівень ризику до вжиття керівництвом та відповідальними за діяльність особами заходів контролю*

* проаналізувати ефективність запроваджених відповідальними за діяльність особами заходів контролю щодо зменшення ризиків з точку зору їх впливу на залишкові ризики. Під час аналізу слід використовувати інформацію, одержану як із зовнішніх джерел, так і наявну у підрозділі внутрішнього аудиту інформацію;
* виявити неідентифіковані відповідальними за діяльність особами ризики та залишкові ризики, які, незважаючи на запроваджені заходи контролю, можуть залишатися високими;
* задокументувати процедуру ідентифікації та оцінки виявлених підрозділом внутрішнього аудиту ризиків, які не було виявлено відповідальними за діяльність особами, та залишкових ризиків.

Результати проведеного аналізу обговорюються працівниками підрозділу внутрішнього аудиту з відповідальними за діяльність особами, зокрема, під час проведення консультацій з питань оцінки ризиків з метою планування діяльності з внутрішнього аудиту. У разі отримання від відповідальних за діяльність осіб обґрунтованих відповідей щодо визначених ними ризиків, обраних способів реагування на ризики, розроблених заходів контролю для впливу на ризики тощо підрозділом внутрішнього аудиту здійснюється заповнення (уточнення) інформації щодо ідентифікації та оцінки ризиків, загальної оцінки ризиків.

Якщо в установі забезпечено здійснення управління ризиками та визначено підходи щодо документування управління ризиками, доцільно унормувати внутрішніми документами вимогу щодо надання структурними підрозділами установи та підпорядкованими підприємствами/установами копій відповідних документів / інформації (про результати ідентифікованих та оцінених ризиків, визначених способів реагування на ризики, розроблених заходів контролю для впливу на ризики) підрозділу внутрішнього аудиту для врахування під час ідентифікації та оцінки ризиків з метою планування діяльності з внутрішнього аудиту.

Підхід до визначення ризиків підрозділом внутрішнього аудиту буде відрізнятися, якщо управління ризиками в установі не запроваджене. У таких випадках внутрішні аудитори самостійно визначають події, які призводять до виникнення ризиків, проводять ідентифікацію та оцінку ризиків щодо впливу на досягнення цілей діяльності установи та ймовірності виникнення ризиків. Така робота є набагато складнішою та вимагає більше часу, ніж у тих випадках, коли у діяльності установи забезпечено здійснення управління ризиками та визначено підходи щодо документування управління ризиками.

У таких випадках існують документальні джерела, які допоможуть підрозділу внутрішнього аудиту виявити ризики. При цьому, внутрішні аудитори повинні використовувати найбільш об’єктивні та актуальні джерела інформації.

Під час визначення ризиків підрозділом внутрішнього аудиту, зокрема:

* враховується широкий спектр фінансових/нефінансових відомостей, а саме:

інформація про типові/системні порушення та недоліки, встановлені за результатами попередніх внутрішніх аудитів;

повідомлення структурних підрозділів/підприємств, установ та організацій про проблемні питання та ризики у їх діяльності;

інформація з медіа, скарг, звернень державних органів, народних депутатів, правоохоронних органів, зовнішніх контролюючих органів;

інформація щодо звітності (зокрема, з фінансової та бюджетної звітності, звітів про виконання паспорту бюджетної програми, звітів про виконання фінансових планів державних підприємств);

* здійснюється аналіз документальних джерел таких як:

нормативно-правові акти, які регулюють діяльність установи;

стратегічні плани діяльності установи, річні, піврічні, квартальні плани діяльності установи;

внутрішні документи (наприклад, положення про структурні підрозділи, в яких визначено завдання та функції, права та обов’язки працівників, порядки та регламенти, які визначають відповідні функції/процеси/процедури);

щорічні звіти про діяльність установи;

звіт про стан організації та здійснення внутрішнього контролю у розрізі елементів внутрішнього контролю державного органу, який щорічно подається Мінфіну відповідно до вимог пункту 10 Основних засад внутрішнього контролю (описує фактичний стан функціонування елементів внутрішнього контролю, зокрема, управління ризиками);

звіти за результатами проведення попередніх внутрішніх аудитів;

акти/звіти зовнішніх контрольних заходів (ревізій, перевірок, державних фінансових аудитів), проведених зовнішніми контролюючими органами (Рахунковою палатою, органами державного фінансового контролю тощо).

До найбільш розповсюджених методів виявлення ризиків також належать консультації, які проводять працівники підрозділу внутрішнього аудиту з вищим керівництвом установи та відповідальними за діяльність особами (керівниками структурних підрозділів установи та підпорядкованих підприємств/установ, які відповідають за програму/послугу/функцію/процес, що можуть бути потенційними об’єктами аудиту для підрозділу внутрішнього аудиту).

Вимога щодо з’ясування та врахування думки керівника установи, а також проведення консультації з відповідальними за діяльність особами щодо проблемних питань та ризиків, які впливають на досягнення установою цілей передбачена абзацом другий пункту 2 Стандарту 7 «Планування діяльності з внутрішнього аудиту».

Думка вищого керівництва установи щодо проблемних питань та ризиків, які впливають на досягнення установою цілей, завжди є важливою для визначення ризиків під час планування діяльності з внутрішнього аудиту. Адже об’єктивність оцінки ризиків може бути зменшена і, як наслідок, відібрані до плану об’єкти аудиту будуть не актуальними, а їх результати не цікавими для вищого керівництва установи.

***З*** *метою формування плану керівник підрозділу внутрішнього аудиту повинен з’ясувати та врахувати думку керівника установи, а також провести консультації з відповідальними за діяльність особами щодо проблемних питань та ризиків, які впливають на досягнення установою цілей (вимоги абзацу другого пункту 2 Стандарту 7 «Планування діяльності з внутрішнього аудиту»).*

***Д****о завдань аудиторського комітету за рішенням керівника державного органу може бути віднесено…надання фахових консультацій та розгляд питань, пов’язаних з організацією та здійсненням внутрішнього контролю та/або функціонуванням окремих його елементів, і підготовка рекомендацій з їх удосконалення (вимоги абзацу вісімнадцятого пункту 15-1 Порядку № 1001)*

З метою виявлення ризиків проводяться консультації з відповідальними за діяльність особами, оскільки вони більш за інших обізнані щодо нюансів реалізації програм/послуг/функцій/процесів, за які відповідають.

Якщо в державному органі функціонує аудиторський комітет та до його завдань віднесено, серед іншого, надання фахових консультацій та розгляд питань, пов’язаних з організацією та здійсненням внутрішнього контролю та/або функціонуванням окремих його елементів, підрозділ внутрішнього аудиту може проводити консультації також з аудиторським комітетом.

Проведення внутрішніми аудиторами консультацій з вищим керівництвом та відповідальними за діяльність особами здійснюється шляхом опитування (інтерв’ювання та/або анкетування). Повноваження щодо проведення працівниками підрозділу внутрішнього аудиту опитування (інтерв’ювання та/або анкетування) працівників державного органу, його територіального органу, підприємства, установи, організації, що належить до сфери управління державного органу, з питань, що стосуються їх діяльності (за згодою), передбачено вимогами підпункту 2 пункту 12 Порядку № 1001.

***П****рацівники підрозділу мають право:*

*…проводити опитування (інтерв’ювання та/або анкетування) працівників державного органу, його територіального органу, підприємства, установи, організації, що належить до сфери управління державного органу, з питань, що стосуються їх діяльності (за згодою) (вимоги підпункту 2 пункту 12 Порядку № 1001)*

Під час проведення підрозділом внутрішнього аудиту консультацій, зокрема:

* + обговорюються проблемні питання та ризики у діяльності структурних підрозділів державного органу, а також підприємств, установ та організацій, що належать до сфери його управління;
  + обговорюються обрані вищим керівництвом та відповідальними за діяльність особами заходи щодо управління ризиками (зокрема, способи реагування на ризики, розроблені заходи контролю для впливу на ідентифіковані та оцінені ризики), їх вплив на рівень залишкового ризику;
  + визначається правильність судження підрозділу внутрішнього аудиту про прийнятий керівництвом установи рівень ризику та невід’ємний рівень ризику;
  + обговорюються ідентифіковані та оцінені підрозділом внутрішнього аудиту ризики (якщо управління ризиками в установі не запроваджене);
  + обговорюються питання щодо повноти ідентифікованих відповідальними за діяльність особами ризиків, доцільності та дієвості обраних ними способів реагування на ризики, ефективності розроблених заходів контролю для впливу на ризики (за результатами проведеного підрозділом внутрішнього аудиту аналізу документів (інформації) з питань управління ризиками);
  + запитуються пропозиції щодо здійснення внутрішніх аудитів у ризикових сферах діяльності установи (зокрема, щодо тематики внутрішніх аудитів, питань, на які слід звертати увагу під час планування та проведення аудиторських досліджень), при цьому, з’ясовуються причини, які зумовлюють необхідність проведення внутрішніх аудитів у таких сферах.

З метою отримання відповідної інформації працівники підрозділу внутрішнього аудиту проводять консультації шляхом:

* + особистого спілкування (через проведення інтерв’ювання посадових осіб, у тому числі використовуючи сучасні онлайн-інструменти та платформи (такі як Zoom, Google Meet тощо);
  + непрямого спілкування (через направлення письмових запитів посадовим особам, у тому числі розроблених підрозділом внутрішнього аудиту анкет для заповнення посадовими особами).

Консультації рекомендовано проводити щорічно (не пізніше 15 листопада).

До початку проведення консультацій працівники підрозділу внутрішнього аудиту:

* + визначають формат проведення консультацій (шляхом особистого спілкування або непрямого спілкування чи поєднують обидва формати під час консультацій), планують яким чином буде здійснюватися аналіз отриманих результатів;
  + забезпечують розробку опитувальника для проведення консультацій (зокрема, визначають перелік питань для надання відповідей, структуру (форму) анкети для заповнення посадовими особами);
  + здійснюють вибірку структурних підрозділів установи, підпорядкованих підприємств/установ, з якими будуть проводитись консультації;
  + визначають працівників підрозділу внутрішнього аудиту, які будуть проводити консультації з відповідними посадовими особами.

Результати проведених підрозділом внутрішнього аудиту консультацій (особистого спілкування з вищим керівництвом установи та відповідальними за діяльність особами) оформлюються документально та можуть містити інформацію, зокрема, щодо:

* мети (цілей) проведення консультацій (наприклад, з метою проведення підрозділом внутрішнього аудиту оцінки ризиків для формування плану діяльності з внутрішнього аудиту на наступний трирічний період та/або з метою здійснення підрозділом внутрішнього аудиту формування та оновлення інформації щодо об’єктів аудиту у базі даних щодо простору аудиту);
* даних посадових осіб установи, з якими проводилися консультації (прізвище, ім’я, посада тощо);
* переліка питань, які обговорювалися під час проведення консультацій;
* відповідей, наданих посадовими особами установи, під час проведення консультацій;
* даних посадових осіб підрозділу внутрішнього аудиту, які проводили консультації (прізвище, ім’я, посада тощо) із зазначенням місця та дати проведення консультацій.

З метою забезпечення додаткової впевненості щодо точності та об’єктивності інформації, отриманої під час консультацій, працівниками підрозділу внутрішнього аудиту може надаватися проект консультацій опитуваним посадовим особам для ознайомлення та надання за необхідності додаткової або уточненої інформації. У разі надання опитуваними посадовими особами додаткової /уточненої інформації працівники підрозділу внутрішнього аудиту забезпечують розгляд такої інформації та вносять корективи до проекту консультацій (за необхідності).

Задокументовані результати консультацій (інтерв’ювання) підписуються працівниками підрозділу внутрішнього аудиту, які проводили такі консультації, а також можуть підписуватися опитуваними посадовими особами (за їх згодою).

Проведення підрозділом внутрішнього аудиту консультацій (інтерв’ю) з метою планування діяльності з внутрішнього аудиту здійснюється за аналогічними підходами, які застосовуються у процесі здійснення внутрішнього аудиту (описані у методичному посібнику «Внутрішній аудит ефективності: Методичні засади та практичні аспекти», розміщеному на офіційному вебсайті Мінфіну у рубриці «Методичні посібники щодо ДВФК» розділу «Державний внутрішній фінансового контроль» глави «Діяльність»).

Проведення підрозділом внутрішнього аудиту консультацій з вищим керівництвом установи та відповідальним за діяльність особам шляхом направлення письмових запитів (непряме спілкування), у тому числі розроблених підрозділом внутрішнього аудиту анкет для заповнення, здійснюється відповідно до регламентів (процедур), встановлених внутрішніми документами установи та запровадженої в установі практики щодо здійснення відповідної роботи. Наприклад, в одних установах забезпечується обмін інформацією виключено через направлення письмових запитів (листів). В інших установах для одержання інформації працівники використовують також сучасні онлайн-інструменти (зокрема, goole forms), які дозволяють проводити консультації, у тому числі анонімно (наприклад, через заповнення анкет посадовими особами).

Під час підготовки працівниками підрозділу внутрішнього аудиту письмових запитів може наводиться інформація, зокрема, щодо мети (цілей) проведення консультацій; переліку питань, на які слід надати письмову відповідь; термінів надання відповідей на письмовий запит підрозділу внутрішнього аудиту.

Під час документування результатів консультацій працівники підрозділу внутрішнього аудиту мають зазначати лише факти, отримані під час проведення консультацій, виключаючи власну думку внутрішніх аудиторів, які проводили консультації.

Результати консультацій працівники підрозділу внутрішнього аудиту опрацьовують шляхом узагальнення та аналізу отриманої інформації та враховують під час планування діяльності з внутрішнього аудиту (зокрема, шляхом заповнення (уточнення) інформації щодо ідентифікації та оцінки ризиків, загальної оцінки ризиків, оцінки факторів відбору).

Документально оформлені результати консультацій додаються до документів (інформації) з питань оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту та зберігаються у підрозділі внутрішнього аудиту.

Водночас, не варто обирати тільки один спосіб виявлення ризиків – лише на підставі аналізу документальних джерел або за результатами проведених консультацій. Адже, документи розробляються для реалізації відповідних програм/послуг/функцій/процесів, однак вони можуть не охоплювати питання, які потрібні підрозділу внутрішнього аудиту для виявлення та оцінки ризиків. Аналогічно, результати консультацій можуть виявитися сумнівними через намагання опитуваних приховати існуючі проблеми та/або не привертати увагу до своєї діяльності взагалі. Загалом результати консультацій практично завжди нерівнозначні, наприклад, в одних випадках опитані можуть наводити «дрібні» ризики, а в інших – занадто «глобальні» ризики. Інколи опитуваним важко вникнути у сутність поняття «ризику», тому, замість ризиків, зазначаються негативні події, які виникали у минулому.

З метою виявлення ризиків корисно проводити колективне обговорення у підрозділі внутрішнього аудиту різних подій, які можуть створювати ризики у діяльності установи («сесії мозкового штурму»). Ризики легше виявляти, якщо зрозуміти події, які впливають на досягнення визначених установою цілей. На такі зустрічі доцільно запрошувати відповідальних за діяльність осіб, де в форматі діалогу та обговорення виробляються спільні рішення щодо зменшення впливу ризиків.

З метою об’єктивності та повноти виявлення ризиків підрозділ внутрішнього аудиту повинен застосовувати одночасно декілька способів виявлення ризиків (зокрема, за результатами аналізу документальних джерел, проведення консультацій з вищим керівництвом установи та відповідальними за діяльність особами, «сесій мозкового штурму», проведених у підрозділі внутрішнього аудиту).

Під час визначення ризиків також корисними є знання та досвід, отримані внутрішніми аудиторами за результатами здійснення внутрішніх аудитів.

Після проведеної підрозділом внутрішнього аудиту роботи щодо виявлення ризиків стосовно кожного об’єкта аудиту у базі даних щодо простору аудиту ідентифікуються події (зовнішні та внутрішні), що можуть вплинути на досягнення установою визначених цілей та які, залежно від впливу, поділяються на можливості (позитивний вплив на досягнення установою визначених цілей) та ризики (негативний вплив на досягнення установою визначених цілей).

У таблиці представлено класифікацію подій, що можуть створювати ризики:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Події, що створюють ризики | | | | |
| Операційні | **ІТ та зв’язок** | **Нормативно-правові** | **Кадрові** | **Репутаційні** |
| невиконання функцій, процесів, операцій | знищення найбільш важливих облікових записів або відсутність до них доступу | недотримання вимог законодавства, судові позови, порушення контрактів (угод) | втрата кваліфікованих працівників (плинність кадрів, звільнення, вихід на пенсію) | негативна інформація від державних органів, правоохоронних органів |
| відсутність/ недостатність контролю за реалізацією процесу, операції | недоступні або недостовірні дані, несанкціонований виток чутливої інформації | відсутність, суперечність або нечітка регламентація положень законодавства | не здійснення заходів з навчання та підвищення кваліфікації персоналу | втрата довіри зі сторони зацікавлених сторін через операційні недоліки |
| втрата матеріально-технічного обладнання | вірусні атаки на основне програмне забезпечення | неналежна претензійна-позовна діяльність | наявність вакансії впродовж тривалого часу | негативне висвітлення діяльності установи у медіа |
|  | відсутність інтернету, телефонного зв’язку | зупинення важливої діяльності |  | незадоволення працівників (скарги, звернення, у тому числі на гарячі телефонні лінії) |

Під час ідентифікації та формулювання ризиків доцільно дотримуватися наступних рекомендацій[[1]](#footnote-1):

* + 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). Формулювання ризиків у причинно-наслідковому зв’язку достатньо чітко описує суть ризику та не потребує будь-яких пояснень. Найбільш простий спосіб встановлення причин та наслідків виникнення ризиків є проведення консультацій з особами, відповідальними за процес та пов’язані з ним ризики. Водночас, ризики, сформульовані без визначення причинно-наслідкових зв’язків, загалом непридатні для правильного визначення ризикових об’єктів аудиту, що надалі впливає на відбір об’єктів аудиту до плану та загалом на правильність визначення тематики внутрішнього аудиту.

У таблиці представлені приклади формулювання ризиків (правильне позначено – **✓**, неправильне – **Х**).

|  |  |  |
| --- | --- | --- |
| 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 | **Х** | Ризик сформульований як зворотний від цілі |
| Виток персональних даних фізичних осіб | **Х** | Відсутній причинно-наслідковий зв’язок. Виток даних фізичних осіб – це наслідок у разі матеріалізації ризику, а не сам ризик |
| Виникнення помилок у роботі бази даних | **Х** | 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 |

Визначаючи ризики або події, що можуть створювати ризики, корисним є отримати відповідь на запитання "що може відбутися неправильно?" (тобто, що може завадити досягненню цілей установи). Внутрішній аудитор повинен оцінити ризики з врахуванням низки можливостей. Водночас, будь-яка подія не є процесом, а результатом реалізації певних процесів.

Для внутрішніх аудиторів важливо спочатку встановити зв’язок між ризиками та процесами. Тому, потрібно зрозуміти ціль процесу як ключового елементу будь-якого процесу. Ціль процесу повинна визначати чого намагається досягнути процес. Неправильне трактування внутрішнім аудитором цілей процесу може призвести до невірного визначення ризиків, що надалі негативно позначиться на результатах роботи підрозділу внутрішнього аудиту загалом.

Ризики мають стосуватися, в першу чергу, досягнення цілей діяльності установи. Ризики існують на двох рівнях: 1) ризики високого рівня, які створюють загрозу досягненню цілей установи (ризики стратегічного рівня); 2) ризики діяльності, що стосуються питань результативності, економічності та ефективності (ризики оперативного рівня).

Загалом існує багато ризиків, які можуть здатися порівняно простими, проте нерідко такі ризики пов’язані з досить складним ланцюгом подій. Любий, навіть «невеликий та незначний процес», завжди пов’язаний з низкою ризиків. При наявності таких ризиків ціль таких процесів досягається частково або взагалі не досягається.

Для внутрішнього аудитора важливо встановити особу, яка найбільш зацікавлена в управлінні відповідним ризиком («власника ризика»), оскільки усунення певного ризика сприяє досягненню цілі процесу. Водночас, існує немало ризиків для яких досить складно визначити єдину відповідальну особу («власника ризика»). До таких ризиків належать ризики, які мають декілька причин виникнення. У таких ризиків є декілька «власників», оскільки різні причини виникнення ризика призводять до різних варіантів розвитку подій. У такому випадку доцільно визначати декілька окремих ризиків.

Взагалі необхідно визначити єдиного «власника ризика», оскільки коли власників декілька, вкрай складно визначити відповідальну особу, яка в більшій мірі відповідає за управління певним ризиком. Уточнення «власників ризиків» можна зробити під час проведення підрозділом внутрішнього аудиту консультацій з відповідальними за діяльність особами.

Важливо пам’ятати, що цілі відповідного процесу (на відміну від причин ризика), змінюються частіше. У зв’язку з чим, під час кожної зміни цілі процесу потрібно переглядати зв’язок ризиків та наявних процесів.

**3. Оцінка ризиків за впливом та ймовірністю**

**П**ісля ідентифікації ризиків, здійснюється **оцінка ризиків** **щодо** **впливу** (визначає фінансові та нефінансові наслідки для установи у випадку настання ризику) та **ймовірності** (передбачає можливість виникнення ризику). Ціль етапу – визначення найбільш ризикових об’єктів аудиту.

Вимоги щодо формування плану діяльності з внутрішнього аудиту на підставі результатів оцінки ризиків, яка має бути документально оформлена, та проводиться не рідше одного разу на рік передбачено абзацом третім пункту 6 Порядку № 1001 та пунктами 2, 3 Стандарту 7 «Планування діяльності з внутрішнього аудиту».

***П****лан формується підрозділом на підставі результатів оцінки ризиків… (вимоги абзацу третього пункту 6 Порядку № 1001).*

***К****ерівник підрозділу внутрішнього аудиту забезпечує формування плану на підставі результатів оцінки ризиків… (вимоги пункту 2 Стандарту 7 «Планування діяльності з внутрішнього аудиту»).*

***П****лан формується підрозділом внутрішнього аудиту на підставі документально оформленої оцінки ризиків, яка проводиться не рідше одного разу на рік (вимоги пункту 3 Стандарту 7 «Планування діяльності з внутрішнього аудиту»)*

Усі ризики, які заслуговують на увагу, мають певну силу впливу. Оцінка впливу є більш складним процесом, ніж оцінка ймовірності, однак проведення таких оцінок є важливим аспектом під час оцінюванні ризиків.

