ЗАГАЛЬНІ РЕЗУЛЬТАТИ ОПИТУВАННЯ КЕРІВНИКІВ ПІДРОЗДІЛІВ ВНУТРІШНЬОГО АУДИТУ ДЕРЖАВНИХ ОРГАНІВ ЩОДО ПРОВЕДЕННЯ ІТ АУДИТІВ ТА ВИКОРИСТАННЯ ІТ ІНСТРУМЕНТІВ ПРИ ЇХ ПРОВЕДЕННІ

Серпень 2024

ЗМІСТ

ВСТУП

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Інформаційні технології є важливим інструментом, який майже щодня використовується в різних напрямах діяльності. Технології пропонують нові переваги, але залежність від них також несе нові виклики, загрози та ризики, які зростають у міру того, як використання технологій стає більш поширенішим.

У щорічному виданні Міжнародного інституту внутрішніх аудиторів "Північноамериканський пульс внутрішнього аудиту: орієнтири для керівників внутрішнього аудиту" за 2023 рік, наведені результати опитування керівників внутрішнього аудиту, які зазначили, що ***проблеми, які становлять високі або дуже високі ризики для їхніх установ, були пов'язані з технологіями,*** зокрема:

- 78% зазначили про ризики, пов'язані з кібербезпекою;
- 57% - ІТ загалом;
- 51% - взаємозв'язки із третіми сторонами (організаціями), які часто надають ІТ-послуги.

ПРОВЕДЕННЯ ІТ АУДИТІВ

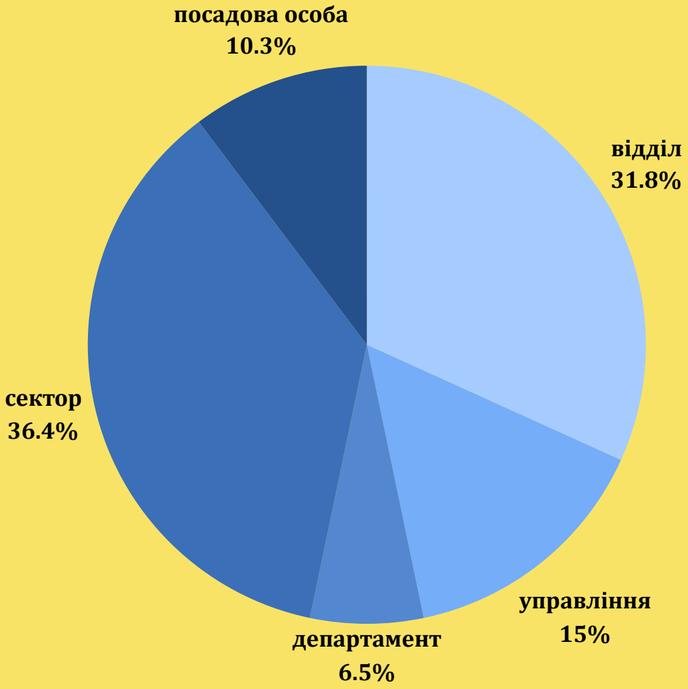
Зазначені зміни впливають й на діяльність з внутрішнього аудиту, яка повинна зосереджувати свою увагу на оцінці ризикових і пріоритетних сфер діяльності установи. Саме тому в сучасних умовах аудит інформаційних технологій (ІТ аудит) став важливою частиною діяльності з внутрішнього аудиту. Крім того, використання різних ІТ інструментів може суттєво полегшити та оптимізувати роботу внутрішніх аудиторів.

Проведення оцінки надійності, ефективності та результативності інформаційних систем і технологій є відносно новим завданням для більшості підрозділів внутрішнього аудиту державних органів в Україні. З метою збору інформації про стан розвитку функції внутрішнього аудиту щодо використання інформаційних систем і технологій та проведення їх оцінки Міністерство фінансів України провело опитування керівників підрозділів внутрішнього аудиту.