Для оцінки впливу може бути розроблено багато критеріїв, але бажано обмежитися чотирма найбільш важливими, зокрема, використовуються наступні критерії для оцінки впливу:

* фінансовий вплив (фінансові наслідки для установи у випадку виникнення ризику);
* кадровий вплив (неочікувана втрата ключових спеціалістів може істотно вплинути на виконання установою завдань та функцій, досягнення нею цілей);
* операційний вплив (ступінь впливу ризику на реалізацію установою завдань та функцій, досягнення нею цілей);
* репутаційний вплив (вплив на репутацію установи, керівника цієї установи з точки зору міжнародних рейтингів, донорів тощо).

Щодо кожного критерію впливу визначається рівень (низький, середній, високий та дуже високий), що дозволяє визначати бали ризикам уніфікованим способом. Рівень ризику визначається за допомогою присвоєння ризикам відповідних балів.

На прикладі представлено визначення балів для чотирьох критеріїв впливу:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Приклади визначення рівнів (балів) для 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 напрямами 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 критичних збоїв у роботі цього підрозділу | Критичне зниження/втрата спроможностей може заважати продовженню виконання завдань та функцій за двома і більше напрямами 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 напрямами 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 |

За допомогою оцінки ймовірності визначаються можливості, що подія, яка створює ризик, відбудеться протягом певного часу. Критерії ймовірності часто схожі між собою (приклади критеріїв ймовірності наводяться у таблиці):

|  |  |
| --- | --- |
| Приклади визначення рівнів (балів) для критеріїв ймовірності | |
| Рівень (бал) | **Критерії ймовірності** |
| Рідко/майже не можливо (1) | Ймовірність виникнення ризику дуже низька (з вірогідністю 0-24 %) |
| Малоймовірно (2) | Ймовірність виникнення ризику віддалена (з вірогідністю 25-50 %) |
| Можливо (3) | Ймовірність виникнення ризику впродовж 1-2 років (з вірогідністю 51-74 %) |
| Часто/очікується (4) | Ризик існує або очікується (з вірогідністю 75-100 %) |

Після визначення відповідних критеріїв для оцінки впливу та оцінки ймовірності, їх застосовують для усіх ідентифікованих ризиків (включаючи ризики, що самостійно виявлені підрозділом внутрішнього аудиту, яких не було ідентифіковано відповідальними за діяльність особами, та залишкові ризики, які залишаються високими, незважаючи на запроваджені заходи контролю відповідальними за діяльність особами).

Оцінку впливу та оцінку ймовірності (присвоєння балів) можна здійснювати різними методами, зокрема, шляхом:

* визначення середніх показників на підставі індивідуальних письмових оцінок проведених різними внутрішніми аудиторами;
* колегіальної оцінки ризиків на підставі думки кожного внутрішнього аудитора, загального обговорення та узгодження щодо присвоєним ризикам балів. Наприклад, колективну оцінку ризиків можна проводити під час проведення робочих зустрічей, нарад у підрозділі внутрішнього аудиту.

Незалежно від застосованого методу оцінки ризиків, рівень сприйняття ризику працівниками є різним – деякі працівники схильні уникати ризиків, в той час як інші – готові йти на ризик. Якщо одним працівником оцінено ризик як «високий», а іншим – як «низький», то результат не повинен визначатися як середньоарифметичне значення рівня (балу) ризику, слід шляхом переговорів дійти консенсусу.

Як правило, підрозділ внутрішнього аудиту повинен, в першу чергу, цікавитися ризиками із значенням «високий» або «дуже високий», проте досить часто до цієї групи ризиків потрапляють:

* «глобальні» ризики, які обумовлені великою кількістю причин та наслідків, (наприклад, ризик «створення неадекватної структури внутрішнього контролю, що призведене до неналежного функціонування внутрішнього контролю в установі»);
* «зовнішні» ризики, які виникають поза установою, але впливають на її діяльність (наприклад, ризик «погіршення економічної ситуації в країні призведе до несприятливих для діяльності установи наслідків», «реформи органів державної влади…», «зміна пріоритетів діяльності Уряду…», «законодавчі зміни…»);
* ризики форс-мажорних обставин.

Наявність у групі ризиків з «високою»/«дуже високою» оцінкою значної кількості «глобальних» та «зовнішніх» ризиків, ризиків форс-мажорних обставин може свідчити про неправильне визначення причинно-наслідкових зв’язків. Найкращою практикою роботи з «глобальними» ризиками є їх розділення на більш «дрібні» ризики (а саме, сформулювати перелік взаємопов’язаних ризиків, суть яких відповідає суті початкового варіанту ризику). Стосовно «зовнішніх» ризиків та ризиків форс-мажорних обставин, то початковий вплив та ймовірність виникнення таких ризиків залишається незмінними незалежно від розроблених заходів контролю щодо зменшення впливу ризиків.

Загальна оцінка ризику (загальний бал) визначається шляхом множення оцінки впливу та оцінки ймовірності, як це наведено у таблиці «Матриця оцінки ризиків»:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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) |

У таблиці «Матриця оцінки ризиків» ризики з рівнем від 1 до 3 вважаються «низькими» (і на цьому рівні ризик вважається прийнятним, позначено синім кольором), з рівнем від 4 до 6 – «середні» ризики (жовтий колір), з рівнем від 8 до 16 – «високі»/«дуже високі» ризики (червоний/рожевий колір).

Водночас, не доцільно визначати бали лише математичним способом – слід оцінювати ризики та визначати бали відповідно до визначених критеріїв для оцінки впливу та оцінки ймовірності. Частіше використовується трирівнева система присвоєння балів, але такий підхід може призвести до переоцінки ризиків за шкалою «середніх» значень. На прикладі «Матриці оцінки ризиків» використовується 4-бальна шкала оцінки.

Ідентифікацію та оцінку ризиків доцільно проводити у взаємопов’язаний спосіб, оскільки, можливо, необхідно буде внести зміни до раніше сформульованих ризиків. Крім того, під час оцінки ризиків може виникнути потреба в уточненні (внесення змін до простору аудиту, зокрема, в частині розподілу об’єктів аудиту за категоріями). Саме тому, бажано, під час проведення оцінки ризиків одночасно розділяти простір аудиту за відповідними категоріями або проводити «мозкові штурми» можливих подій, які допомагають визначити категорії у просторі аудиту.

Після визначення загальної оцінки ризику (визначення загального балу) відповідно до «Матриці оцінки ризиків» здійснюється документування процедури ідентифікації та оцінки ризиків, загальної оцінки ризиків за впливом/ймовірністю.

Під час проведення та документування процедури ідентифікації та оцінки ризиків, узагальнення результатів оцінки ризиків працівниками підрозділу внутрішнього аудиту застосовується власне судження про ризики та управління ними, яке формується на підставі аналізу документів (інформації) з питань управління ризиками, опрацювання інших документів (інформації), які стосуються діяльності установи, а також з урахуванням проведених працівниками підрозділу внутрішнього аудиту консультацій з вищим керівництвом установи та відповідальними за діяльність особами щодо проблемних питань та ризиків у діяльності установи.

Документування процедури ідентифікації та оцінки ризиків здійснюється за визначеними у внутрішніх документах з питань здійснення внутрішнього аудиту в частині планування шаблонами та формами, що містять інформацію щодо:

* назви ризиків, сформульованих у причинно-наслідковому зв’язку (включаючи ризики, що самостійно виявлені підрозділом внутрішнього аудиту, яких не було ідентифіковано відповідальними за діяльність особами, та залишкові ризики, які залишаються високими, незважаючи на запроваджені відповідальними за діяльність особами заходи контролю);
* результатів оцінки впливу;
* результатів оцінки ймовірності;
* результатів загальної оцінки ризиків (за впливом та ймовірністю).

Зразки шаблонів (форм) щодо ідентифікації та оцінки ризиків, алгоритм їх наповнення відповідною інформація наведено у [***додатку 2***](#_Додаток_2._Приклад).

Проведення оцінки ризиків рекомендовано організовувати та завершувати не пізніше 30 листопада перед складанням плану діяльності з внутрішнього аудиту.

Під час проведення підрозділом внутрішнього аудиту ідентифікації та оцінки ризиків слід розуміти різницю між поняттями «управління ризиками у діяльності установи» та «оцінкою ризиків з метою планування діяльності з внутрішнього аудиту».

**Управління ризиками у діяльності установи** – елемент системи внутрішнього контролю. Діяльність з управління ризиками належить до повноважень (відповідальності) вищого керівництва та керівників структурних підрозділів установи. Сутність діяльності з управління ризиками визначено в Основних засадах внутрішнього контролю та Методичних рекомендаціях з внутрішнього контролю.

**Оцінка ризиків з метою планування діяльності з внутрішнього аудиту** – етап планування діяльності з внутрішнього аудиту, метою якого є визначення найбільш важливих (ризикових) об’єктів аудиту. Результати оцінки ризиків слугують базою для формування плану діяльності з внутрішнього аудиту.

Водночас підходи до ідентифікації та оцінки ризиків є однаковими як для вищого керівництва та керівників структурних підрозділів установи, так і для працівників підрозділу внутрішнього аудиту.

***Д****іяльність підрозділу внутрішнього аудиту має здійснюватись із застосуванням систематичного, послідовного та ризик-орієнтованого підходів до оцінки об’єкта внутрішнього аудиту та сприяти удосконаленню системи управління, внутрішнього контролю та управління ризиками через надання незалежних й об’єктивних висновків та рекомендацій.*

***П****ід час проведення внутрішнього аудиту здійснюються дослідження та оцінка системи управління та внутрішнього контролю, у тому числі управління ризиками (з питань та в обсязі, що відповідають об’єкту, темі та цілям внутрішнього аудиту).*

***О****цінка та надання відповідних рекомендацій щодо системи управління мають враховувати питання ефективності управління діяльністю, ступеня виконання і досягнення визначених цілей, якості виконання відповідних завдань та функцій, що стосуються об’єкта внутрішнього аудиту.*

Основна відмінність між процесом управління ризиками у діяльності установи та процесом оцінки ризиків для планування діяльності з внутрішнього аудиту полягає у тому, що вищому керівництву та керівникам структурних підрозділів установи необхідно оцінити невід’ємні ризики з метою розробки та впровадження заходів контролю для впливу на ризики.

Під час процесу оцінки ризиків для планування діяльності з внутрішнього аудиту оцінюється повнота визначення відповідальними за діяльність особами невід’ємних ризиків, доцільність та дієвість обраних ними способів реагування на ризики, ефективність розроблених відповідальними за діяльність особами заходів контролю для впливу на ризики тощо.

Під час здійснення внутрішніх аудитів здійснюється оцінка процесів управління, функціонування систем внутрішнього контролю та управління ризиками тощо, а також надаються рекомендації щодо їх вдосконалення. Аудиторські рекомендації, основані на об’єктивній думці внутрішнього аудитора, дають можливість керівнику установи приймати обґрунтовані та дієві управлінські рішення.

***О****цінка та надання відповідних рекомендацій щодо процесів управління ризиками мають враховувати питання ідентифікації ризиків та проведення їх оцінки, вжиття заходів реагування на ідентифіковані та оцінені ризики, здійснення їх перегляду, а також своєчасності доведення результатів оцінки ризиків до керівника та заінтересованих підрозділів установи.*

***О****цінка та надання відповідних рекомендацій щодо системи внутрішнього контролю мають враховувати питання досягнення визначених мети (місії), стратегічних та інших цілей, ефективності управління бюджетними коштами, використання і збереження активів, ефективності та надійності інформаційних систем і технологій, достовірності і повноти фінансової та операційної інформації, дотримання законодавства та внутрішніх вимог щодо діяльності, яка є об’єктом внутрішнього аудиту (вимоги пунктів 1, 2 Стандарту 5 «Сутність діяльності з внутрішнього аудиту»)*

Вимоги щодо здійснення підрозділом внутрішнього аудиту дослідження та оцінки системи управління та внутрішнього контролю, у тому числі управління ризиків передбачено Стандартом 5 «Сутність діяльності з внутрішнього аудиту».

Водночас, під час здійснення внутрішніх аудитів з оцінки процесів управління, функціонування систем внутрішнього контролю та управління ризиками внутрішні аудити не повинні брати безпосередню участь в організації внутрішнього контролю, управлінні ризиками і прийнятті управлінських рішень, створенні та організації процесів, що забезпечують операційну діяльність установи (вимоги пункту 3 Стандарту 5 «Сутність діяльності з внутрішнього аудиту»).

***К****ерівник та працівники підрозділу внутрішнього аудиту не повинні брати безпосередню участь в організації внутрішнього контролю, управлінні ризиками і прийнятті управлінських рішень, створенні та організації (у тому числі разом з іншими структурними підрозділами установи) будь-яких заходів та процесів, що забезпечують операційну діяльність установи (вимоги пункту 3 Стандарту 5 «Сутність діяльності з внутрішнього аудиту»)*

Загалом здійснення підрозділом внутрішнього аудиту оцінки системи управління ризиками (як елемента внутрішнього контролю) сприятиме більш ефективному управлінню ризиками у діяльності установи.

Зокрема, може підштовхнути керівництво установи до запровадження у діяльності установи власного процесу ідентифікації та оцінки ризиків. У такому випадку підрозділ внутрішнього аудиту може надавати допомогу вищому керівництву та структурним підрозділам установи у забезпеченні здійснення управління ризиками у діяльності установи, зокрема, шляхом:

* здійснення консультаційної діяльності, що полягає у наданні порад і рекомендацій щодо підвищення ефективності та результативності діючих процесів, допомоги під час розгляду нових правил та процедур, які впроваджуватимуться в установі, сприяння заходам з реагування на зовнішні виклики та загрози, ключовим заходам з управління ризиками, дорадчій участі у робочих групах/комісіях, колективного обговорення проблем тощо;
* проведення робочих зустрічей та семінарів з вищим керівництвом та керівниками і працівниками структурних підрозділів установи з питань управління ризиками, на яких розглянути питання щодо ідентифікації та оцінки ризиків, визначення підходів щодо документування цієї процедури.

Під час надання такої допомоги внутрішнім аудиторам необхідно вживати заходи для обмеження негативного впливу на незалежність та об’єктивність діяльності з внутрішнього аудиту, а також врахувати кваліфікаційну спроможність підрозділу внутрішнього аудиту та можливий вплив на безпосереднє здійснення внутрішніх аудитів.

Зокрема, залучення керівника та/або працівників підрозділу внутрішнього аудиту до діяльності різних комісій, робочих груп тощо (за рішенням керівника установи) можливе виключно в якості незалежного експерта, який виконує функцію консультування (дорадчу функцію) та не бере участь у прийнятті управлінських рішень. При цьому, у внутрішньому документі установи про відповідну комісію, робочу групу має бути визначено, що внутрішній аудитор приймає участь в її роботі в якості експерта/консультанта з правом дорадчого голосу (без права голосу щодо прийняття рішень).

У разі неможливості залучення працівників підрозділу внутрішнього аудиту до діяльності комісій, робочих груп виключно в якості експертів чи консультантів слід ініціювати внесення змін до нормативно-правових актів та/або внутрішніх документів установи, якими регламентовано діяльність таких комісій, робочих груп, з метою виключення внутрішніх аудиторів з переліку осіб, які мають входити до їх складу.

Здійснення консультаційної діяльності підрозділом внутрішнього аудиту рекомендовано документально оформлювати (зокрема, відповідно до положень, визначених внутрішніми документами з питань внутрішнього аудиту). Під час документування результатів консультацій доцільно зазначати працівників підрозділу внутрішнього аудиту, які залучались до консультації (посада, прізвище, ім’я тощо), кількість робочих днів, витрачених на консультацію (у розрізі внутрішніх аудиторів) тощо.

Консультаційна діяльність підрозділу внутрішнього аудиту включається до плану діяльності з внутрішнього аудиту в частині здійснення іншої діяльності з внутрішнього аудиту.

**4. Визначення об’єктів аудиту за допомогою факторів відбору**

**П**ісля оцінювання ризиків за впливом та ймовірністю **визначається пріоритетність об’єктів аудиту за допомогою набору факторів відбору, а також частота дослідження кожного об’єкта аудиту, включеного до бази даних щодо простору аудиту**. Ціль етапу – відбір пріоритетних об’єктів аудиту щодо яких будуть здійснюватися внутрішні аудити протягом наступних трьох планових періодах.

Вимоги щодо визначення факторів відбору для здійснення планових внутрішніх аудитів та частоти їх здійснення щодо кожного об’єкта аудиту у внутрішніх документах з питань здійснення внутрішнього аудиту в частині планування передбачено абзацом другим пункту 4 Стандарту 1 «Завдання, права та обов’язки».

***В****нутрішні документи з питань здійснення внутрішнього аудиту мають врегульовувати такі питання:*

*планування діяльності з внутрішнього аудиту, в тому числі 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… (вимоги абзацу другого пункту 4 Стандарту 1 «Завдання, права та обов’язки»)*

За результатами оцінки ризиків у базі даних щодо простору аудиту визначається велика кількість об’єктів аудиту та ризиків, пов’язаних з такими об’єктами аудиту. Зокрема, виявляється, що одна з груп об’єктів аудиту (наприклад, з «середньою» оцінкою) є найбільшою за обсягом, хоча містить дуже різноманітні об’єкти аудиту. Водночас, наявність ризиків, навіть з «високою» та «дуже високою» оцінкою, не може бути єдиним фактором відбору об’єктів аудиту для включення до плану.

Для аналізу важливості кожного об’єкта аудиту додатково використовується набір «факторів відбору», який допомагає підрозділу внутрішнього аудиту визначити пріоритетність (першочерговість) дослідження відповідного об’єкту аудиту. Термін «фактори відбору» точно відображає сутність цього етапу – відбір тих об’єктів аудиту, дослідження яких є найбільш доцільним.

До найбільш використовуваних факторів відбору належать:

* **фінансова важливість/матеріальність** (ґрунтується на обсягах державних ресурсів, доходах та прибутках, наданих послугах тощо. Підприємства, установи та організації з високим рівнем ризику, що використовують незначну частину бюджету, будуть менш пріоритетними для внутрішнього аудиту, ніж підприємства, установи та організації з середнім рівнем ризику, які використовують 50 % бюджету);
* **складність діяльності** (складні напрями (сфери) діяльності установи визначаються складністю правової бази, кількістю залученого персоналу, географічним розташуванням. Складні напрями діяльності важче реалізувати належним чином, тому ймовірність того, що вони будуть виконані неякісно та/або несвоєчасно є вищою. Наприклад, вартість будівельних проектів нерідко є вищою від запланованої, а тривалість проектів більшою, ніж очікувалось);
* **загальна політика внутрішнього контролю** (застосовується у розумінні Основних засад внутрішнього контролю). У разі наявності належної системи внутрішнього контролю в установі, в якій визначено чіткі цілі діяльності, функції та обов’язки працівників, етичні норми поведінки; забезпечується управлінська відповідальність та підзвітність керівника та працівників установи, яка ґрунтується на вимогах законодавства та стосується всієї діяльності установи; налагоджена ефективна система управління (зокрема, управлінські рішення приймаються відповідно до цілей діяльності державного органу та своєчасно доводяться до виконавців, забезпечується контроль та звітування за виконанням управлінських рішень на усіх етапах їх виконання, здійснюється оцінка досягнутих результатів та за необхідності своєчасне коригування планів діяльності установи); забезпечено здійснення управління ризиками та визначено підходи щодо документування управління ризиками; запроваджено ефективну політику та практику управління персоналом, відсутні часті зміни персоналу; забезпечено належну професійну підготовку персоналу та виконання ними посадових обов’язків; відсутні повідомлення про помилки, порушення та недоліки, а також скарги від різних зацікавлених сторін. У випадку слабкої системи внутрішнього контролю ймовірність виникнення помилок, шахрайства, корупції є набагато більшою;
* **репутаційна чутливість** (деякі сфери діяльності установи є об’єктом прискіпливої уваги з боку медіа, громадян, Уряду тощо, тому виникнення проблем у таких сферах, може створювати високі ризики для репутації установи загалом);
* **масштаб змін** (до будь-яких змін потрібно звикнути, однак такі події підвищують ймовірність допущення помилок. Наприклад, законодавчі зміни, кадрові зміни, зміни у функціях/процесах);
* **надійність керівництва** (досвідчені керівники, як правило, вирішують проблеми більш ефективно та досягають кращих результатів, а також знають та розуміють проблеми/ризики у діяльності установи та своєчасно приймають відповідні рішення щодо розв’язання проблем/зменшення ризиків, натомість часті зміни керівництва, тимчасові керівники або керівники з незначним досвідом, недостатньою кваліфікацією викликають більшу невпевненість);
* **можливість для зловживань** (кожна функція/процес має тимчасовий та/або набутий потенціал для корупційних схем. Водночас, деякі сфери діяльності більш вразливі для шахрайства та корупції, наприклад, високий рівень готівкових розрахунків або делеговані повноваження з накладання та збору штрафів);
* **питання, які цікавлять керівництво** (окремі функції/процеси викликають або можуть викликати занепокоєння керівництва установи; невідповідність висновків, наданих зовнішніми контролюючими органами, рівню впевненості керівництва; керівники структурних підрозділів установи, як правило, краще обізнані щодо напрямів (сфер) діяльності із найбільшим та найменшим рівнем ризику, тому їх думку слід враховувати та використовувати як фактор відбору);
* **час від попереднього аудиту** (у кожному внутрішньому аудиті присутній дисциплінуючий фактор, навіть, об’єкти аудиту з низьким ризиком час від часу повинні охоплюватися аудитом. Об’єкти аудиту, які не підлягали аудиту вже протягом кількох років, можуть мати високий рівень ризику);
* **стан впровадження аудиторських рекомендацій**, наданих за результатами проведення попередніх внутрішніх аудитів (низький рівень усунення проблем/недоліків у системі внутрішнього контролю можуть свідчити про підвищення ризиковості відповідних об’єктів аудиту).

У таблиці поетапно представлено процедуру здійснення ризик-орієнтованого відбору об’єктів аудиту з метою визначення пріоритетних об’єктів аудиту та частоти здійснення планових внутрішніх аудитів щодо кожного об’єкта аудиту:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Етап 1. Визначення балів для оцінки факторів відбору**  *Після визначення факторів відбору здійснюється їх оцінка через призму визначених критеріїв. Зокрема, щодо кожного фактору відбору розробляється набір критеріїв, які використовуються для визначення балів. Оцінка фактору відбору повинна базуватися на визначених та зрозумілих критеріях – чому саме такий, а не інший бал присвоєно цьому фактору.*  *Приклади критеріїв щодо оцінки кожного фактору відбору наведено у таблиці.*  *Оцінка кожного фактору відбору* ***(а-j)*** *відбувається шляхом присвоєння балів* ***(Р)*** *від 1 до 4 (низький – 1, середній – 2, високий – 3, дуже високий – 4).* | | | | | | |
| **Фактор відбору**  **(а-j)** | **Критерії** | | | | **Бал**  **(Р)** |
| а. Фінансова важливість/ матеріальність | На об’єкт аудиту (програму, систему, ресурси тощо) припадає | менше 10 % річного бюджету | | | 1 |
| 11 – 50 % річного бюджету | | | 2 |
| 51 – 80 % річного бюджету | | | 3 |
| не менше 81 % річного бюджету | | | 4 |
| b. Складність діяльності | Виконання функції (процесу) суттєво не впливає на досягнення мети та цілей діяльності установи; реалізація функції (процесу) передбачає невелику кількість процедур та задіяного персоналу | | | | 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 |
| Виконання функції (процесу) впливає на досягнення мети та цілей діяльності установи; реалізація функції (процесу) передбачає велику кількість процедур та задіяного персоналу | | | | 3 |
| Виконання функції (процесу) відіграє ключову роль у досягненні мети та цілей діяльності установи; реалізація функції (процесу) передбачає найбільшу кількість процедур та задіяного персоналу | | | | 4 |
| c. Загальна політика внутрішнього контролю | Надійні системи внутрішнього контролю та управління ризиками | | | | 1 |
| Системи внутрішнього контролю та управління ризиками в цілому налагодженні та працюють, але мають окремі недоліки | | | | 2 |
| Системи внутрішнього контролю та управління ризиками є слабкими та ненадійними (перебуває на стадії становлення) | | | | 3 |
| Система внутрішнього контролю неефективна, має суттєві проблеми (розроблена формально та належно не функціонує, управління ризиками в установі не запроваджене) | | | | 4 |
| d. Репутаційна чутливість | Мінімальний зовнішній інтерес до функції (процесу) або його цілковита відсутність | | | | 1 |
| Можливість виникнення непорозумінь з громадськістю, пов’язаних з виконанням функції (процесу) | | | | 2 |
| Виникали поодинокі випадки непорозумінь з громадськістю, пов’язаних з виконанням функції (процесу) | | | | 3 |
| Підвищена увага з боку медіа до реалізації відповідної функції (процесу). Виникнення серйозних/системних проблем та/або втрата репутації установи за наявності таких проблем | | | | 4 |
| e. Масштаб змін | У законодавчих та нормативно-правових актах, які регулюють виконання відповідної функції (процесу), кадрових змінах, змінах у процедурах в рамках реалізації функції (процесу) тощо | за останній рік відбулося менше 10 % змін | | | 1 |
| за останній рік відбулося від 10 до 30 % змін | | | 2 |
| за останній рік відбулося від 30 до 50 % змін | | | 3 |
| за останній рік відбулося більше 50 % змін | | | 4 |
| f. Надійність керівництва | Вище керівництво установи та особи, відповідальні за реалізацію відповідної функції (процесу), мають досвід більше 3 років та практику успішної реалізації проектів/програм з відповідного напряму діяльності у державному секторі | | | | 1 |
| Вище керівництво установи та особи, відповідальні за реалізацію відповідної функції (процесу), мають досвід від 2 до 3 років та практику реалізації проектів/програм з відповідного напряму діяльності у державному секторі | | | | 2 |
| Вище керівництво установи та особи, відповідальні за реалізацію відповідної функції (процесу), мають досвід від 1 до 2 років з відповідного напряму діяльності у державному секторі | | | | 3 |
| Вище керівництво установи та особи, відповідальні за реалізацію відповідної функції (процесу), мають досвід менше 1 року з відповідного напряму діяльності у державному секторі | | | | 4 |
| g. Можливість для зловживань | Мінімальна можливість для виникнення фактів шахрайства та корупції | | | | 1 |
| Можливість виникнення зловживань, однак фактів шахрайства та корупції ще не виникало | | | | 2 |
| Існують поодинокі факти шахрайства та корупції | | | | 3 |
| Існують системні факти шахрайства та корупції | | | | 4 |
| h. Питання, які цікавлять керівництво | Невисока увага з боку вищого керівництва установи, існують поодинокі проблеми, які вийшли на рівень вищого керівництва у минулому | | | | 1 |
| Вище керівництво установи приділяє помірну увагу, наявність проблем, які вийшли на рівень вищого керівництва у минулому | | | | 2 |
| Висока увага з боку вищого керівництва установи, суттєві або повторювані проблеми, які вийшли на рівень вищого керівництва у минулому | | | | 3 |
| Постійна увага з боку вищого керівництва установи, існують суттєві повторювані проблеми, які вийшли на рівень вищого керівництва у недалекому минулому | | | | 4 |
| i. Час від попереднього аудиту\* | Проведено менше 1 року тому | | | | 1 |
| Проведено більше 1 року, але менше 5 років тому | | | | 2 |
| Проведено більше 5 років, але менше 7 років тому | | | | 3 |
| За останні 7 та більше років внутрішній аудит не проводився | | | | 4 |
| **\****наведені у критеріях оцінки фактору відбору «Час від попереднього аудиту» приклади періодів проведення внутрішніх аудитів можуть змінюватися в залежності від визначених частоти здійснення внутрішніх аудитів щодо кожного об’єкта аудиту та загального періоду внутрішнього аудиту (приклад наведено з додатку 2)* | | | | | | |
| j. Стан впровадження аудиторських рекомендацій | Повністю виконано аудиторські рекомендації або внутрішній аудит не здійснювався | | | | 1 |
| Більшість аудиторських рекомендацій виконано, інформація про стан їх впровадження надається систематично/своєчасно та свідчить про прогрес у діяльності | | | | 2 |
| Частково виконано аудиторські рекомендації, інформація про стан їх впровадження надається несистематично/несвоєчасно та не свідчить про прогрес у діяльності | | | | 3 |
| Не виконано аудиторські рекомендації | | | | 4 |
| **Етап 2. Визначення показників вагомості для оцінки факторів відбору**  *Показники вагомості використовуються для ілюстрації відмінностей різних факторів відбору, оскільки не всі фактори відбору будуть однаково важливі. За допомогою певних процесів зважування, визначаються фактори, які будуть вважатися найважливішими, та отримують вищі значення.*  *На підставі оціночного судження щодо важливості відповідного фактору відбору, кожному з них присвоюється показник вагомості. Такі показники визначаються підрозділом внутрішнього аудиту з урахуванням особливостей діяльності державного органу. Зокрема, показники вагомості можуть визначатися, у тому числі за результатами консультацій з відповідальними за діяльність особами.*  *Показникам вагомості* ***(Wa-Wj)*** *надається значення від 1 до 5 (мінімальне значення – 1, максимальне значення – 5).*  *Приклад застосування різних показників вагомості наведено у таблиці. Зокрема, такі фактори відбору як питання, які цікавлять керівництво, та можливість для зловживань отримали найбільші значення (відповідно 5 та 4), а фактор відбору – стан впровадження аудиторських рекомендацій отримав найменше значення (1).* | | | | | | |
| **Фактор відбору (а-j)** | | | **Показник вагомості (Wa-Wj)** | **Приклад застосування різних значень для показників вагомості (наведено з** [***додатку 2***](#_Додаток_2._Приклад)**)** | | |
| а. Фінансова важливість/матеріальність | | | Wa | 3 | | |
| b. Складність діяльності | | | Wb | 3 | | |
| c. Загальна політика внутрішнього контролю | | | Wc | 2 | | |
| d. Репутаційна чутливість | | | Wd | 2 | | |
| e. Масштаб змін | | | We | 2 | | |
| f. Надійність керівництва | | | Wf | 2 | | |
| g. Можливість для зловживань | | | Wg | 4 | | |
| h. Питання, які цікавлять керівництво | | | Wh | 5 | | |
| i. Час від попереднього аудиту | | | Wi | 2 | | |
| j. Стан впровадження аудиторських рекомендацій | | | Wj | 1 | | |
| **Етап 3. Розрахунок індексу пріоритетності та визначення ступеня пріоритету**  *За допомогою формули розраховується індекс пріоритетності* ***(Ip)*** *за кожним об’єктом аудиту шляхом множення загальної оцінки ризику (за впливом та ймовірністю)* ***(Rа)*** *та оцінки кожного фактору відбору (а-j) за допомогою бальних оцінок* ***(Рa-Pj)*** *та вагових коефіцієнтів* ***(Wa-Wj)****:*  ***Ip = Rа x*** *(),*  *де* ***Ip*** *– індекс пріоритетності;*  ***Rа*** *– загальна оцінка ризику (за ймовірністю та впливом), присвоєна за кожним об’єктом аудиту;*  ***Рa-Pj*** *– бал, присвоєний за відповідним фактором відбору;*  ***Wa-Wj*** *– показник вагомості фактору відбору;*  ***n*** *– загальна кількість застосованих факторів відбору.*  *Визначений індекс пріоритетності використовується для визначення об'єктів аудиту з різним ступенем пріоритету (від «дужого високого» / «високого» до «низького»).*  *На прикладі застосовується чотирибальна шкала пріоритетів:* | | | | | | |
| **Ступінь пріоритету** | | | **Приклад значень індексу пріоритетності (Ip) (наведено з** [***додатку 2***](#_Додаток_2._Приклад)**)** | | | |
| дуже високий | | | від 100 та більше | | | |
| високий | | | від 61 до 99 | | | |
| середній | | | від 41 до 60 | | | |
| низький | | | до 40 | | | |
| *У групу з «дуже високим» ступенем пріоритету включаються об’єкти аудиту з індексом пріоритетності від 100 та більше, групу з «високим» ступенем пріоритету – з індексом пріоритетності від 61 до 99, групу з «середнім» ступенем пріоритету – з індексом пріоритетності від 41 до 60, групу з «низьким» ступенем пріоритету – з індексом пріоритетності до 40.*  **Етап 4. Визначення загального періоду внутрішнього аудиту**  *Загальний період внутрішнього аудиту – це кількість років, протягом яких внутрішніми аудитами може бути охоплено весь простір аудиту (тобто забезпечено проведення внутрішніх аудитів щодо усіх об’єктів аудиту, включених до бази даних щодо простору аудиту).*  *Загальний період внутрішнього аудиту залежить від величини простору аудиту, результатів ризик-орієнтованого відбору об’єктів аудиту та спроможності підрозділу внутрішнього аудиту – кількісної (кількість внутрішніх аудитів, що можуть бути здійснені протягом трирічного планового періоду), якісної (різна фахова спеціалізація внутрішніх аудиторів, їх різний рівень досвіду, знань та навичок) та наявних у підрозділі внутрішнього аудиту ресурсів (людських, часових, фінансових, технічних тощо).*  *Для визначення загального періоду внутрішнього аудиту слід загальну кількість людино-днів, необхідних для охоплення внутрішніми аудитами усього простору аудиту, поділити на загальну річну кількість людино-днів, необхідних для здійснення внутрішніх аудитів.*  *Загальна кількість людино-днів, необхідних для охоплення внутрішніми аудитами усього простору аудиту, обчислюється на підставі даних щодо кількості об’єктів аудиту, включених до бази даних, та визначеної в середньому кількості людино-днів, необхідної на дослідження кожного об’єкта аудиту, включеного до бази даних щодо простору аудиту. При цьому, під час визначення середньої кількості людино-днів на дослідження кожного об’єкта аудиту, слід враховувати кількість людино-днів, необхідних на здійснення внутрішніх аудитів з оцінки ефективності та здійснення внутрішніх аудитів з оцінки відповідності. Наприклад, на здійснення внутрішніх аудитів з оцінки ефективності необхідно виділити більший обсяг робочого часу (зокрема, використати більше робочих днів на їх проведення та/або залучити більше внутрішніх аудиторів до проведення таких аудитів), ніж на здійснення внутрішніх аудит з оцінки відповідності. Такі розрахунки доцільно здійснювати з урахуванням досвіду проведення подібних внутрішніх аудитів у попередніх роках.*  *Загальна річна кількість людино-днів, необхідних для здійснення внутрішніх аудитів, обчислюється на підставі загального планового обсягу робочого часу (людино-дні), фактичної чисельності працівників підрозділу внутрішнього аудиту (на момент здійснення відповідних розрахунків) та визначених у внутрішніх документах установи з питань здійснення внутрішнього аудиту коефіцієнтів участі у здійсненні внутрішніх аудитів для відповідної категорії посад працівників підрозділу внутрішнього аудиту. Відповідні розрахунки щорічно наводяться у розділі ІХ плану діяльності з внутрішнього аудиту (плану із змінами). До планового обсягу робочого часу на здійснення внутрішніх аудитів включається час на організацію внутрішнього аудиту, планування та виконання аудиторського завдання, документування перебігу та результатів внутрішнього аудиту.*  *Визначення (уточнення) загального періоду внутрішнього аудиту доцільно проводити одночасно з проведенням (актуалізацією) оцінки ризиків та здійсненням ризик-орієнтованого відбору об’єктів аудиту.*  **Етап 5. Визначення частоти здійснення планових внутрішніх аудитів**  *Частота здійснення планових внутрішніх аудитів щодо кожного об’єкта аудиту розраховується з урахуванням попередньо визначеного ступеню пріоритету об’єктів аудиту та індексу пріоритетності, а також визначеного загального періоду внутрішнього аудиту.*  *Наприклад, при встановленому в установі загальному періоді внутрішнього аудиту – сім років, визначаємо частоту здійснення планових внутрішніх аудитів щодо кожного об’єкта аудиту (або групи об’єктів аудиту з відповідним ступенем пріоритету):* | | | | | | |
| **Ступінь пріоритету** | **Приклад визначення частоти здійснення планових внутрішніх аудитів щодо кожного об’єкту аудиту**  **(наведено з** [***додатку 2***](#_Додаток_2._Приклад)**)** | **Приклад значень індексу пріоритетності (Ip) (наведено з** [***додатку 2***](#_Додаток_2._Приклад)**)** | | | |
| дуже високий | 4 рази на 7 років | від 100 та більше | | | |
| високий | 3 рази на 7 років | від 61 до 99 | | | |
| середній | 2 рази на 7 років | від 41 до 60 | | | |
| низький | 1 раз на 7 років | до 40 | | | |
| *Віднесені об’єкти аудиту до групи з «високим» та «дуже високим» ступенем пріоритету є найбільш ризиковими та мають досліджуватися часто (3-4 рази на 7 років), до групи з «середнім» ступенем пріоритету досліджуються рідше, ніж об’єкти з високим ступенем пріоритету (2 рази на 7 років), до групи з «низьким» ступенем пріоритету – рідше, ніж об’єкти з середнім ступенем пріоритету (1 раз на 7 років).*  *Водночас, якщо за результатами розрахунків виявляється, що за наявними спроможностями підрозділу внутрішнього аудиту, об’єкти аудиту, включені до бази даних щодо простору аудиту можливо охопити за 10 та більше років, то для ефективного використання ресурсів, підрозділу внутрішнього аудиту необхідно, в першу чергу, концентруватися на об’єктах аудиту з «високим» та «дуже високим» ступенем пріоритету. Однак, об’єкти аудиту з «низьким» ступенем пріоритету з часом можуть викликати високі ризики (особливо, коли тривалий період щодо таких об’єктів аудиту не здійснюються внутрішні аудити та/або не проводяться контрольні заходи зовнішніми контролюючими органами (Рахунковою палатою, органами державного фінансового контролю тощо)). Отже, проводити внутрішні аудити щодо об’єктів аудиту лише з «високим» та «дуже високим» ступенем пріоритету не рекомендується. Одночасно, слід не забувати враховувати об’єкти аудити з «середнім» ступенем пріоритету, зважаючи на їх можливу переважну більшість після проведення відповідних оцінок.*  *Тому, до планів доцільно включати об’єкти аудиту з різних груп (з оцінкою від «дуже високої» до «низької»), що забезпечує регулярне охоплення дослідженнями об’єктів аудиту з різних груп та зменшує вірогідність виникнення ризику щодо тривалого не охоплення відповідних об’єктів аудиту.*  *Включені до плану об’єкти аудиту є пріоритетними для дослідження підрозділом внутрішнього аудиту протягом наступного трирічного планового періоду.* | | | | | | |

Документування процедури ризик-орієнтованого відбору об’єктів аудиту здійснюється за визначеними у внутрішніх документах з питань здійснення внутрішнього аудиту в частині планування шаблонами (формами), що містить інформацію щодо:

* результатів оцінки кожного фактору відбору за визначеними бальними оцінками та ваговими коефіцієнтами;
* індексу пріоритетності;
* ступеня пріоритету об’єкта аудиту;
* частоти здійснення планових внутрішніх аудитів щодо кожного об’єкта аудиту.

Зразок шаблонів (форм) документів щодо ризик-орієнтованого відбору об’єктів аудиту, алгоритм наповнення відповідною інформацією такого документу наведено у [***додатку 2***](#_Додаток_2._Приклад).

**5. Формування плану діяльності з внутрішнього аудиту  
(внесення змін до нього)**

**Формування плану** діяльності з внутрішнього аудиту здійснюється **на підставі результатів оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту** (ґрунтується на результатах ідентифікації й оцінці ризиків та ризик-орієнтованого відбору об’єктів аудиту). Етапи цієї роботи описані у попередніх розділах.

Процедура формування та затвердження плану діяльності з внутрішнього аудиту, внесення змін до нього, оприлюднення плану та направлення копії затвердженого плану Мінфіну передбачена вимогами пункту 6 Порядку № 1001.

Формування та затвердження плану включає наступні послідовні етапи:

* визначення підрозділом внутрішнього аудиту потреб у ресурсах для забезпечення виконання запланованої діяльності;
* формування та затвердження плану на підставі результатів оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту;

***П****лан формується підрозділом на підставі результатів оцінки ризиків та затверджується керівником державного органу, його територіального органу, бюджетної установи не пізніше початку планового періоду.*

***В****несення змін до плану здійснюється у тому ж порядку, що і його затвердження, не пізніше завершення планового періоду.*

***П****лан (зведений план) та зміни до нього оприлюднюються на офіційному веб-сайті державного органу, його територіального органу та бюджетної установи.*

***К****опії затвердженого плану (зведеного плану) та зміни до нього разом із відповідними обґрунтуваннями щодо необхідності внесення таких змін надсилаються Мінфіну протягом десяти робочих днів з дати їх затвердження (вимоги абзаців третього – четвертого, сьомого – восьмого пункту 6 Порядку № 1001)*

* перегляд та внесення змін до плану (за потреби), формування та затвердження плану (із змінами);
* оприлюднення затвердженого плану (плану із змінами) на офіційному вебсайті установи;
* направлення Мінфіну копій затвердженого плану (плану із змінами).

**Визначення підрозділом внутрішнього аудиту потреб у ресурсах для забезпечення виконання запланованої діяльності**

Для розробки плану керівником підрозділу внутрішнього аудиту визначається потреба у ресурсах на здійснення внутрішніх аудитів та виконання заходів з іншої діяльності з внутрішнього аудиту.

Визначення потреб у ресурсах внутрішнього аудиту здійснюється з урахуванням:

* результатів, які очікуються від здійснення внутрішніх аудитів та виконання заходів з іншої діяльності з внутрішнього аудиту;
* складності та важливості запланованих об’єктів аудиту та заходів з іншої діяльності з внутрішнього аудиту;
* основних знахідок попередніх внутрішніх аудитів, що можуть вказувати на зміни у сферах діяльності установи;
* компетенції працівників підрозділу внутрішнього аудиту (ненавчені чи недосвідчені працівники довше виконуватимуть завдання) та кількості внутрішніх аудиторів, залучених до виконання завдання;
* досвіді щодо здійснення попередніх внутрішніх аудитів та виконання подібних заходів з іншої діяльності з внутрішнього аудиту (їх тривалості та кількості залучених внутрішніх аудиторів).

Потреби у ресурсах на здійснення внутрішніх аудитів визначаються з урахуванням усіх етапів проведення внутрішнього аудиту, зокрема:

* **організації внутрішнього аудиту та планування аудиторського завдання** (підготовка розпорядчого документа на проведення внутрішнього аудиту; визначення складу аудиторської групи та розподіл трудових ресурсів для проведення внутрішнього аудиту; попереднє вивчення об’єкта аудиту; проведення попередньої оцінки ризиків, пов’язаних з об’єктом аудиту; визначення обсягу аудиторського завдання; підготовка програми внутрішнього аудиту тощо). Під час визначення потреб на цьому етапі може виникнути потреба у залученні експертів/фахівців для здійснення внутрішнього аудиту (експертів-будівельників, ІТ-спеціалістів тощо). Вимоги щодо залучення до виконання аудиторського завдання експертів/фахівців містяться у підпункті 3 пункту 12 Порядку № 1001, пункту 3 Стандарту 3 «Професійна компетентність та ретельність»;

***П****рацівники підрозділу мають право:*

*…ініціювати перед керівником державного органу, його територіального органу та бюджетної установи залучення експертів, фахівців відповідних органів державної влади та органів місцевого самоврядування, державних фондів, підприємств, установ, організацій, інших юридичних осіб для забезпечення виконання аудиторського завдання (вимоги підпункту 3 пункту 12 Порядку № 1001).*

***У*** *разі якщо працівники підрозділу внутрішнього аудиту не мають достатніх знань, навичок чи інших вмінь, необхідних для виконання окремих питань аудиторського завдання, керівник підрозділу внутрішнього аудиту повинен ініціювати перед керівником установи залучення відповідних фахівців установи чи експертів відповідних органів влади та місцевого самоврядування, державних фондів, підприємств, установ, організацій, інших юридичних осіб для забезпечення виконання аудиторського завдання (вимоги пункту 3 Стандарту 3 «Професійна компетентність та ретельність»)*

* **виконання аудиторського завдання** (збір аудиторських доказів; аналіз зібраних даних; опитування вищого керівництва та відповідальних за діяльність осіб; дослідження питань програми внутрішнього аудиту; проведення вступних та заключних зустрічей з керівництвом та відповідальними за діяльність особами тощо);
* **документування перебігу та результатів внутрішнього аудиту** (документування зібраних даних та підготовка проекту аудиторського звіту з висновками та рекомендаціями; ознайомлення та обговорення з вищим керівництвом та відповідальними за діяльність особами проекту аудиторського звіту; внесення коректив у проект аудиторського звіту за результатами обговорення (за необхідності); підписання звіту керівником аудиторської групи або керівником і членами аудиторської групи; розгляд коментарів відповідальних за діяльність осіб та надання письмових висновків на них (за наявності); інформування керівника установи про результати здійснення внутрішнього аудиту; формування робочих та офіційних документів у справу за результатами здійснення внутрішнього аудиту тощо).

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

* **здійснення методологічної роботи** (здійснення моніторингу та аналізу змін у нормативно-правових актах з питань внутрішнього аудиту з метою актуалізації основних внутрішніх документів з питань внутрішнього аудиту; підготовка проектів основних внутрішніх документів з питань внутрішнього аудиту, їх погодження та затвердження відповідно до процедур та регламентів, визначених внутрішніми розпорядчими документами установи; розробка внутрішньої методології (зокрема, щодо ризик-орієнтованого планування діяльності з внутрішнього аудиту, здійснення внутрішніх аудитів, спрямованих на оцінку ефективності, результативності та якості виконання завдань та функцій, визначених актами законодавства (внутрішні аудити з оцінки ефективності), проведення внутрішніх оцінок якості внутрішнього аудиту) тощо);
* **здійснення ризик-орієнтованого планування діяльності з внутрішнього аудиту** (формування, наповнення, ведення та оновлення інформації у базі даних щодо об’єктів аудиту; проведення та документування результатів оцінки (актуалізації оцінки) ризиків та ризик-орієнтованого відбору об’єктів аудиту; проведення консультацій з відповідальними за діяльність особами; формування та затвердження керівником установи плану на підставі результатів оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту; перегляд та внесення змін до плану (за необхідності), формування та затвердження керівником установи плану (із змінами) тощо);
* **здійснення моніторингу врахування рекомендацій за результатами внутрішнього аудиту** (направлення відповідальним за діяльність особам листів-нагадувань щодо необхідності впровадження аудиторських рекомендацій для одержання підтвердження про вжиття відповідних заходів; узагальнення та аналіз інформації щодо стану впровадження аудиторських рекомендацій; формування, наповнення, ведення та оновлення у базі даних щодо моніторингу врахування рекомендацій за результатами здійснених внутрішніх аудитів тощо);
* **звітування (внутрішнє та зовнішнє) про діяльність підрозділу внутрішнього аудиту** (здійснення узагальнення та аналізу інформації про діяльність підрозділу внутрішнього аудиту, підготовка та подання звіту про результати діяльності підрозділу внутрішнього аудиту керівнику установи та Мінфіну за визначеними законодавством структурою/формою та термінами тощо);
* **проведення внутрішніх оцінок якості внутрішнього аудиту** (підготовка та затвердження Програми забезпечення і підвищення якості внутрішнього аудиту, відстеження стану виконання заходів, передбачених програмою; періодичне вивчення позиції зацікавлених сторін (вищого керівництва установи та відповідних за діяльність осіб) щодо діяльності з внутрішнього аудиту шляхом опитування; узагальнення та аналіз результатів проведених внутрішніх оцінок якості; підготовка керівнику установи звіту про результати внутрішньої оцінки якості);
* **професійний розвиток працівників підрозділу внутрішнього аудиту** (зокрема, проведення внутрішніх навчань у підрозділі внутрішнього аудиту; участь у навчальних заходах (семінарах тощо) з питань внутрішнього аудиту, внутрішнього контролю, бухгалтерського обліку та аудиту, основних напрямів діяльності державного органу; вивчення вітчизняного та міжнародного досвіду з питань внутрішнього аудиту (методичних посібників тощо); розроблення моделі загальних компетенцій, навиків та знань, необхідних для належного виконання аудиторських завдань тощо);
* **здійснення консультаційної діяльності**[[2]](#footnote-2) (надання порад і рекомендацій, роз’яснень вищому керівництву установи та відповідальним за діяльність особам (включаючи за письмовими запитами), зокрема, з питань підвищення ефективності та результативності діючих в установі процесів, впровадження в установі нових правил та процедур; дорадча участь у робочих групах/комісіях; надання допомоги вищому керівництву установи та відповідальним за діяльність особам з питань управління ризиками, зокрема, проведення робочих зустрічей, навчальних заходів з відповідних питань).

За результатами визначення потреб у ресурсах керівник підрозділу внутрішнього аудиту повинен забезпечити, зокрема:

* до початку виконання запланованої діяльності – подання/інформування керівника установи щодо потреб/обмежень (фінансових, людських, технічних, ІТ-ресурсів, необхідності залучення профільних експертів/спеціалістів тощо), у тому числі про вплив та наслідки обмеження у ресурсах внутрішнього аудиту з наданням відповідних пропозицій щодо шляхів вирішення цього питання (вимоги пункту 6 Стандарту 7 «Планування діяльності з внутрішнього аудиту»). Зразок визначення потреби в ресурсах для забезпечення виконання плану діяльності з внутрішнього аудиту наведено у [***додатку 3***](#_Додаток_9._Приклад);

***Д****ля забезпечення виконання підрозділом внутрішнього аудиту плану керівник підрозділу внутрішнього аудиту подає керівнику установи інформацію про потреби в ресурсах.*

***У*** *разі обмеження підрозділу внутрішнього аудиту в ресурсах керівник підрозділу внутрішнього аудиту письмово інформує керівника установи та аудиторський комітет (у разі його утворення) із зазначенням наслідків таких обмежень та надає пропозиції щодо вирішення зазначеного питання.*

***Д****ля ефективного використання трудових ресурсів керівник підрозділу внутрішнього аудиту визначає обсяги планового робочого часу на здійснення внутрішніх аудитів та виконання заходів з іншої діяльності з внутрішнього аудит (вимоги абзаців першого – третього пункту 6 Стандарту 7 «Планування діяльності з внутрішнього аудиту»).*

*Звіт про результати діяльності підрозділу внутрішнього аудиту має містити інформацію про стан виконання плану та/або причини його невиконання, рівень забезпечення ресурсами для провадження діяльності з внутрішнього аудиту (вимоги абзацу дев’ятого пункту 2 Стандарту 13 «Звітування про діяльність підрозділу внутрішнього аудиту»)*

* до початку виконання запланованої діяльності – визначення обсягів робочого часу на здійснення внутрішніх аудитів та виконання заходів з іншої діяльності з внутрішнього аудиту (вимоги пункту 6 Стандарту 7 «Планування діяльності з внутрішнього аудиту»). Результати цієї роботи відображаються у розділі IX плану (зведеного плану) (таких планів із змінами), роз’яснення щодо визначення планових обсягів робочого часу на здійснення внутрішніх аудитів та виконання заходів з іншої діяльності з внутрішнього аудиту наведено у рекомендаціях щодо складання плану (зведеного плану) діяльності з внутрішнього аудиту, внесення до них змін (відповідні форми планів та рекомендації щодо їх складання розміщено на офіційному вебсайті Мінфіну у рубриці «Зразки документів з внутрішнього контролю та внутрішнього аудиту» розділу «Державний внутрішній фінансового контроль» глави «Діяльність»);
* за результатами діяльності підрозділу внутрішнього аудиту – письмове (внутрішнє) інформування керівника установи у звіті про результати діяльності підрозділу внутрішнього аудиту (здійснюється не рідше одного разу на рік у терміни, визначені у внутрішніх документах з питань внутрішнього аудиту), зокрема, про стан виконання плану та/або причини його невиконання, рівень забезпечення ресурсами для здійснення діяльності з внутрішнього аудиту (вимоги пункту 2 Стандарту 13 «Звітування про діяльність підрозділу внутрішнього аудиту»).

**Формування плану діяльності з внутрішнього аудиту на підставі результатів оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту**

План діяльності з внутрішнього аудиту – це документ, який повинен надаватися керівнику установи на розгляд та затвердження. Тому план повинен демонструвати керівнику можливості підрозділу внутрішнього аудиту у допомозі в удосконаленні діяльності установи, підвищенні ефективності процесів управління, досягненні визначених мети (місії), стратегічних та інших цілей діяльності установи. Загалом план має бути своєрідною «вітриною», яка надає можливість вищому керівництву установи та відповідальним за діяльність особам усвідомити сутність роботи підрозділу внутрішнього аудиту та підкреслити переваги, які з'являться за результатами його діяльності.

План повинен бути чітко структурований, зрозумілий та логічно викладений, не містити протиріч (у визначених цілях, завданнях, об’єктах аудиту тощо), що забезпечує краще розуміння функції внутрішнього аудиту, допомагає у сприйнятті складних аспектів та/або ключових підходів у роботі підрозділу внутрішнього аудиту (наприклад, щодо ризик-орієнтованого планування діяльності з внутрішнього аудиту).

Підходи до формування плану діяльності з внутрішнього аудиту визначені пунктом 6 Порядку та Стандартом 7 «Планування діяльності з внутрішнього аудиту».

***К****ерівник підрозділу внутрішнього аудиту забезпечує формування плану на підставі результатів оцінки ризиків з метою визначення пріоритетів та результатів роботи підрозділу внутрішнього аудиту на наступні три роки, що мають враховувати стратегію (пріоритети) та цілі діяльності установи. У плані щороку визначаються завдання підрозділу внутрішнього аудиту на наступний календарний рік з урахуванням визначених пріоритетів та результатів діяльності підрозділу внутрішнього аудиту на відповідний трирічний період (вимоги абзацу другого пункту 6 Порядку № 6, пункту 2 Стандарту 7 «Планування діяльності з внутрішнього аудиту»)*

Зокрема, план діяльності з внутрішнього аудиту передбачає:

* визначення пріоритетів та результатів діяльності підрозділу внутрішнього аудиту на наступні три роки, які враховують стратегію (пріоритети) та цілі діяльності державного органу (стратегічний аспект);
* щорічно визначення завдань підрозділу внутрішнього аудиту на наступний календарний рік з урахуванням визначених пріоритетів та результатів діяльності підрозділу внутрішнього аудиту на відповідний трирічний період (операційний аспект).

Під час формування плану рекомендовано використовувати форму, розміщену на офіційному вебсайті Мінфіну у рубриці «Зразки документів з внутрішнього контролю та внутрішнього аудиту» розділу «Державний внутрішній фінансового контроль» глави «Діяльність». За потреби форми планів можуть додатково містити іншу інформацію з урахуванням особливостей діяльності державного органу.

Передбачений формами підхід до формування плану встановлює щорічне складання плану на трирічний плановий період – базовий плановий рік та наступні за ним два планових роки (тобто, фактично щороку в плані зміщується один плановий рік).

Наприклад, у 2024 році підрозділом внутрішнього аудиту формується план на 2025 – 2027 роки. Зокрема, у 2024 році сформований підрозділом внутрішнього аудиту план на 2024 – 2026 роки переглядається на предмет актуальності визначених стратегічних цілей внутрішнього аудиту, завдань та ключових показників результативності, ефективності та якості внутрішнього аудиту, включених до плану ризикових сфер та пріоритетних об’єктів аудиту та забезпечується складання плану на наступний трирічний період (2025 – 2027 роки). Інформація щодо попереднього планового року (2024 року) до плану на 2025 – 2027 роки не включається.

У разі необхідності протягом 2024 року (але не пізніше його завершення) до плану на 2024 – 2026 роки вносяться зміни в частині 2024 року шляхом формування плану на 2024 – 2026 роки (із змінами).

За аналогічною процедурою відбувається формування плану у наступних планових періодах.

Такий підхід до формування плану враховує сучасні міжнародні методології та практики щодо формування плану діяльності з внутрішнього аудиту у державному секторі різних країн, матеріали співтовариства PEMPAL, узгоджується з нормами Міжнародних стандартів внутрішнього аудиту, враховує вимоги національного законодавства у сфері внутрішнього аудиту.

Для формування реалістичного та корисного загалом для установи плану, керівник підрозділу внутрішнього аудиту виходячи з професійного досвіду повинен врахувати:

* наявні ресурси (наприклад, хоча вакансії можуть бути заповнені впродовж року, на момент формування плану слід враховувати лише існуючі трудові ресурси);
* можливість залучення та перерозподілу трудових ресурсів у плановому періоді, що включає заповнення вакантних посад; тимчасову відсутність персоналу (відпустки, навчання тощо); ротацію кадрів;
* організаційні, географічні та часові обмеження (наприклад, організаційно-структурні зміни у системі державного органу; місце розташування підприємств, установ та організацій, на яких передбачається здійснення внутрішнього аудиту; місця, до яких не можливо добратися у зимові періоди; відпускні періоди – як правило, літній період; періоди свят – Різдво, Новий рік, Великдень тощо);
* обмеження, передбачені вимогами абзацу першого пункту 4 Стандарту 7 «Планування діяльності з внутрішнього аудиту» щодо не включення до плану здійснення 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. Водночас, це обмеження не поширюється на повторні внутрішні аудити, що здійснюються підрозділом внутрішнього аудиту для дослідження фактів, викладених у скарзі на дії працівників підрозділу внутрішнього аудиту, що надійшла до установи (вимоги абзацу другого пункту 4 Стандарту 7 «Планування діяльності з внутрішнього аудиту»);

***Д****о планів не включається здійснення внутрішніх аудитів на підприємствах, в установах та організаціях, у яких із тих самих питань і за той самий період підрозділом внутрішнього аудиту здійснено внутрішні аудити менше ніж один календарний рік тому.*

***Д****ія цього Стандарту не поширюється на повторні внутрішні аудити, що здійснюються підрозділом внутрішнього аудиту для дослідження фактів, викладених у скарзі на дії працівників підрозділу внутрішнього аудиту, що надійшла до установи (вимоги пункту 4 Стандарту 7 «Планування діяльності з внутрішнього аудиту»)*

* резервування ресурсів на проведення позапланових внутрішніх аудитів (пункт 6 Стандарту 7 «Планування діяльності з внутрішнього аудиту»).

***П****лан формується з урахуванням резерву робочого часу на здійснення позапланових внутрішніх аудитів (вимоги абзацу четвертого пункту 6 Стандарту 7 «Планування діяльності з внутрішнього аудиту»)*

Здійснення внутрішніх аудитів забезпечується підрозділом внутрішнього аудиту як у плановому порядку (планові внутрішні аудити, які включаються до плану), так і внутрішні аудити можуть проводитися у позаплановому порядку (позапланові внутрішні аудити, які не включаються до плану).

З метою уникнення випадків внесення частих змін до плану під час формування плану слід враховувати резерв робочого часу на проведення позапланових внутрішніх аудитів, який доцільно визначати з урахуванням обсягів робочого часу, що використовувались підрозділом внутрішнього аудиту на проведення позапланових внутрішніх аудитів у попередніх роках.

У разі необхідності проведення позапланового внутрішнього аудиту, керівник підрозділу внутрішнього аудиту повинен переглядати план на предмет впливу позапланових аудитів на стан виконання плану та письмово поінформувати керівника установи про результати такого перегляду/впливу.

Проведення кожного позапланового внутрішнього аудиту керівник підрозділу внутрішнього аудиту повинен обговорювати з керівником установи щодо доцільності його здійснення, зокрема, з’ясовувати причини, які зумовлюють необхідність проведення позапланового внутрішнього аудиту, та переваги, що очікуються від його проведення.

Водночас, керівнику підрозділу внутрішнього аудиту необхідно утримувати певний баланс між виконанням позапланових внутрішніх аудитів та забезпеченням належного рівня здійснення внутрішніх аудитів, включених до плану на підставі результатів оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту.

У разі утворення підрозділів внутрішнього аудиту у територіальних органах та бюджетних установах керівником підрозділу внутрішнього аудиту державного органу забезпечується формування зведеного плану діяльності з внутрішнього аудиту (вимоги пункту 6 Порядку № 1001).

***З****а рішенням керівника державного органу підрозділи внутрішнього аудиту утворюються в територіальних органах та бюджетних установах в межах штатної чисельності їх працівників (вимоги абзацу 2 пункту 3 Порядку № 1001).*

***У*** *разі створення підрозділів у територіальних органах та бюджетних установах складається зведений план діяльності з внутрішнього аудиту (далі – зведений план) у державному органі, його територіальних органах та бюджетних установах, який формується підрозділом та затверджується керівником державного органу.*

***К****ерівники територіальних органів та бюджетних установ забезпечують подання плану керівнику підрозділу внутрішнього аудиту державного органу для подальшого формування зведеного плану керівником підрозділу внутрішнього аудиту державного органу з подальшим його затвердженням керівником державного органу (вимоги абзаців п’ятого – шостого пункту 6 Порядку № 1001)*

Зведений план формується у розрізі підрозділу внутрішнього аудиту апарату державного органу та підрозділів внутрішнього аудиту територіальних органів та бюджетних установ.

Процес формування та затвердження зведеного плану, внесення змін до нього, його оприлюднення на офіційному вебсайті державного органу здійснюється за аналогічними процедурами, визначеними для складання плану.

Під час формування зведеного плану діяльності з внутрішнього аудиту та зведеного плану діяльності з внутрішнього аудиту (із змінами) рекомендовано використовувати форми та рекомендації щодо їх складання, які розміщено на офіційному вебсайті Мінфіну у рубриці «Зразки документів з внутрішнього контролю та внутрішнього аудиту» розділу «Державний внутрішній фінансового контроль» глави «Діяльність». За потреби форми зведеного плану (плану із змінами) можуть додатково містити іншу інформацію з урахуванням особливостей діяльності державного органу.

**Внесення змін до плану діяльності з внутрішнього аудиту (за потреби)**

Підрозділом внутрішнього аудиту здійснюється моніторинг ключових подій, що відбулись у державному органі впродовж року, та які впливають на зміну стратегії (пріоритетів) та цілей діяльності державного органу та, відповідно, на ризики у діяльності державного органу (наприклад, створюють нові ризики). Зокрема, забезпечується перегляд прийнятих нормативно-правових актів, які визначають нові напрями (сфери) діяльності державного органу, або передбачають зміну завдань та функцій державного органу. Зміна керівництва установи (зокрема, призначення нового керівника установи), доручення Президента України, Верховної Ради України, Кабінету Міністрів України, публікації у медіа щодо діяльності установи також можуть вплинути на актуальність запланованих об’єктів аудиту.

За результатами такого моніторингу керівник підрозділу внутрішнього аудиту оцінює вплив таких подій на визначені у плані стратегічні цілі та завдання внутрішнього аудиту, ризикові сфери внутрішнього аудиту та пріоритетні об’єкти аудиту.

З метою оновлення визначених у плані пріоритетних об’єктів аудиту підрозділом внутрішнього аудиту щороку проводиться оцінка ризиків (або забезпечується актуалізація попередньої оцінки ризиків), здійснюється перегляд та актуалізація (уточнення) оцінки факторів відбору об’єктів аудиту, зокрема:

* здійснюється перегляд та актуалізація (уточнення) ідентифікованих ризиків з урахуванням змін, що відбулися після останнього перегляду, застосованих критеріїв впливу/ймовірності та присвоєних ризикам рівнів (балів) для визначення впливу (розміру наслідків) ризиків. Час від часу корисно ідентифікувати ризики та проводити їх оцінку «з чистого листа» з подальшим порівнянням одержаних результатів з раніше визначеними та оціненими ризиками;
* здійснюється перегляд та актуалізація (уточнення) присвоєних факторам відбору бальних оцінок та вагових коефіцієнтів, визначеного ступеня пріоритету об’єктів аудиту для визначення змін у переліку включених до плану пріоритетних об’єктів аудиту за рік;
* враховуються результати здійснених внутрішніх аудитів за попередні роки, які можуть призводити до змін початкової оцінки ризиків. Наприклад, за результатами здійснення внутрішнього аудиту встановлено відсутність/неефективність запроваджених заходів контролю, що потребує здійснення внутрішнього аудиту щодо об’єктів аудиту, стосовно яких можуть виникнути подібні проблеми.

Актуалізацію попередньої оцінки ризиків та факторів відбору об’єктів аудиту доцільно здійснювати не рідше одного разу на рік – до початку формування плану на наступні планові періоди (рекомендовано до 30 листопада). Результати актуалізації попередньої оцінки ризиків повинні документально оформлюватися.

За результатами проведеної роботи підрозділом внутрішнього аудиту забезпечується перегляд та внесення змін до плану в частині актуалізації стратегічних цілей, завдань та ключових показників ефективності, результативності та якості внутрішнього аудиту, переліку пріоритетних об’єктів аудиту та, за потреби, заходів з іншої діяльності з внутрішнього аудиту.

Підстави та умови для перегляду і внесення змін до плану визначено абзацом першим пункту 5 Стандарту 7 «Планування діяльності з внутрішнього аудиту». Зокрема, внесення змін можливе у разі зміни стратегії (пріоритетів) та цілей діяльності державного органу, за результатами проведення оцінки ризиків та з інших обґрунтованих підстав.

***У*** *разі зміни стратегії (пріоритетів) та цілей діяльності державного органу, за результатами щорічної оцінки ризиків та з інших обґрунтованих підстав керівник підрозділу внутрішнього аудиту забезпечує перегляд та внесення змін до плану (вимоги пункту 5 Стандарту 7 «Планування діяльності з внутрішнього аудиту»)*

Серед інших обґрунтованих підстав для внесення змін до плану можуть бути доручення керівника установи на проведення внутрішнього аудиту. Підставою для прийняття такого рішення керівником установи можуть бути, зокрема, доручення вищих органів влади (Офісу Президента України, Верховної Ради України, Кабінету Міністрів України), депутатські звернення, звернення державних органів, бюджетних установ, державних підприємств та організацій, скарги фізичних та юридичних осіб, а також звернення вищого керівництва установи та відповідальних за діяльність осіб (керівників структурних підрозділів установи, підпорядкованих підприємств/установ) щодо здійснення внутрішніх аудитів.

У разі прийняття керівником установи рішення щодо проведення внутрішнього аудиту у періоді, на який вже сформовано план, здійснення такого аудиту може забезпечуватися підрозділом внутрішнього аудиту у плановому порядку (відповідно, проведення внутрішнього аудиту включається до плану за дорученням/зверненням шляхом внесенням відповідних змін до плану), а також можливе у позаплановому порядку (відповідно, здійснення внутрішнього аудиту не включається до плану).

Внесення змін до плану здійснюється шляхом формування керівником підрозділу внутрішнього аудиту плану діяльності з внутрішнього аудиту (із змінами).

Обґрунтування щодо необхідності внесення змін до плану керівник підрозділу внутрішнього аудиту письмово надає керівнику установи.

***З****а потреби внесення змін до плану керівник підрозділу внутрішнього аудиту надає керівнику установи відповідне письмове обґрунтування (вимоги абзацу другого пункту 5 Стандарту 7 «Планування діяльності з внутрішнього аудиту»)*

Форми обґрунтувань щодо внесення змін до плану (зведеного плану) наведено у додатку до форми плану (із змінами) та у додатку до форми зведеного плану (із змінами) (відповідні форми планів розміщено на офіційному вебсайті Мінфіну у рубриці «Зразки документів з внутрішнього контролю та внутрішнього аудиту» розділу «Державний внутрішній фінансового контроль» глави «Діяльність»).

**Затвердження плану діяльності з внутрішнього (плану із змінами)**

Терміни затвердження плану діяльності з внутрішнього аудиту та внесення змін до нього встановлені пунктом 6 Порядку № 1001.

Зокрема, підписаний керівником підрозділу внутрішнього аудиту план подається на розгляд та затвердження керівнику установи не пізніше початку планового періоду.

Внесення змін до плану здійснюється у тому ж порядку, що і його затвердження. Підрозділом внутрішнього аудиту формується план діяльності з внутрішнього аудиту (із змінами), який підписується керівником підрозділу внутрішнього аудиту та подається керівнику установи на розгляд та затвердження не пізніше завершення планового періоду. Відповідно, якщо здійснення внутрішніх аудитів передбачається провести у плановому порядку (згідно із планом діяльності внутрішнього аудиту), відповідні зміни до плану має бути внесено до початку проведення таких аудитів.

***П****лан формується підрозділом внутрішнього аудиту на підставі результатів оцінки ризиків та затверджується керівником державного органу, його територіального органу, бюджетної установи не пізніше початку планового періоду.*

***В****несення змін до плану здійснюється у тому ж порядку, що і його затвердження, не пізніше завершення планового періоду.*

***П****лан (зведений план) та зміни до нього оприлюднюються на офіційному веб-сайті державного органу, його територіального органу та бюджетної установи (вимоги абзаців третього-четвертого, сьомого пункту 6 Порядку № 1001)*

**Оприлюднення затвердженого плану діяльності з внутрішнього аудиту (плану із змінами)**

Оприлюднення затвердженого керівником установи плану діяльності з внутрішнього аудиту здійснюється на офіційному вебсайті установи.

Враховуючи, що зміни до плану вносяться у порядку їх затвердження, то план діяльності з внутрішнього аудиту (із змінами) також має оприлюднюватися на офіційному вебсайті установи.

З метою розміщення плану діяльності з внутрішнього аудиту (плану із змінами) на вебсайті установи доцільно створити окремий розділ під назвою «Внутрішній аудит», в якому розміщувати такі плани, а також може оприлюднюватися інша інформація, яка стосується діяльності з внутрішнього аудиту (наприклад, внутрішні документи з питань здійснення внутрішнього аудиту, інформацію про аудиторський комітет (зокрема, Положення про аудиторський комітет, його персональний склад)).

**Направлення Мінфіну копії затвердженого плану діяльності з внутрішнього аудиту (плану із змінами)**

Після затвердження керівником установи плану діяльності з внутрішнього аудиту (плану із змінами) та їх оприлюднення на офіційному вебсайті установи, копії затвердженого плану (плану із змінами з відповідним обґрунтуванням щодо необхідності внесення таких змін) надсилаються Мінфіну протягом 10 робочих днів з дати їх затвердження (вимоги пункту 6 Порядку № 1001).

***К****опії затвердженого плану (зведеного плану) та зміни до нього разом із відповідними обґрунтуваннями щодо необхідності внесення таких змін надсилаються Мінфіну протягом десяти робочих днів з дати їх затвердження**(вимоги абзацу восьмого пункту 6 Порядку № 1001)*

Під час направлення Мінфіну копії затвердженого плану (плану із змінами) слід вказувати розділ на офіційному вебсайті установи, у якому розміщена копія такого плану.

Міністерством фінансів України здійснюється опрацювання надісланих державними органами копій затверджених планів (зведених планів) діяльності з внутрішнього аудиту (таких планів із змінами) на предмет, зокрема:

* дотримання вимог законодавства у сфері внутрішнього аудиту (зокрема, формування плану на підставі результатів оцінки ризиків; невключення до плану діяльності, не пов’язаної безпосередньо із здійсненням внутрішнього аудиту; врахування резерву робочого часу на проведення позапланових внутрішніх аудитів під час здійснення у плані розрахунків обсягів робочого часу; невключення до плану здійснення 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; включення до плану повного комплексу завдань (заходів) з іншої діяльності з внутрішнього аудиту; своєчасності затвердження керівником установи плану (плану із змінами); своєчасності направлення Мінфіну копії затвердженого плану (плану із змінами), подання Мінфіну відповідних обґрунтувань щодо необхідності внесення змін до плану);
* наявності зв’язку між визначеними стратегічними цілями/завданнями/ключовими показниками результативності, ефективності та якості внутрішнього аудиту та запланованими пріоритетними об’єктами аудиту;
* визначення ключових показників результативності, ефективності та якості внутрішнього аудиту, за якими можна виміряти та оцінити (кількісно та/або якісно) результат виконання стратегічних цілей та завдань внутрішнього аудиту, а саме: чітких та конкретних, вимірюваних, реалістичних та можливих для досягнення, необхідних для державного органу, визначених у часових межах щодо їх досягнення;
* включення внутрішніх аудитів, спрямованих на оцінку ефективності, результативності та якості виконання бюджетних програм, надання адміністративних послуг, здійснення контрольно-наглядових функцій, функціональних процесів, ступеня виконання і досягнення цілей тощо (планування внутрішніх аудитів з оцінки ефективності);
* забезпечення належного рівня завантаженості працівників підрозділу внутрішнього аудиту безпосередньо здійсненням внутрішніх аудитів;
* повноти та/або коректності інформаційного наповнення плану (зокрема, забезпечення логічності та послідовності викладення інформації у взаємопов’язаних розділах плану, відсутності арифметичних помилок під час здійснення розрахунків обсягів робочого часу на здійснення внутрішніх аудитів та виконання заходів з іншої діяльності з внутрішнього аудиту).

За результатами проведеного Мінфіном аналізу на адресу державних органів надсилаються рекомендації, спрямовані на забезпечення належного здійснення ризик-орієнтованого планування діяльності з внутрішнього аудиту та покращення якості формування планів діяльності з внутрішнього аудиту, їх інформаційного наповнення.

Якщо за результатами такого аналізу виявлено питання, які потребують детального дослідження, відповідні факти враховуються під час планування оцінки функціонування системи внутрішнього аудиту (зовнішньої оцінки якості внутрішнього аудиту) у державних органах.

**6. Визначення у внутрішніх документах аспектів ризик-орієнтованого планування діяльності з внутрішнього аудиту**

**Процес планування діяльності з внутрішнього аудиту** (починаючи від визначення простору аудиту і закінчуючи етапом формування та затвердження плану) **визначається** керівником підрозділу внутрішнього аудиту **у внутрішніх документах з питань здійснення внутрішнього аудиту в частині планування діяльності з внутрішнього аудиту**, які затверджуються керівником установи (вимоги пунктів 3, 4 Стандарту 1 «Завдання, права та обов’язки»).

Зокрема, внутрішні документи з питань здійснення внутрішнього аудиту мають визначати:

***В****нутрішні документи з питань здійснення внутрішнього аудиту мають врегульовувати такі питання:*

*планування діяльності з внутрішнього аудиту, в тому числі 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…*

*Внутрішні документи з питань здійснення внутрішнього аудиту затверджує керівник установи (вимоги пунктів 3 та 4 Стандарту 1 «Завдання, права та обов’язки»)*

* методологічні підходи до визначення простору аудиту, його формалізації та документування шляхом ведення бази даних та підтримки її в актуальному стані, а саме:

визначати структуру (форму) складання, наповнення, ведення та оновлення інформації у базі даних щодо об’єктів аудиту;

передбачати структурування простору аудиту за напрямами (сферами) діяльності державного органу, їх частинами – бюджетними програмами; адміністративними послугами; контрольно-наглядовими функціями; функціональними процесами; загальними процесами (горизонтальний принцип розподілу об’єктів аудиту), а також за організаційною структурою та місцем розташування – структурними підрозділами установи; підприємствами, установами та організаціями, які належать до сфери управління державного органу (вертикальний принцип розподілу об’єктів аудиту), забезпечити зв’язок об’єктів аудиту з структурними підрозділами установи, підпорядкованими підприємствами, установами та організаціями, відповідальними за реалізацію відповідних програм/послуг/функцій/процесів;

визначати повний спектр документальних джерел з метою правильного визначення об’єктів аудиту та належного розподілу об’єктів аудиту у просторі аудиту (за горизонтальним та вертикальним принципами);

передбачати включення до бази даних інформації, яка передбачає зв’язок кожного об’єкта аудиту з процедурами ідентифікації й оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту з метою належного здійснення ризик-орієнтованого планування діяльності з внутрішнього аудиту;

передбачати за кожним об’єктом аудиту, що міститься у базі даних, включення відомостей щодо здійснених внутрішніх аудитів/проведених контрольних заходів зовнішніми контролюючими органами (Рахунковою палатою, органами державного фінансового контролю тощо) у системі державного органу з метою отримання повноти даних щодо відповідного об’єкта аудиту та покращення процесу відбору об’єктів аудиту (зокрема, щодо тематики внутрішнього аудиту/контрольного заходу; інформації про виявлені проблеми та порушення/недоліки; дати здійснення внутрішнього аудиту/контрольного заходу; періоду, за який здійснювався внутрішній аудит/контрольний захід; назви структурного підрозділу установи, підприємств, установ та організацій, які належать до сфери управління державного органу, де здійснювався внутрішній аудит/контрольний захід; стану реагування на аудиторські висновки та рекомендації/виконання обов’язкових вимог за результатами здійснених внутрішніх аудитів/контрольних заходів);

визначати процедуру взаємодії підрозділу внутрішнього аудиту з вищим керівництвом установи та відповідальними за діяльність особами (керівниками структурних підрозділів установи, підпорядкованих підприємств/установ) з питань формування та оновлення інформації у базі даних з метою з’ясування думки щодо повноти включених до бази даних об’єктів аудиту, їх важливості та актуальності, достатності/недостатності або надмірного рівня деталізації (зокрема, щодо проведення та документування результатів консультацій та/або направлення письмових запитів з метою отримання відповідної інформації; визначення переліку питань, які мають обговорюватися під час консультацій, та/або надаватися для отримання письмової відповіді, умови та терміни проведення консультацій/направлення письмових запитів);

визначати умови та терміни актуалізації інформації у базі даних (наприклад, здійснювати уточнення простору аудиту не рідше одного разу на рік до початку формування плану на наступні планові періоди);

* методологічні підходи до організації, здійснення та документування процесу ризик-орієнтованого планування діяльності з внутрішнього аудиту, а саме:

передбачати врахування повного спектру відомостей для ідентифікації ризиків (зокрема, інформації про типові/системні порушення/недоліки, встановлені за результатами внутрішніх аудитів, звіти/акти зовнішніх контролюючих органів) та переліку документальних джерел, які допомагають визначати як фінансові, так і нефінансові ризики (зокрема, річні, піврічні, квартальні плани, річні звіти про діяльність установи);

визначати підходи до ідентифікації та документування підрозділом внутрішнього аудиту ризиків якщо у діяльності установи забезпечено здійснення управління ризиками та визначено підходи щодо документування такої діяльності (зокрема, щодо здійснення аналізу підрозділом внутрішнього аудиту ідентифікованих та оцінених ризиків відповідальними за діяльність особами, визначених ними способів реагування на ризики та розроблених заходів контролю для впливу на ризики з метою врахування результатів такого аналізу під час проведення (актуалізації) оцінки ризиків), у тому числі процедуру взаємодії підрозділу внутрішнього аудиту з іншими структурними підрозділами установи з питань управління ризиками (зокрема, щодо щорічного надання підрозділу внутрішнього аудиту інформації про результати ідентифікованих та оцінених ризиків, визначених способів реагування на ризики, розроблених заходів контролю для впливу на ризики з метою проведення (актуалізації) оцінки ризиків для планування діяльності з внутрішнього аудиту);

визначати підходи до ідентифікації та документування підрозділом внутрішнього аудиту ризиків, коли в діяльності установи управління ризиками не запроваджене (зокрема, щодо ідентифікації ризиків, їх оцінки за визначеними критеріями впливу та ймовірності, загальної оцінки ризиків за впливом та ймовірністю);

визначати процедуру проведення та документування результатів консультацій з вищим керівництвом та відповідальними за діяльність особами (керівниками структурних підрозділів установи, підпорядкованих підприємств/установ) щодо проблемних питань та ризиків у діяльності установи та/або направлення письмових запитів з метою отримання відповідної інформації; перелік питань, які мають обговорюватися під час консультацій та/або надаватися для отримання письмової відповіді, умови та терміни проведення консультацій/направлення письмових запитів;

визначати критерії та шкалу оцінювання ризиків – за розміром наслідків для установи у випадку настання події (оцінка впливу) та за ймовірністю настання подій, що створюють ризики (оцінка ймовірності);

визначати процедури та терміни проведення (актуалізації) оцінки ризиків, узагальнення результатів ідентифікованих та оцінених ризиків, забезпечення своєчасного перегляду та оновлення ідентифікованих та оцінених ризиків, документування процедури ідентифікації та оцінки (актуалізації оцінки) ризиків;

передбачати широкий набір фінансових/нефінансових факторів відбору об’єктів аудиту для проведення планових внутрішніх аудитів (фінансова важливість/матеріальність, складність діяльності, масштаб змін, репутаційна чутливість, загальна політика внутрішнього контролю, надійність керівництва, можливість для зловживань, питання, які цікавлять керівництво, час від попереднього аудиту, стан впровадження аудиторських рекомендацій);

визначати процедури проведення та документування оцінки кожного фактору відбору, у тому числі критерії оцінки кожного фактору відбору з відповідними бальними оцінками та ваговими коефіцієнтами, розрахунок індексу пріоритетності з метою визначення ступеня пріоритету об’єктів аудиту та частоти здійснення планових внутрішніх аудитів щодо кожного об’єкта аудиту;

передбачати процедуру визначення частоти здійснення планових внутрішніх аудитів щодо кожного об’єкта аудиту з урахуванням визначеного ступеня пріоритету об’єкта аудиту та розрахованого індексу пріоритетності;

передбачити процедуру визначення загального періоду внутрішнього аудиту;

передбачати шаблони (форми) документів, які будуть застосовуватися під час ідентифікації й оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту;

визначати резерв робочого часу на здійснення позапланових внутрішніх аудитів з урахуванням обсягів робочого часу, використаних на проведення позапланових внутрішніх аудитів у попередніх роках;

передбачати процедуру здійснення розрахунків обсягів планового робочого часу на здійснення внутрішніх аудитів та виконання заходів з іншої діяльності з внутрішнього аудиту, у тому числі коефіцієнти участі працівників підрозділу внутрішнього аудиту у здійсненні внутрішніх аудитів (з урахуванням рівня посад) (роз’яснення з відповідних питань наведено у рекомендаціях щодо складання плану (зведеного плану) діяльності з внутрішнього аудиту (таких планів із змінами), які розміщено на офіційному вебсайті Мінфіну у рубриці «Зразки документів з внутрішнього контролю та внутрішнього аудиту» розділу «Державний внутрішній фінансового контроль» глави «Діяльність»);

визначати структуру (форму) та наповнення плану (зведеного плану) діяльності з внутрішнього аудиту (таких планів із змінами) (відповідні форми планів та рекомендації щодо їх складання розміщено на офіційному вебсайті Мінфіну у рубриці «Зразки документів з внутрішнього контролю та внутрішнього аудиту» розділу «Державний внутрішній фінансового контроль» глави «Діяльність»);

* інші обов’язкові вимоги в частині планування діяльності з внутрішнього аудиту, встановлені законодавством у сфері внутрішнього аудиту, зокрема, щодо:

визначення простору аудиту, його формалізації та документування шляхом ведення бази даних та підтримки її в актуальному стані (пункт 1 Стандарту 7);

забезпечення формування плану на підставі результатів оцінки ризиків, яка проводиться не рідше одного разу на рік, а також документального оформлення результатів оцінки ризиків (пункти 2, 3 Стандарту 7);

визначення підходів до формування плану – у плані визначаються пріоритети та результати діяльності підрозділу внутрішнього аудиту на наступні три роки, які враховують стратегію (пріоритети) та цілі діяльності державного органу; у плані 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 № 1001, пункт 2 Стандарту 7);

з’ясування та врахування думки керівника установи, а також проведення консультацій з відповідальними за діяльність особами щодо проблемних питань та ризиків, які впливають на досягнення установою цілей (пункт 2 Стандарту 7);

не включення до плану здійснення внутрішніх аудитів на підприємствах, в установах та організаціях, у яких із тих самих питань і за той самий період підрозділом внутрішнього аудиту здійснено внутрішні аудити менше ніж один календарний рік тому (пункт 4 Стандарту 7);

не поширення дії внутрішніх документів з питань здійснення внутрішнього аудиту в частині планування на повторні внутрішні аудити, що здійснюються підрозділом внутрішнього аудиту для дослідження фактів, викладених у скарзі на дії працівників підрозділу внутрішнього аудиту, що надійшла до установи (пункт 4 Стандарту 7);

визначення підстав, відповідно до яких здійснюється перегляд та внесення змін до плану – у разі зміни стратегії (пріоритетів) та цілей діяльності установи, за результатами проведення оцінки ризиків та з інших обґрунтованих підстав, надання керівнику установи відповідного письмового обґрунтування за потреби внесення змін до плану (пункт 5 Стандарту 7);

подання керівнику установи інформації щодо потреби у ресурсах для забезпечення виконання плану, письмового інформування керівника установи та аудиторський комітет (у разі його утворення) про наявність обмежень у ресурсах із зазначенням наслідків таких обмежень та надання пропозицій щодо вирішення зазначеного питання, визначення обсягів планового робочого часу на здійснення внутрішніх аудитів та виконання заходів з іншої діяльності з внутрішнього аудиту (пункт 6 Стандарту 7);

визначення термінів формування підрозділом внутрішнього аудиту та затвердження керівником установ плану – не пізніше початку планового періоду, внесення змін до плану у тому ж порядку, що і його затвердження – не пізніше завершення планового періоду (пункт 6 Порядку № 1001);

висвітлення плану (змін до нього) на офіційному вебсайті установи, надання Мінфіну копії затвердженого плану (зміни до нього разом із відповідними обґрунтуваннями щодо необхідності внесення таких змін) протягом 10 робочих днів з дати їх затвердження (пункт 6 Порядку № 1001);

інформування керівника установи про стан виконання плану та/або причини його невиконання під час звітування про результати діяльності підрозділу внутрішнього аудиту (пункт 2 Стандарту 13).

У положенні про підрозділ внутрішнього аудиту визначаються завдання та функції (відповідальність) підрозділу внутрішнього аудиту, його права та обов’язки в частині ключових аспектів планування діяльності з внутрішнього аудиту, зокрема, щодо:

* визначення простору аудиту, його формалізації та документування шляхом формування, наповнення, ведення та своєчасного оновлення інформації у базі даних щодо об’єктів аудиту;
* проведення (актуалізації) оцінки ризиків не рідше одного разу на рік, її документального оформлення;
* проведення консультацій з вищим керівництвом та відповідальними за діяльність особами (керівниками структурних підрозділів установи, підпорядкованих підприємств/установ) з питань формування та оновлення інформації у базі даних щодо об’єктів аудиту, проведення оцінки ризиків;
* формування плану на підставі результатів оцінки ризиків;
* перегляду та внесення змін до плану у разі зміни стратегії (пріоритетів) та цілей діяльності державного органу, за результатами оцінки ризиків та з інших обґрунтованих підстав, надання керівнику установи письмового обґрунтування щодо необхідності внесення змін до плану;
* подання керівнику установи та аудиторському комітету (у разі його утворення) письмової інформації про потреби/обмеження у ресурсах для забезпечення виконання підрозділом внутрішнього аудиту плану, із зазначенням наслідків таких обмежень та надання пропозицій щодо вирішення зазначеного питання.

Аналогічні завдання та функції (відповідальність), права та обов’язки визначаються у посадових інструкціях працівників підрозділу внутрішнього аудиту. При цьому, у посадових інструкціях забезпечується розподіл повноважень та відповідальності працівників підрозділу внутрішнього аудиту з урахуванням рівня посад, зокрема, щодо безпосереднього виконання зазначених завдань та функцій або участі у їх виконанні.

Якщо у державному органі функціонує посадова особа, на яку покладаються повноваження щодо здійснення внутрішнього аудиту, питання щодо планування діяльності з внутрішнього аудиту, передбачені положенням про підрозділ внутрішнього аудиту, включаються до посадової інструкції працівника, на якого покладаються повноваження щодо здійснення діяльності з внутрішнього аудиту.

З урахуванням наведених у цьому посібнику аспектів щодо ризик-орієнтованого планування діяльності з внутрішнього аудиту у внутрішніх документах з питань здійснення внутрішнього аудиту визначаються єдині підходи до планування діяльності з внутрішнього аудиту, які поширюються на роботу підрозділу внутрішнього аудиту державного органу та підрозділів внутрішнього аудиту територіальних органів та бюджетних установ (вимоги пункту 7 Стандарту 7 «Планування діяльності з внутрішнього аудиту»).

***У*** *разі утворення підрозділів внутрішнього аудиту в територіальних органах та бюджетних установах, що належать до сфери управління державного органу, керівник підрозділу внутрішнього аудиту державного органу визначає єдині підходи до планування діяльності з внутрішнього аудиту (вимоги пункту 7 Стандарту 7 «Планування діяльності з внутрішнього аудиту»)*

Зокрема, єдині підходи визначаються до порядку/процедур:

* формування, наповнення, ведення та оновлення інформації у зведеній базі даних (зокрема, визначення строків та умов надання підрозділу внутрішнього аудиту державного органу інформації щодо об’єктів аудиту, розроблення шаблонів документів щодо подання відповідної інформації, формування зведеної бази даних підрозділом внутрішнього аудиту державного органу);
* ідентифікації й оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту (зокрема, встановлення строків надання підрозділу внутрішнього аудиту державного органу відповідної інформації для формування зведеного плану, розроблення шаблонів документів щодо подання інформації, стандартних форм документів щодо ідентифікації та оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту);
* формування, погодження та затвердження зведеного плану, внесення змін до нього (зокрема, визначення порядку та строків надання підрозділу внутрішнього аудиту державного органу пропозицій щодо включення/виключення до/з плану об’єктів аудиту/тематики внутрішніх аудитів, здійснення підрозділом внутрішнього аудиту державного органу розгляду, опрацювання, надання зауважень/пропозицій та погодження проекту плану підрозділів внутрішнього аудиту територіальних органів та бюджетних установ, розроблення шаблонів документів щодо подання підрозділом внутрішнього аудиту державного органу інформації для формування зведеного плану (зведеного плану із змінами), подання їх на затвердження керівнику державного органу).

Керівник підрозділу внутрішнього аудиту державного органу координує діяльність підрозділів внутрішнього аудиту територіального органу та бюджетної установи, а також надає пропозиції щодо забезпечення належної якості здійснення внутрішнього аудиту такими підрозділами (вимоги абзацу восьмого пункту 10 Порядку № 1001).

***К****ерівник підрозділу внутрішнього аудиту державного органу координує діяльність підрозділів внутрішнього аудиту територіального органу та бюджетної установи, а також надає пропозиції щодо забезпечення належної якості здійснення внутрішнього аудиту такими підрозділами (вимоги абзацу восьмого пункту 10 Порядку № 1001)*

Відповідна координація має здійснюватися на всіх етапах діяльності з внутрішнього аудиту, у тому числі – на етапі планування.

Процедура координації повинна бути врегульована у внутрішніх документах з питань здійснення внутрішнього аудиту в частині планування, зокрема, щодо здійснення аналізу підрозділом внутрішнього аудиту державного органу:

* баз даних підрозділів внутрішнього аудиту територіальних органів та бюджетних установ на предмет правильності та повноти включення інформації щодо об’єктів аудиту;
* обґрунтувань до плану діяльності з внутрішнього аудиту (змін до нього), наданих підрозділами внутрішнього аудиту територіальних органів та бюджетних установ, на предмет включення до плану об’єктів аудиту на підставі результатів оцінки ризиків та ризик-орієнтованого відбору;
* обсягів робочого часу, визначених підрозділами внутрішнього аудиту територіальних органів та бюджетних установ, на здійснення внутрішніх аудитів та виконання заходів з іншої діяльності з внутрішнього аудиту з метою їх ефективного розподілу та використання.

**Додатки**

## **Додаток 1. Приклад формалізації та документування простору аудиту шляхом ведення бази даних**

Зразок формалізації та документування простору аудиту шляхом ведення бази даних підготовлено за підходами, визначеними у цьому посібнику. Зокрема, за структурою (формою) та наповненням приклад передбачає розподіл об’єктів аудиту за горизонтальним та вертикальними принципами, зв’язок об’єктів аудиту з структурними підрозділами державного органу та підпорядкованими підприємствами/установами, відповідальними за реалізацію відповідних програм/послуг/функцій/процесів, а також поєднання об’єктів аудиту з процедурами ідентифікації й оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту (детально документування відповідних процедур проілюстровано у [***додатку 2***](#_Додаток_8._Приклад)).

З метою отримання повноти даних щодо кожного об’єкта аудиту для покращення процесу відбору об’єктів у зразку передбачено включення інших відомостей (зокрема, щодо здійснених внутрішніх аудитів, проведених контрольних заходів зовнішніми контролюючими органами). Для формування зведеної бази даних у прикладі передбачено включення інформації у розрізі підрозділів внутрішнього аудиту державного органу та підрозділів внутрішнього аудиту територіальних органів та бюджетних установ.

Приклад розроблено з використанням програми MS Office Excel. Ця програма призначена для роботи з електронними таблицями та дозволяє керувати даними. За допомогою застосування спеціальних інструментів у таблиці Excel можна фільтрувати та сортувати дані, застосовувати формули та гіперпосилання. Під час формування бази даних можна скористатися вбудованими шаблонами Microsoft Excel. У прикладі проілюстровано можливості Microsoft Excel під час формування та ведення бази даних в електронному вигляді.

Приклад розміщено на офіційному вебсайті Мінфіну у рубриці «Зразки документів з внутрішнього контролю та внутрішнього аудиту» розділу «Розвиток державного внутрішнього фінансового контролю» глави «Діяльність».

Зразок формалізації та документування простору аудиту шляхом ведення бази даних розроблено на прикладі сфери ІТ-систем та технологій та включає головну таблицю бази даних «Інформація про об’єкти простору внутрішнього аудиту» (рис. 1 – 2) та допоміжні таблиці (рис. 3 – 12), які використовуються під час заповнення головної таблиці. Допоміжні таблиці розміщуються на окремих аркушах книги Excel.

Головна таблиця «Інформація про об’єкти простору внутрішнього аудиту» (рис. 1 – 2) містить інформацію щодо кожного об’єкта аудиту, включеного до бази даних щодо простору аудиту, яка необхідна підрозділу внутрішнього аудиту для отримання повноти даних щодо кожного об’єкта аудиту, що надалі впливає на покращення процесу відбору об’єктів аудиту, а саме:

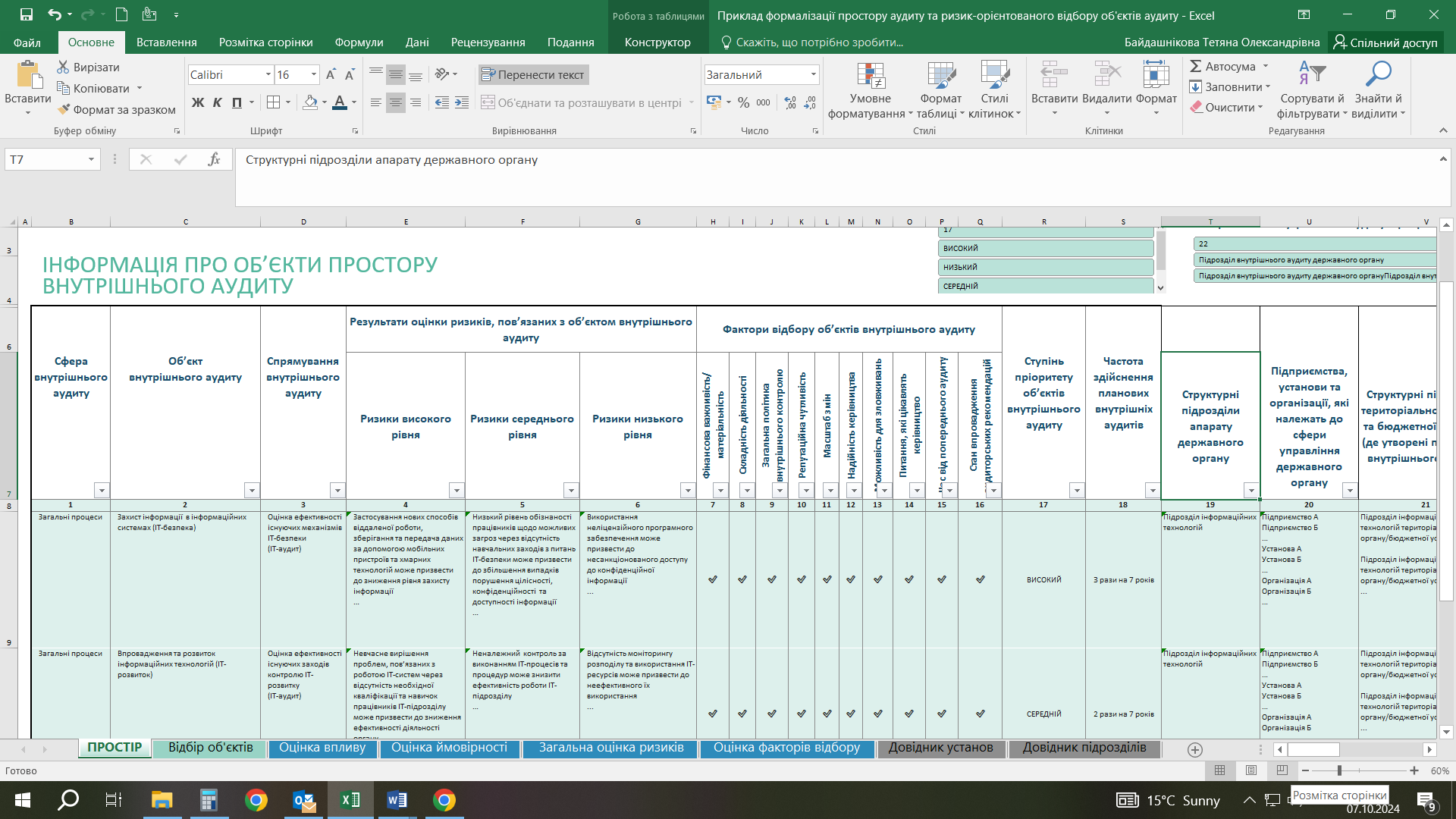
* назву сфери внутрішнього аудиту (зокрема, визначення сфери для об’єкта аудиту дозволяє виокремити функціональні процеси від загальних процесів, а також виділити окремо бюджетні програми, адміністративні послуги, контрольно-наглядові функції від функціональних та загальних процесів);
* назву об’єкта внутрішнього аудиту (зокрема, об’єкт аудиту визначається у відповідності до законодавчо визначеного поняття «об’єкта внутрішнього аудиту», передбаченого вимогами пункту 2 Порядку № 1001);
* спрямування внутрішнього аудиту (оцінка ефективності планування і виконання бюджетних програм та результатів їх виконання, управління бюджетними коштами, якості надання адміністративних послуг та здійснення контрольно-наглядових функцій, функціональних та загальних процесів, надійності, ефективності та результативності інформаційних систем і технологій, ефективності функціонування системи управління, внутрішнього контролю та управління ризиками, ступеня виконання та досягнення цілей тощо (*оцінка ефективності*); оцінка дотримання вимог законодавства під час виконання бюджетних програм, надання адміністративних послуг, здійснення контрольно-наглядових функцій, функціональних процесів, загальних процесів (наприклад, фінансово-господарської діяльності або окремих її аспектів) (*оцінка відповідності*));
* результати оцінки ризиків, пов’язаних з відповідним об’єктом аудиту, застосовані фактори відбору для здійснення планових внутрішніх аудитів, визначені ступінь пріоритету та частота здійснення внутрішніх аудитів для кожного об’єкта аудиту (приклад ідентифікації й оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту наведено у [***додатку 2***](#_Додаток_8._Приклад));
* назви структурних підрозділів апарату державного органу, у яких можуть здійснюватися внутрішні аудити підрозділом внутрішнього аудиту державного органу;
* назву територіальних органів державного органу, а також підприємств, установ та організацій, що належать до сфери управління державного органу, у яких можуть здійснюватися внутрішні аудити підрозділом внутрішнього аудиту державного органу. Включається інформація, за наявністю, у державного органу – територіальних органів та підпорядкованих підприємств / установ / організацій;
* назву структурних підрозділів територіального органу та бюджетної установи, у яких можуть здійснюватися внутрішні аудити підрозділом внутрішнього аудиту територіального органу та бюджетної установи. Включається інформація, якщо ведеться зведена база даних щодо простору аудиту;
* назву підрозділу внутрішнього аудиту державного органу та, якщо ведеться зведена база даних щодо простору аудиту, включається інформація щодо підрозділів внутрішнього аудиту територіальних органів та бюджетних установ;
* відомості щодо здійснення внутрішніх аудитів (тема, за якою здійснено внутрішній аудит, коротка інформація щодо виявлених проблем та недоліків, дата здійснення внутрішнього аудиту та період, за який він здійснювався, назва структурного підрозділу державного органу, територіальних органів державного органу та підприємств, установ та організацій, які належать до сфери його управління, де здійснювався внутрішній аудит, стан реагування на аудиторські висновки та рекомендації);
* відомості щодо проведення контрольних заходів (ревізій, перевірок, державних фінансових аудитів тощо) зовнішніми контролюючими органами (Рахунковою палатою, органами державного фінансового контролю тощо) у системі державного органу (тема контрольного заходу, коротка інформація щодо виявлених проблем, порушень та недоліків, дата проведення контрольного заходу та період, за який він проводився, назва структурного підрозділу державного органу, територіального органу державного органу, підприємства, установи та організації, які належать до сфери його управління, де проводились контрольні заходи, інформація про стан виконання обов’язкових вимог/реагування на аудиторські висновки та рекомендації).

Головна таблиця «Інформація про об’єкти простору внутрішнього аудиту» за потреби може додатково містити іншу інформацію з урахуванням специфіки діяльності відповідного державного органу.

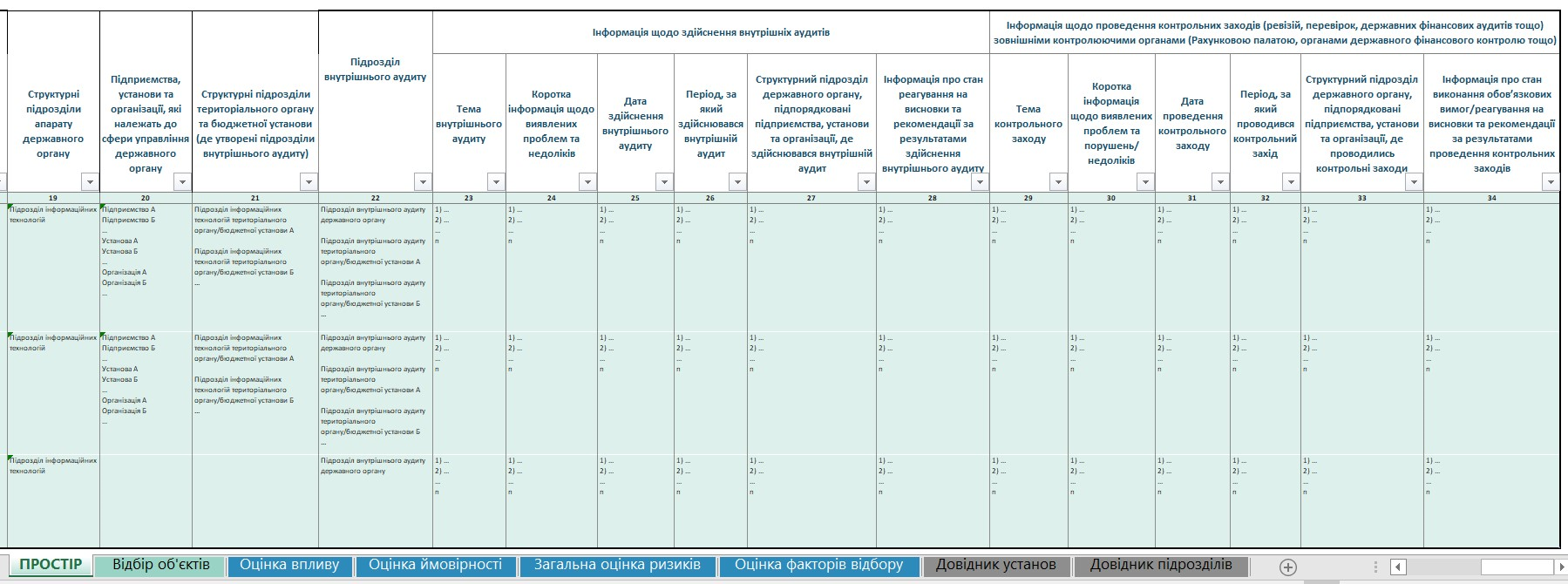
На підставі інформації, що міститься у головній таблиці, здійснюється включення даних до звітності ф. № 1-ДВА, зокрема, щодо кількості об’єктів аудиту, структурних підрозділів апарату державного органу, територіальних органів та бюджетних установ, а також кількості територіальних органів, підприємств, установ та організацій, які належать до сфери управління державного органу.

Зокрема, з колонки 2 головної таблиці включаються дані щодо кількості об’єктів аудиту до відповідних граф рядка 6100 глави 1 розділу І Звіту ф. № 1-ДВА, а з колонок 19 та 21 включаються дані щодо кількості структурних підрозділів апарату державного органу, структурних підрозділів територіальних органів та бюджетних установ, з колонки 20 – щодо кількості територіальних органів державного органу, підприємств, установ та організацій, які належать до сфери управління державного органу – до відповідних граф рядка 6200 глави 1 розділу І Звіту ф. 1-ДВА.

Роз’яснення щодо підходів та алгоритму заповнення рядків 6100 та 6200 глави 1 розділу І Звіту ф. 1-ДВА надано Мінфіном листом від 18.05.2023 № 33030-07-5/13645.



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



***Рис. 2. Продовження головної таблиці «Інформація про об’єкти простору внутрішнього аудиту» бази даних щодо простору аудиту   
(колонки 19 – 34)***

|  |  |
| --- | --- |
| ***Рис. 3. Приклад визначення у зведеній базі даних об’єктів аудиту у розрізі підрозділу внутрішнього аудиту апарату державного органу та підрозділів внутрішнього аудиту територіальних органів та бюджетних установ*** | Під час формування зведеної бази даних у головній таблиці зазначаються об’єкти аудиту (колонка 2) у розрізі підрозділу внутрішнього аудиту державного органу та підрозділів внутрішнього аудиту територіальних органів та бюджетних установ (колонка 22) (рис. 3).  Наприклад, процес «захист інформації в інформаційних системах (ІТ-безпека)» реалізується ІТ-підрозділами як апарату державного органу, так і територіальних органів та бюджетних установ, а також окремими підприємствами, установами та організаціями, де також забезпечується захист інформації.  У разі утворення у територіальних органах та бюджетних установах підрозділів внутрішнього аудиту, зазначений об’єкт аудиту доцільно включати для дослідження також зазначеними підрозділами внутрішнього аудиту.  Під час формування зведеної бази даних щодо простору аудиту слід застосовувати єдині підходи, зокрема, до формулювання назви об’єктів аудиту та ідентифікованих ризиків, що допомагає при формуванні зведеного плану діяльності з внутрішнього аудиту. |

Наприклад, якщо у базі даних територіального органу А зазначено об’єкт аудиту – «захист інформації», територіального органу Б – «безпека інформації», а підрозділом внутрішнього аудиту державного органу сформульовано назву об’єкта аудиту як «захист інформації в інформаційних системах (ІТ-безпека)», то назва «захист інформації в інформаційних системах (ІТ-безпека)» буде назвою об’єкта аудиту та має міститися у зведеній базі даних у розрізі усіх підрозділів внутрішнього аудиту, що функціонують у системі державного органу.

Також визначені у базі даних щодо простору аудиту назви об’єктів аудиту мають співпадати з назвами об’єктів аудиту, визначених у результатах ідентифікації й оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту, а також з назвами об’єктів аудиту, які включалися до планів (зведених планів) діяльності з внутрішнього аудиту за результатами оцінки ризиків.

Для заповнення головної таблиці «Інформація про об’єкти простору внутрішнього аудиту» використовуються допоміжні таблиці, які розміщуються на окремих аркушах книги Excel, які містять інформацію за кожним об’єктом аудиту щодо результатів:

* проведеної ідентифікації та оцінки ризиків (включає оцінку ризиків за критеріями впливу / критеріями ймовірності, загальну оцінку ризиків за впливом та ймовірністю);
* здійсненого ризик-орієнтованого відбору об’єктів аудиту (включає оцінку кожного фактору відбору за допомогою бальних оцінок та вагових коефіцієнтів, визначених ступеня пріоритету об'єктів аудиту та частоти здійснення планових внутрішніх аудитів щодо кожного пріоритетного об’єкту аудиту).

У відповідних допоміжних таблицях документуються результати проведення ідентифікації й оцінки ризиків та здійснення ризик-орієнтованого відбору об’єктів аудиту, зокрема:

оцінки ризиків за визначеними критеріями впливу – у таблиці «Оцінка впливу»;

оцінки ризиків за визначеними критеріями ймовірності – у таблиці «Оцінка ймовірності»;

загальної оцінки ризиків за впливом та ймовірністю – у таблиці «Загальна оцінка ризиків»;

оцінки кожного фактору відбору за допомогою визначених критеріїв з використанням бальних оцінок та вагових коефіцієнтів – у таблиці «Оцінка факторів відбору»;

визначення ступеня пріоритету об’єкта аудиту та частоти здійснення планових внутрішніх аудитів щодо кожного об’єкта аудиту за допомогою розрахованого індексу пріоритетності – у таблиці «Ризик-орієнтований відбір об’єктів внутрішнього аудиту…».

У кожній з цих допоміжних таблиць розміщено дані, які використовуються під час проведення відповідних процедур. Наприклад, у таблиці «Оцінки впливу» міститься перелік критеріїв впливу та шкала оцінювання ризиків за впливом (рис. 4), у таблиці «Оцінка ймовірності» – перелік критеріїв ймовірності та шкала оцінювання ризиків за ймовірністю (рис. 5), у таблиці «Загальна оцінка ризиків» – матриця оцінки ризиків (рис. 6), у таблиці «Оцінка факторів відбору» – набір критеріїв щодо оцінки кожного фактору відбору з відповідними бальними оцінками та прикладами значень вагових коефіцієнтів (рис. 7), у таблиці «Ризик-орієнтований відбір об’єктів внутрішнього аудиту…» – формула, за якою розраховується індекс пріоритетності (передбачено також автоматичний розрахунок індексу пріоритетності у колонці «Індекс пріоритетності (Ip)»), приклади значень розрахованого індексу пріоритетності для визначення ступеня пріоритету об’єкта аудиту (з оцінкою від «дуже високого» до «низького»), приклад визначення частоти здійснення планових внутрішніх аудитів щодо кожного об’єкта аудиту в залежності від визначеного ступеня пріоритету об’єкта аудиту (рис. 8).

|  |
| --- |
|  |
| ***Рис. 4. Приклад ідентифікації та оцінки ризиків (оцінка ризиків за впливом)*** |
|  |
| ***Рис. 5. Приклад ідентифікації та оцінки ризиків (оцінка ризиків за ймовірністю)*** |
|  |
| ***Рис. 6. Приклад ідентифікації та оцінки ризиків (загальна оцінка ризиків за впливом та ймовірністю)*** |
|  |
| ***Рис. 7. Приклад ризик-орієнтованого відбору об’єктів аудиту (оцінка факторів відбору за допомогою визначених критеріїв, бальних оцінок та вагових коефіцієнтів)*** |
|  |
| ***Рис. 8. Приклад ризик-орієнтованого відбору об’єктів аудиту (розрахунок індексу пріоритетності для визначення ступеня пріоритету об’єкта аудиту та частоти здійснення внутрішніх аудитів щодо кожного об’єкта аудиту)*** |

Допоміжні таблиці можуть містити довідники, наприклад:

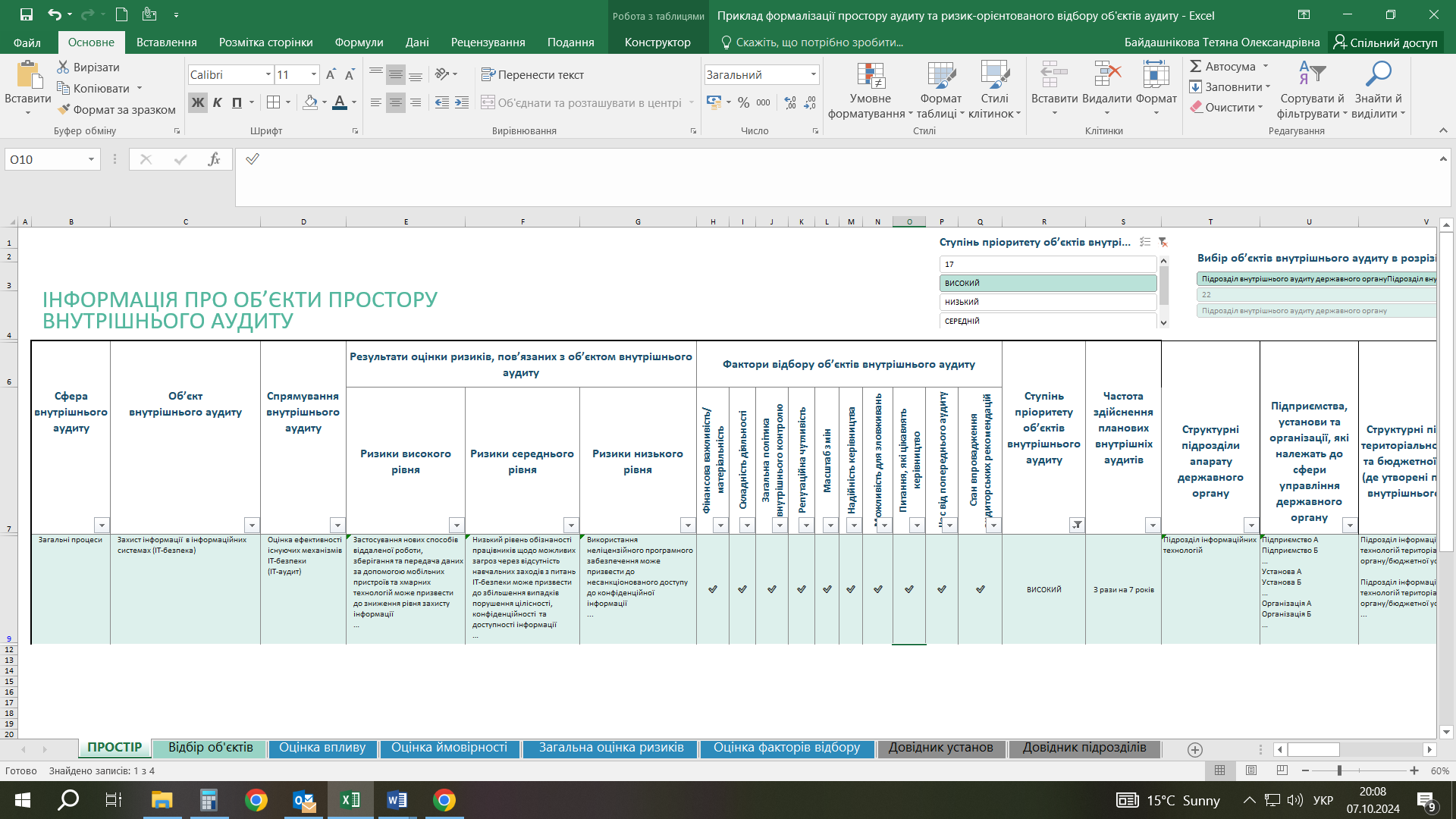
* підприємств, установ та організацій, які належать до сфери управління державного органу, їх місцезнаходження, коду ЄДРПОУ, контактні дані відповідальних за діяльність осіб, інших посадових осіб (рис. 9);
* структурних підрозділів державного органу, прізвища, ім’я, по-батькові керівника підрозділу, його контактні дані (електронну адресу тощо) (рис. 10). Під час формування зведеної бази даних щодо простору аудиту до довідників включається інформація, зокрема, щодо структурних підрозділів територіального органу та бюджетної установи.

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | |
| **Рис. 9. Приклад ведення довідника підприємств, установ та організацій, які належать до сфери управління державного органу** | | **Рис. 10. Приклад ведення довідника структурних підрозділів державного органу** | |
| ***Рис. 11. Приклад вибору ризику з розкривного списку*** | | | Дані до головної таблиці заносяться за допомогою розкривних списків або гіперпосилань (в залежності від обсягу), зокрема, за допомогою розкривного списку можна вибрати з переліку ризиків потрібний ризик (рис. 11).  Аналогічно за допомогою розкривних списків вибираються структурні підрозділи державного органу або підприємства, установи та організації, а саме: на рис. 12 зображено вибір необхідного структурного підрозділу, відповідального за процес, що охоплюватиметься внутрішнім аудитом, а на рис. 13 – державного підприємства, яке реалізує обраний для дослідження процес. |
|  |  | | |
| ***Рис. 12. Приклад застосування довідника при виборі структурного підрозділу державного органу*** | ***Рис. 13. Приклад застосування довідника при виборі підприємства*** | | |

У таблицях інформація може відображатися за допомогою фільтрування даних, що дозволяє швидко вибрати необхідні дані.

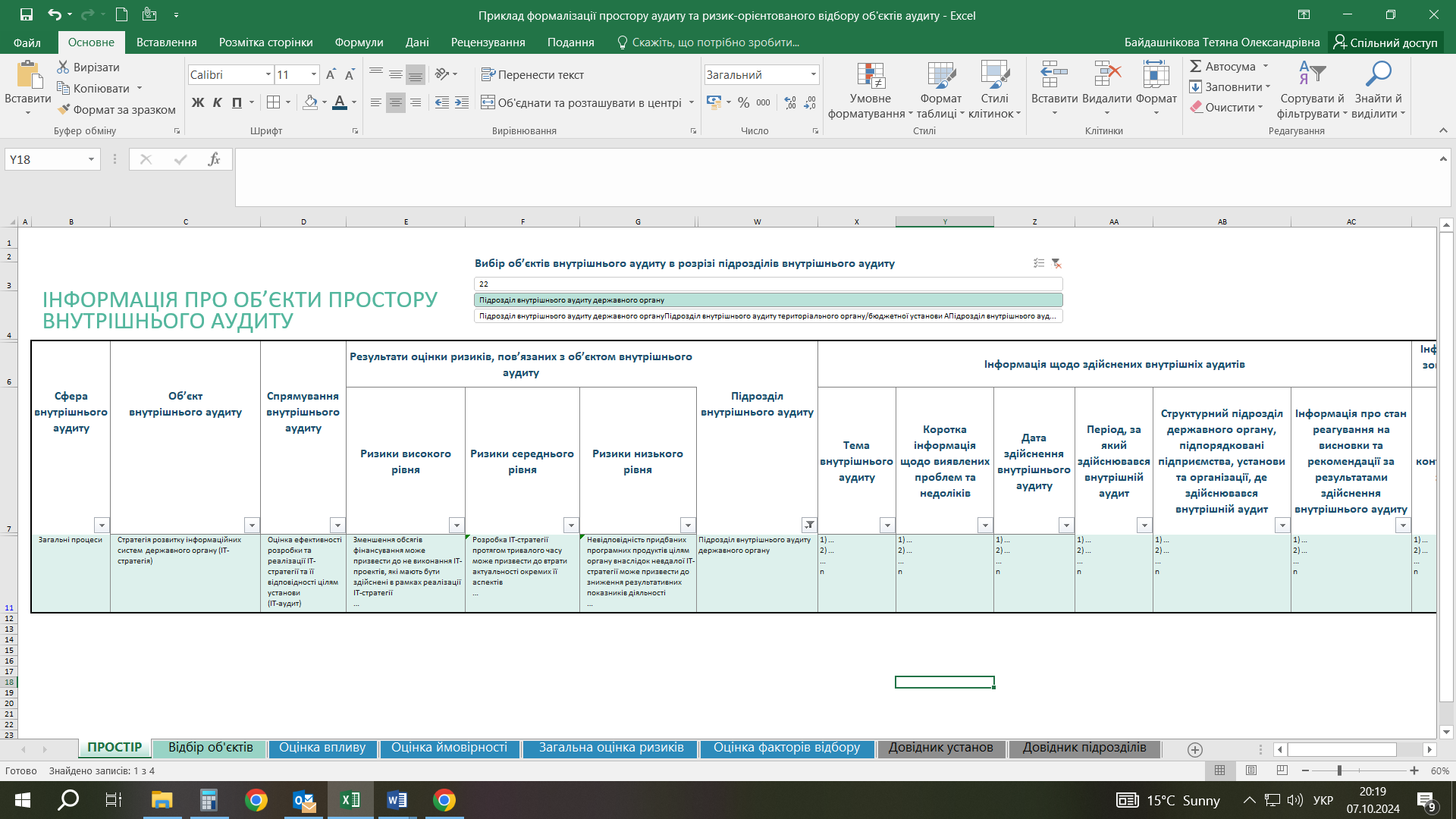
На рис. 14 представлено, як за допомогою кнопки «високий» можна відібрати всі об’єкти аудиту з високим ступенем пріоритету (для прикладу застосовано один об’єкт аудиту для визначеного ступеня пріоритету).

Аналогічно можна фільтрувати дані, зокрема, за сферами внутрішнього аудиту (наприклад, виокремити лише загальні процеси), за рівнями ризиків (наприклад, відібрати ризики лише високого рівня тощо).



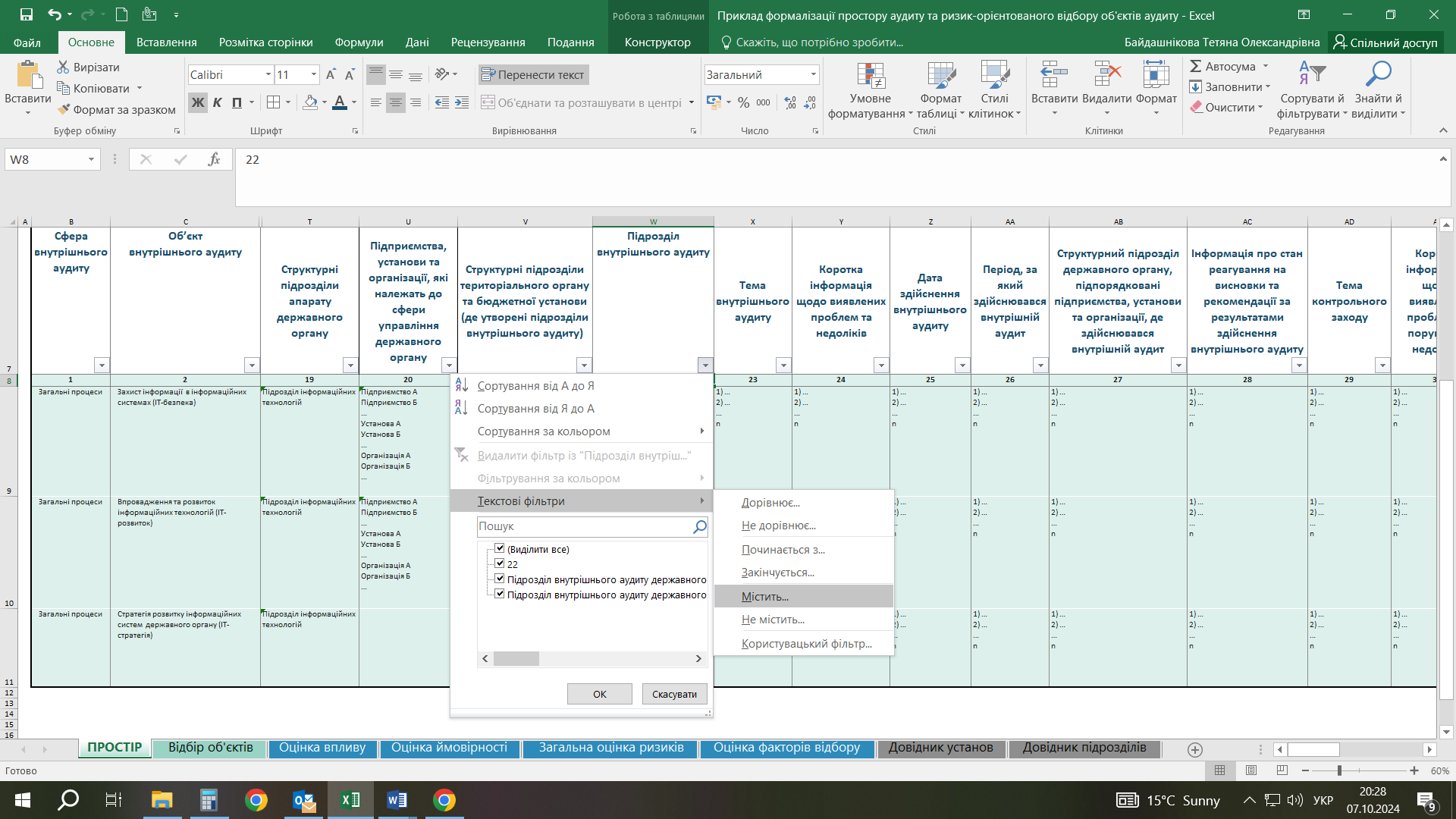
**Рис. 14. Приклад фільтрування об’єктів аудиту за ступенем пріоритету**

Функція вибору даних за допомогою фільтрів використовується також при роботі із зведеною базою даних (рис. 15 – 16), зокрема, при виборі підрозділу внутрішнього аудиту. При цьому у таблиці відображаються об’єкти аудиту, які можуть охоплюватися підрозділом внутрішнього аудиту державного органу або підрозділами внутрішнього аудиту територіального органу та бюджетної установи. Зокрема, на рис. 15 зображено відбір об’єктів аудиту, які можуть охоплюватися підрозділом внутрішнього аудиту державного органу.



***Рис. 15. Приклад фільтрування об’єктів аудиту в розрізі відповідних підрозділів внутрішнього аудиту***

Аналогічно можна фільтрувати дані за допомогою кнопок, розташованих у заголовку таблиці, що дозволяє задати умови фільтрування для відображення об’єктів аудиту відповідного підрозділу внутрішнього аудиту (рис. 16).



***Рис. 16. Приклад іншого способу фільтрування об’єктів аудиту в розрізі відповідних підрозділів внутрішнього аудиту***

## [**Додаток 2. Приклад поетапної процедури проведення та документування результатів ідентифікації й оцінки ризиків та ризик-орієнтованого відбору об’єктів аудиту**](#_Додаток_2._Приклад_2)

Ідентифікацію й оцінку ризиків та ризик-орієнтований відбір об’єктів аудиту (за визначеними у посібнику підходами) здійснено на прикладі об’єктів аудиту та ризиків наведених у [***додатку 1***](#_Додаток_1._Приклад).

**Ідентифікація ризиків, пов’язаних з об’єктами аудиту**

Після визначення у просторі аудиту об’єктів аудиту проводиться ідентифікація ризиків, пов’язаних з відповідним об'єктом аудиту. На прикладі за кожним об’єктом аудиту ідентифіковано три ризика, які сформульовані у причинно-наслідковому зв’язку:

|  |  |  |  |
| --- | --- | --- | --- |
| **Сфера внутрішнього аудиту** | **Об’єкт внутрішнього аудиту** | **№ з/п** | **Назва ризику** |
| ***Загальні процеси*** | **Захист інформації в інформаційних системах (ІТ-безпека)** | 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 |
| ***Загальні процеси*** | **Впровадження та розвиток інформаційних технологій (ІТ-розвиток)** | 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 |
| ***Загальні процеси*** | **Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)** | 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 |

**Оцінка ідентифікованих ризиків, пов’язаних з об’єктами аудиту**

Після ідентифікації ризиків, пов’язаних з об’єктами аудиту, проводиться оцінка ризиків, яка включає такі послідовні етапи:

оцінка ризиків за впливом відповідно до визначених критеріїв та шкали оцінювання ризиків за впливом (оцінка впливу);

оцінка ризиків за ймовірністю відповідно до визначених критеріїв та шкали оцінювання ризиків за ймовірністю (оцінка ймовірності);

загальна оцінка ризиків відповідно до проведених оцінок ризиків за впливом / ймовірністю (загальна оцінка за впливом / ймовірністю).

Оцінка ідентифікованих ризиків проведена на прикладі критеріїв та шкали оцінювання ризиків за впливом / ймовірністю, наведених у розділі 3 «Оцінка ризиків за впливом та ймовірністю» посібника:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | Рівень (бал) | Критерії впливу | | | | | **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 напрямами 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 критичних збоїв у роботі цього підрозділу | Критичне зниження/втрата спроможностей може заважати продовженню виконання завдань та функцій за двома і більше напрямами 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 напрямами 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 | | |  |  | | --- | --- | | Рівень (бал) | Критерії ймовірності | | Рідко/майже не можливо (1) | Ймовірність виникнення ризику дуже низька (з вірогідністю 0-24 %) | | Малоймовірно (2) | Ймовірність виникнення ризику віддалена (з вірогідністю 25-50 %) | | Можливо (3) | Ймовірність виникнення ризику впродовж 1-2 років (з вірогідністю 51-74 %) | | Часто/очікується (4) | Ризик існує або очікується (з вірогідністю 75-100 %) | |

*Оцінка впливу*

За кожним ідентифікованим ризиком здійснюється оцінка за впливом на виконання державним органом завдань і функцій та досягнення цілей діяльності, визначених у стратегічних та річних планах. Оцінка ризика за впливом проводиться за фінансовим, кадровим, операційним та репутаційним критеріями впливу для визначення рівня впливу («низького», «середнього», «високого» або «дуже високого») та присвоєння ризику відповідного балу (1, 2, 3 або 4).

Наприклад, ризик *«невідповідність придбаних програмних продуктів цілям державного органу внаслідок невдалої ІТ-стратегії може призвести до зниження результативних показників діяльності»* оцінено як такий, що має «*середній*» рівень впливу (присвоєно ризику бал – 2):

= 2,25 (≈2).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| **Загальні процеси** | **Захист 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 напрямами діяльності. Суттєва втрата спроможностей. Повільне відновлення у роботі (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 = 4) | **дуже високий** |
| **Загальні процеси** | **Захист інформації в інформаційних системах (ІТ-безпека)** | 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 напрямами діяльності. Суттєва втрата спроможностей. Повільне відновлення у роботі (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 =  3,66 ( ≈ 4)) | **дуже високий** |
| **Загальні процеси** | **Захист інформації в інформаційних системах (ІТ-безпека)** | 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 суттєвих збоїв у роботі цього підрозділу (2) | Відсутність можливості продовжувати звично виконувати завдання та функції. Повсюдний збій за всіма напрямами діяльності. Суттєва втрата спроможностей.  Повільне відновлення у роботі (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 = 3,5 ( ≈ 4)) | **дуже високий** |
| **Загальні процеси** | **Впровадження та розвиток інформаційних технологій (ІТ-розвиток)** | 4 | Відсутність моніторингу розподілу та використання ІТ-ресурсів може призвести до неефективного їх використання | Фінансово-матеріальний вплив вище 100 тис. грн, але нижче 500 тис. грн (2) | Незапланована відсутність (хвороба тощо) деяких ключових працівників у одному підрозділі може призвести до затримки у роботі цього підрозділу (1) | Суттєве зниження/втрата спроможностей може заважати продовженню виконання завдань та функцій за одним/декількома напрямами діяльності. Швидке відновлення у роботі (2) | 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 (2) | **2** ((2 + 1 + 2 + 2) / 4 = 1,75 ( ≈ 2)) | **середній** |
| **Загальні процеси** | **Впровадження та розвиток інформаційних технологій (ІТ-розвиток)** | 5 | Неналежний контроль за виконанням ІТ-процесів та процедур може знизити ефективність роботи ІТ-підрозділу | Фінансово-матеріальний вплив вище 500 тис. грн, але нижче 1 млн грн (3) | Незапланована відсутність (хвороба тощо) деяких ключових працівників у одному підрозділі може призвести до суттєвих збоїв у роботі цього підрозділу (2) | Критичне зниження/втрата спроможностей може заважати продовженню виконання завдань та функцій за двома і більше напрямами діяльності. Повільне відновлення у роботі (3) | 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) | **3** ((3 + 2 + 3 + 3) / 4= 2,75 ( ≈ 3)) | **високий** |
| **Загальні процеси** | **Впровадження та розвиток інформаційних технологій (ІТ-розвиток)** | 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 | Значний фінансово-матеріальний вплив вище 1 млн грн (4) | Незапланована відсутність (хвороба тощо) більшості ключових працівників у одному підрозділі може призвести до критичних збоїв у роботі цього підрозділу (3) | Відсутність можливості продовжувати звично виконувати завдання та функції. Повсюдний збій за всіма напрямами діяльності. Суттєва втрата спроможностей.  Повільне відновлення у роботі (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 + 3 + 4 + 3) / 4 = 3,5 ( ≈ 4)) | **дуже високий** |
| **Загальні процеси** | **Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)** | 7 | Розробка ІТ-стратегії протягом тривалого часу може призвести до втрати актуальності окремих її аспектів | Фінансово-матеріальний вплив вище 500 тис. грн, але нижче 1 млн грн (3) | Незапланована відсутність (хвороба тощо) деяких ключових працівників у одному підрозділі може призвести до затримки у роботі цього підрозділу (1) | Критичне зниження/втрата спроможностей може заважати продовженню виконання завдань та функцій за двома і більше напрямами діяльності. Повільне відновлення у роботі (3) | 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) | **3** ((3 + 1 + 3 + 4) / 4 = 2,75 ( ≈ 3)) | **високий** |
| **Загальні процеси** | **Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)** | 8 | Невідповідність придбаних програмних продуктів цілям органу внаслідок невдалої ІТ-стратегії може призвести до зниження результативних показників діяльності | Фінансово-матеріальний вплив вище 100 тис. грн, але нижче 500 тис. грн (2) | Незапланована відсутність (хвороба тощо) деяких ключових працівників у одному підрозділі може призвести до суттєвих збоїв у роботі цього підрозділу (2) | Суттєве зниження/втрата спроможностей може заважати продовженню виконання завдань та функцій за одним/декількома напрямами діяльності. Швидке відновлення у роботі (2) | 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) | **2** ((2 + 2 + 2 + 3) / 4 = 2,25 ( ≈ 2)) | **середній** |
| **Загальні процеси** | **Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)** | 9 | Зменшення обсягів фінансування може призвести до не виконання ІТ-проектів, які мають бути здійснені в рамках реалізації ІТ-стратегії | Фінансово-матеріальний вплив вище 500 тис. грн, але нижче 1 млн грн (3) | не застосовується | Відсутність можливості продовжувати звично виконувати завдання та функції. Повсюдний збій за всіма напрямами діяльності. Суттєва втрата спроможностей.  Повільне відновлення у роботі (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) | **3** ((3 + 4 + 3) / 3 =  3,33 ( ≈ 3)) | **високий** |

*Оцінка ймовірності*

За кожним ідентифікованим ризиком здійснюється оцінка ймовірності настання ризика. Оцінка ризика за ймовірністю проводиться за критеріями ймовірності («ймовірність виникнення ризику низька (з вірогідністю від 0 до 24 %)», «ймовірність виникнення ризику віддалена (з вірогідністю від 25 до 50 %)», «ймовірність виникнення ризику впродовж 1-2 років (з вірогідністю від 51 до 74 %)», «ризик існує або очікується (з вірогідністю від 75 до 100 %)») для визначення рівня ймовірності («рідко/майже не можливо», «малоймовірно», «можливо» або «часто/очікується») та присвоєння ризику відповідного балу (1, 2, 3 або 4).

Наприклад, ризик *«невідповідність придбаних програмних продуктів цілям державного органу внаслідок невдалої ІТ-стратегії може призвести до зниження результативних показників діяльності»* оцінено за рівнем ймовірності його настання – «*малоймовірно*» (ймовірність виникнення ризику віддалена – з вірогідністю 25-50 %). Присвоєно ризику бал – 2.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Сфера внутрішнього аудиту** | **Об’єкт внутрішнього аудиту** | **№ з/п** | **Назва ризику** | **Ймовірність виникнення ризику дуже низька (з вірогідністю 0-24 %) (бал)** | **Ймовірність виникнення ризику віддалена  (з вірогідністю 25-50 %) (бал)** | **Ймовірність виникнення ризику впродовж 1-2 років (з вірогідністю 51-74 %) (бал)** | **Ризик існує або очікується (з вірогідністю 75-100 %) (бал)** | **Рівень ймовірності** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
| **Загальні процеси** | **Захист інформації в інформаційних системах (ІТ-безпека)** | 1 | Використання неліцензійного програмного забезпечення може призвести до несанкціонованого доступу до конфіденційної інформації | **1** |  |  |  | **рідко/майже не можливо** |
| **Загальні процеси** | **Захист інформації в інформаційних системах (ІТ-безпека)** | 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** |
| **Загальні процеси** | **Захист інформації в інформаційних системах (ІТ-безпека)** | 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** |
| **Загальні процеси** | **Впровадження та розвиток інформаційних технологій (ІТ-розвиток)** | 4 | Відсутність моніторингу розподілу та використання ІТ-ресурсів може призвести до неефективного їх використання |  | **2** |  |  | **малоймовірно** |
| **Загальні процеси** | **Впровадження та розвиток інформаційних технологій (ІТ-розвиток)** | 5 | Неналежний контроль за виконанням ІТ-процесів та процедур може знизити ефективність роботи ІТ-підрозділу |  |  | **3** |  | **можливо** |
| **Загальні процеси** | **Впровадження та розвиток інформаційних технологій (ІТ-розвиток)** | 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** |
| **Загальні процеси** | **Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)** | 7 | Розробка ІТ-стратегії протягом тривалого часу може призвести до втрати актуальності окремих її аспектів |  |  | **3** |  | **можливо** |
| **Загальні процеси** | **Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)** | 8 | Невідповідність придбаних програмних продуктів цілям органу внаслідок невдалої ІТ-стратегії може призвести до зниження результативних показників діяльності |  | **2** |  |  | **малоймовірно** |
| **Загальні процеси** | **Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)** | 9 | Зменшення обсягів фінансування може призвести до не виконання ІТ-проектів, які мають бути здійснені в рамках реалізації ІТ-стратегії |  |  |  | **4** | **часто/ очікується** |

*Загальна оцінка за впливом та ймовірністю*

За кожним ідентифікованим ризиком визначається рівень ризику (бал) на підставі проведених оцінок впливу та ймовірності.

Наприклад, за результатами оцінки ризика *«невідповідність придбаних програмних продуктів цілям державного органу внаслідок невдалої ІТ-стратегії може призвести до зниження результативних показників діяльності»* за впливом та ймовірністю визначено рівень ризика «*середній*»:

**2** (*оцінка впливу*) **х** **2** (*оцінка ймовірності*) = **4**.

Загальна оцінка ризиків, пов’язаних з відповідним об’єктом аудиту, проводиться шляхом визначення загального рівня (загального балу) ризиків на підставі проведених оцінок за впливом та ймовірністю за кожним ідентифікованим ризиком.

Наприклад, загальний рівень (загальний бал) за результатами проведеної загальної оцінки ризиків, пов’язаних з об’єктом аудиту *«стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)»*, становить «*високий*»:

= 8,33 ( ≈ 8).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Сфера внутрішнього аудиту** | **Об’єкт внутрішнього аудиту** | **№**  **з/п** | **Назва ризику** | **Оцінка**  **впливу (бал)** | **Оцінка**  **ймовірності (бал)** | **Оцінка ризику за впливом та ймовірністю** | | **Загальна оцінка ризиків за впливом та ймовірністю** | |
| **Бал** | **Рівень** | **Бал** | **Рівень** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| **Загальні процеси** | **Захист інформації в інформаційних системах (ІТ-безпека)** | 1 | Використання неліцензійного програмного забезпечення може призвести до несанкціонованого доступу до конфіденційної інформації | **4** | **1** | 4  (4 х 1 = 4) | середній | **8**  ((4 + 12 + 8) / 3 = 8) | **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 | **4** | **3** | 12  (4 х 3 = 12) | 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 | **4** | **2** | 8  (4 х 2 = 8) | високий |
| **Загальні процеси** | **Впровадження та розвиток інформаційних технологій (ІТ-розвиток)** | 4 | Відсутність моніторингу розподілу та використання ІТ-ресурсів може призвести до неефективного їх використання | **2** | **2** | 4  (2 х 2 = 4) | середній | **8**  ((4 + 9 + 12) / 3 =  8,33 ( ≈ 8)) | **високий** |
| 5 | Неналежний контроль за виконанням ІТ-процесів та процедур може знизити ефективність роботи ІТ-підрозділу | **3** | **3** | 9  (3 х 3 = 9) | 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 | **4** | **3** | 12  (4 х 3 = 12) | дуже високий |
| **Загальні процеси** | **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 х 3 = 9) | високий | **8** ((9 + 4 + 12) / 3 =  8,33 ( ≈ 8)) | **високий** |
| 8 | Невідповідність придбаних програмних продуктів цілям органу внаслідок невдалої ІТ-стратегії може призвести до зниження результативних показників діяльності | **2** | **2** | 4  (2 х 2 = 4) | середній |
| 9 | Зменшення обсягів фінансування може призвести до не виконання ІТ-проектів, які мають бути здійснені в рамках реалізації ІТ-стратегії | **3** | **4** | 12  (3 х 4 = 12) | дуже високий |

Загальний рівень (загальний бал) за результатами проведеної загальної оцінки ризиків, пов’язаних з об’єктом аудиту *«стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)»* визначено на прикладі «Матриці оцінки ризиків», наведеної у розділі 3 «Оцінка ризиків за впливом та ймовірністю» посібника:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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) |

Водночас, якщо за результатами проведення загальної оцінки ризиків виявиться, що всі ризики або переважну їх більшість, оцінено як «дуже високі», «високі», «середні» чи «низькі», то слід враховувати, що на остаточний результат відбору об’єктів аудиту більше впливають фактори відбору, що далі на прикладі буде проілюстровано.

Результати загальної оцінки ризиків, пов’язаної з відповідним об’єктом аудиту, враховуються під час здійснення ризик-орієнтованого відбору об’єктів аудиту з метою включення до плану діяльності з внутрішнього аудиту.

**Ризик-орієнтований відбір об’єктів аудиту**

Ризик-орієнтований відбір об’єктів аудиту включає такі послідовні етапи:

визначення набору фінансових / нефінансових факторів відбору для проведення планових внутрішніх аудитів та показників вагомості факторів відбору;

визначення критеріїв для оцінки кожного фактору відбору за допомогою бальних оцінок та вагових коефіцієнтів;

розрахунок індексу пріоритетності для визначення ступеню пріоритету об’єктів аудиту та частоти здійснення планових внутрішніх аудитів щодо кожного об’єкта аудиту.

*Визначення набору фінансових / нефінансових факторів відбору для проведення планових внутрішніх аудитів та показників вагомості факторів відбору*

Для обраних для прикладу об’єктів аудиту застосовано набір фінансових / нефінансових факторів відбору, наведених у розділі 4 «Визначення об’єктів аудиту за допомогою факторів відбору» посібника:

|  |  |  |
| --- | --- | --- |
| **Сфера внутрішнього аудиту: загальні процеси.** | | |
| **Об’єкти аудиту: забезпечення захисту інформації в інформаційних системах (ІТ-безпека);**  **впровадження та розвиток інформаційних технологій (ІТ-розвиток);**  **стратегія розвитку інформаційних систем державного органу (ІТ-стратегія)** | | |
| **Фактор відбору**  **(а-j)** | | **Показник вагомості**  **(Wa-Wj)** |
| 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 |

Під час відбору застосовано однаковий набір факторів відбору за кожним об’єктом аудитом аудиту. З метою підкреслення важливості відповідного фактору відбору застосовано показники вагомості. Наприклад, найвищі значення отримали фактори відбору – «*питання, які цікавлять керівництво*» (5) та «*можливість для зловживань*» (4), найнижчий показник вагомості отримав фактор відбору – «*стан впровадження аудиторських рекомендацій*» (1).

*Визначення критеріїв для оцінки кожного фактору відбору за допомогою бальних оцінок та вагових коефіцієнтів*

Для оцінки кожного фактору відбору використано критерії та бальні оцінки, наведені у розділі 4 «Визначення об’єктів аудиту за допомогою факторів відбору» посібника:

|  |  |  |  |
| --- | --- | --- | --- |
| **Фактор відбору**  **(а-j)** | **Критерії** | | **Бал**  **(Р)** |
| а. Фінансова важливість/ матеріальність | На об’єкт аудиту (програму, систему, ресурси тощо) припадає | менше 10 % річного бюджету | 1 |
| 11 – 50 % річного бюджету | 2 |
| 51 – 80 % річного бюджету | 3 |
| не менше 81 % річного бюджету | 4 |
| b. Складність діяльності | Виконання функції (процесу) суттєво не впливає на досягнення мети та цілей діяльності установи; реалізація функції (процесу) передбачає невелику кількість процедур та задіяного персоналу | | 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 |
| Виконання функції (процесу) впливає на досягнення мети та цілей діяльності установи; реалізація функції (процесу) передбачає велику кількість процедур та задіяного персоналу | | 3 |
| Виконання функції (процесу) відіграє ключову роль у досягненні мети та цілей діяльності установи; реалізація функції (процесу) передбачає найбільшу кількість процедур та задіяного персоналу | | 4 |
| c. Загальна політика внутрішнього контролю | Надійні системи внутрішнього контролю та управління ризиками | | 1 |
| Системи внутрішнього контролю та управління ризиками в цілому налагодженні та працюють, але мають окремі недоліки | | 2 |
| Системи внутрішнього контролю та управління ризиками є слабкими та ненадійними (перебуває на стадії становлення) | | 3 |
| Система внутрішнього контролю неефективна, має суттєві проблеми (розроблена формально та належно не функціонує, управління ризиками в установі не запроваджене) | | 4 |
| d. Репутаційна чутливість | Мінімальний зовнішній інтерес до функції (процесу) або його цілковита відсутність | | 1 |
| Можливість виникнення непорозумінь з громадськістю, пов’язаних з виконанням функції (процесу) | | 2 |
| Виникали поодинокі випадки непорозумінь з громадськістю, пов’язаних з виконанням функції (процесу) | | 3 |
| Підвищена увага з боку медіа до реалізації відповідної функції (процесу). Виникнення серйозних/системних проблем та/або втрата репутації установи за наявності таких проблем | | 4 |
| e. Масштаб змін | У законодавчих та нормативно-правових актах, які регулюють виконання відповідної функції (процесу), кадрових змінах, змінах у процедурах в рамках реалізації функції (процесу) тощо | за останній рік відбулося менше 10 % змін | 1 |
| за останній рік відбулося від 10 до 30 % змін | 2 |
| за останній рік відбулося від 30 до 50 % змін | 3 |
| за останній рік відбулося більше 50 % змін | 4 |
| f. Надійність керівництва | Вище керівництво установи та особи, відповідальні за реалізацію відповідної функції (процесу), мають досвід більше 3 років та практику успішної реалізації проектів/програм з відповідного напряму діяльності у державному секторі | | 1 |
| Вище керівництво установи та особи, відповідальні за реалізацію відповідної функції (процесу), мають досвід від 2 до 3 років та практику реалізації проектів/програм з відповідного напряму діяльності у державному секторі | | 2 |
| Вище керівництво установи та особи, відповідальні за реалізацію відповідної функції (процесу), мають досвід від 1 до 2 років з відповідного напряму діяльності у державному секторі | | 3 |
| Вище керівництво установи та особи, відповідальні за реалізацію відповідної функції (процесу), мають досвід менше 1 року з відповідного напряму діяльності у державному секторі | | 4 |
| g. Можливість для зловживань | Мінімальна можливість для виникнення фактів шахрайства та корупції | | 1 |
| Можливість виникнення зловживань, однак фактів шахрайства та корупції ще не виникало | | 2 |
| Існують поодинокі факти шахрайства та корупції | | 3 |
| Існують системні факти шахрайства та корупції | | 4 |
| h. Питання, які цікавлять керівництво | Невисока увага з боку вищого керівництва установи, існують поодинокі проблеми, які вийшли на рівень вищого керівництва у минулому | | 1 |
| Вище керівництво установи приділяє помірну увагу, наявність проблем, які вийшли на рівень вищого керівництва у минулому | | 2 |
| Висока увага з боку вищого керівництва установи, суттєві або повторювані проблеми, які вийшли на рівень вищого керівництва у минулому | | 3 |
| Постійна увага з боку вищого керівництва установи, існують суттєві повторювані проблеми, які вийшли на рівень вищого керівництва у недалекому минулому | | 4 |
| i. Час від попереднього аудиту | Проведено менше 1 року тому | | 1 |
| Проведено більше 1 року, але менше 5 років тому | | 2 |
| Проведено більше 5 років, але менше 7 років тому | | 3 |
| За останні 7 та більше років внутрішній аудит не проводився | | 4 |
| j. Стан впровадження аудиторських рекомендацій | Повністю виконано аудиторські рекомендації або внутрішній аудит не здійснювався | | 1 |
| Більшість аудиторських рекомендацій виконано, інформація про стан їх впровадження надається систематично/своєчасно та свідчить про прогрес у діяльності | | 2 |
| Частково виконано аудиторські рекомендації, інформація про стан їх впровадження надається несистематично/несвоєчасно та не свідчить про прогрес у діяльності | | 3 |
| Не виконано аудиторські рекомендації | | 4 |

На прикладі проілюстровано оцінку кожного фактору відбору за критеріями, які використовуються для визначення балу:



*Розрахунок індексу пріоритетності для визначення ступеню пріоритету об’єктів аудиту та частоти здійснення планових внутрішніх аудитів щодо кожного об’єкта аудиту*

Розрахунок індексу пріоритетності за кожним об’єктом аудиту здійснено за формулою, наведеною у розділі 4 «Визначення об’єктів аудиту за допомогою факторів відбору» посібника:

***Ip = Rа x*** *(),*

*де* ***Ip*** *– індекс пріоритетності;*

***Rа*** *– загальна оцінка ризику (за ймовірністю та впливом), присвоєна за кожним об’єктом аудиту;*

***Рa-Pj*** *– бал, присвоєний за відповідним фактором відбору;*

***Wa-Wj*** *– показник вагомості фактору відбору;*

***n*** *– загальна кількість застосованих факторів відбору.*

|  |  |
| --- | --- |
| ***Об’єкт аудиту*** | ***Розрахунок індексу пріоритетності*** |
| Захист інформації в інформаційних системах (ІТ-безпека) | *8 x ( =* ***67,2******(≈ 67)*** |
| Впровадження та розвиток інформаційних технологій (ІТ-розвиток) | *8 x ( =* ***45,6******(≈ 46)*** |
| Стратегія розвитку інформаційних систем державного органу (ІТ-стратегія) | *8 x ( =* ***35,2******(≈ 35)*** |

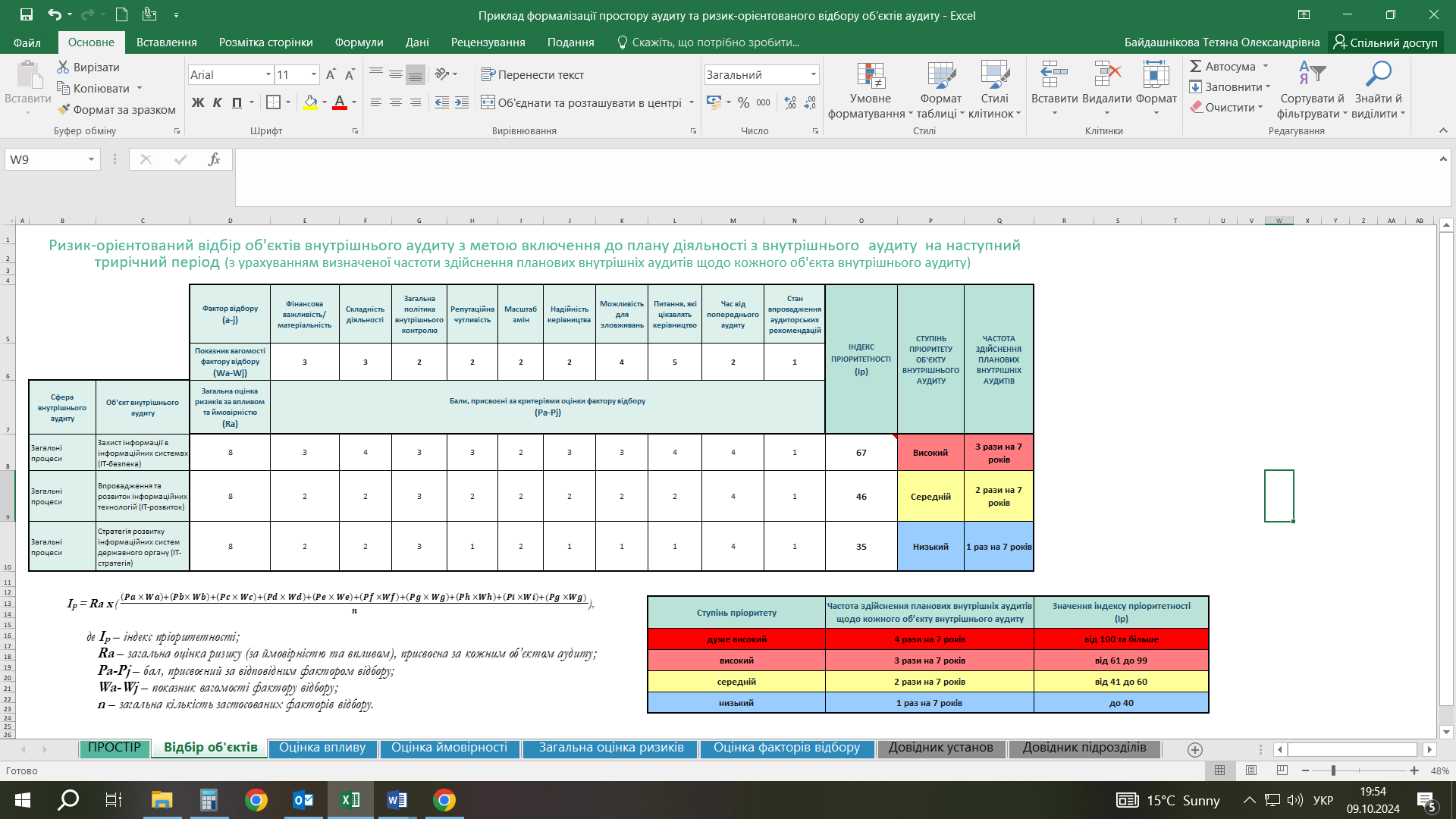
Визначені індекси пріоритетності використовується для визначення об'єктів аудиту з різним ступенем пріоритету:

|  |  |
| --- | --- |
| **Значення індексу пріоритетності (Ip)** | **Ступінь пріоритету** |
| від 100 та більше | дуже високий |
| від 61 до 99 | високий |
| від 41 до 60 | середній |
| до 40 | низький |

Частота здійснення планових внутрішніх аудитів щодо кожного об’єкта аудиту розраховується з урахуванням визначеного ступеню пріоритету об’єктів аудиту та індексу пріоритетності:

|  |  |  |
| --- | --- | --- |
| **Частота здійснення планових внутрішніх аудитів щодо кожного об’єкту аудиту** | **Ступінь пріоритету** | **Значення індексу пріоритетності (Ip)** |
| 4 рази на 7 років | дуже високий | від 100 та більше |
| 3 рази на 7 років | високий | від 61 до 99 |
| 2 рази на 7 років | середній | від 41 до 60 |
| 1 раз на 7 років | низький | до 40 |

Наприклад, щодо об’єкта аудиту – *захист інформації в інформаційних системах (ІТ-безпека)* присвоєно значення індексу пріоритетності – 67. Відповідне значення застосовується для визначення об’єкта аудиту з «високим» ступенем пріоритету. Частота дослідження такого об’єкта аудиту становить 3 рази на 7 років.



## [**Додаток 3.**](#_Додаток_3._Приклад) **Приклад розрахунку потреби у ресурсах для забезпечення виконання плану діяльності з внутрішнього аудиту**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Розрахунок потреби у 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. х 18 днів х 60 грн | 5400,00 |  |
| Квитки | 5 чол. х 800 грн х 6 разів | 24000,00 |  |
| Проживання у готелі | 1000 грн х 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 (підпис)*  *внутрішнього аудиту)*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(дата формування потреби)* | | | | | |

## 

1. *для визначення підходів до формулювання ризиків використано керівництво з управління ризиками «The Orange Book. Management of Risk – Principles and Concepts»* [↑](#footnote-ref-1)
2. *Детальніше щодо діяльності підрозділу внутрішнього аудиту з консультування можна ознайомитися за посиланням* [*https://www.mof.gov.ua/storage/files/Audit%20Presentation.pdf*](https://www.mof.gov.ua/storage/files/Audit%20Presentation.pdf) [↑](#footnote-ref-2)