УЧАСТЬ РЕСПОНДЕНТІВ

В проведеному опитуванні взяли участь *107 керівників підрозділів внутрішнього аудиту* державних органів, у тому числі: 18 міністерств, 43 інших центральних органів виконавчої влади, 22 інших головних розпорядників коштів державного бюджету, 22 обласних і 2 районні державні адміністрації.

Найбільша частка респондентів - це керівники відділів і секторів внутрішнього аудиту 73 особи (або 68%), керівники управлінь внутрішнього аудиту 16 осіб (або 15%).



Діаграма 1. Структура респондентів за рівнем підрозділу

Діаграма 2. Структура респондентів за рівнем державного органу

АКТУАЛЬНІСТЬ ІТ АУДИТІВ

83%

У відповідях на опитуваньник ***89 керівників підрозділів внутрішнього аудиту*** (або 83%) зазначили про актуальність проведення оцінки надійності, ефективності та результативності інформаційних систем і технологій.

17%

Водночас ***18 керівників підрозділів внутрішнього аудиту*** (або 17%) зазначили про неактуальність проведення такої оцінки з огляду на:

- відсутність ІТ систем (9 осіб);
- результати оцінки ризиків (3 особи);
- можливість дослідження цих питань у рамках інших аудитів (2 особи);
- незначне застосування інформаційних технологій (1 особа);
- відсутність знань у цій сфері (1 особа);
- проведення таких перевірок іншим структурним підрозділом (2 особи).

ОРГАНІЗАЦІЙНА СПРОМОЖНІСТЬ ПІДРОЗДІЛІВ ВНУТРІШНЬОГО АУДИТУ У СФЕРІ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

ОКРЕМІ ПІДРОЗДІЛИ ІТ АУДИТУ

Лише в 4-х державних органах у складі підрозділу внутрішнього аудиту створені окремі підрозділи ІТ аудиту, фактична чисельність їх працівників - 17 од.

ОКРЕМІ ПРАЦІВНИКИ

У 18-ти державних органах працюють 25 внутрішніх аудиторів, які володіють знаннями, вміннями та навичками з проведення ІТ аудиту.

Із загальної фактичної чисельності внутрішніх аудиторів державних органів (станом на 31.12.2023 - 1180 аудиторів), ***лише 42 внутрішні аудитори (або 3,6%)*** володіють знаннями, вміннями та навичками з проведення ІТ аудиту.

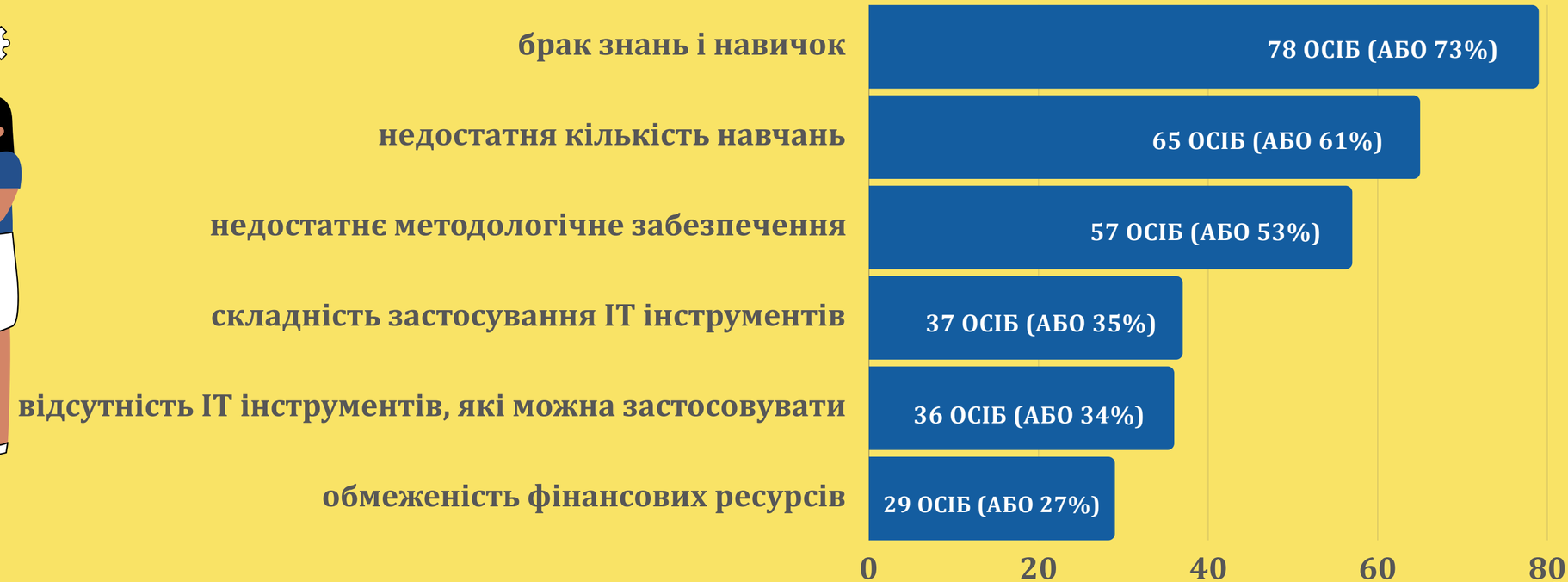
Водночас у більшості підрозділів внутрішнього аудиту державних органів ***(85 підрозділів, або 79% респондентів)*** відсутні працівники, які володіють такими знаннями, вміннями та навичками. Основними причинами цього, на думку респондентів, є:

- малочисельність підрозділів внутрішнього аудиту - ***45 установ (або 52% респондентів);***
- відсутність інформаційних систем, які можуть бути об'єктами внутрішнього аудиту - ***9 установ (або 10% респондентів);***
- неактуальність зазначеної тематики - ***5 установ (або 6% респондентів).***

При цьому ***10 керівників департаментів та управлінь внутрішнього аудиту*** в опитуванні зазначили про відсутність у складі їх підрозділів працівників, які володіють знаннями, вміннями та навичками з проведення ІТ аудиту, хоча для цих підрозділів тематика ІТ аудиту є актуальною.

ФАКТОРИ, ЯКІ ПЕРЕШКОДЖАЮТЬ РОЗВИТКУ ІТ АУДИТУ

За результатами проходження опитування керівники підрозділів внутрішнього аудиту виділили ***6 головних факторів***, які не сприяють або перешкоджають проведенню підрозділом внутрішнього аудиту оцінки надійності, ефективності та результативності інформаційних систем і технологій, зокрема:



Загальна кваліфікаційна спроможність підрозділів внутрішнього аудиту

Знання політик і процедур:

39% підрозділів внутрішнього аудиту добре обізнані із політиками та процедурами щодо інформаційної безпеки, інших питань, пов'язаних з використанням інформаційних технологій в установі, при цьому ***лише 4%*** таких підрозділів часто застосовують такі знання у своїй практичній діяльності;

Розуміння основ кібербезпеки:

50% підрозділів внутрішнього аудиту мають добре розуміння основ кібербезпеки, однак ***лише 4%*** таких підрозділів часто застосовують такі знання у своїй практичній діяльності;

Знання загальної ІТ інфраструктури та мереж:

38% підрозділів внутрішнього аудиту у відповідях на опитувальник зазначили, що мають добре розуміння загальної ІТ інфраструктури та мереж, *але зазначений показник може бути дещо завищеним, оскільки для доброго розуміння таких питань потрібні відповідні знання та освіта в цій сфері.*

Самооцінка підрозділів внутрішнього аудиту

Більшість підрозділів внутрішнього аудиту у відповідях на опитувальник зазначили про ***загальний (базовий) рівень знань*** щодо політик і процедур стосовно інформаційної безпеки, інших питань, пов'язаних з використанням інформаційних технологій в установі ***(49%)***, розуміння основ кібербезпеки ***(39%)***, загальної ІТ інфраструктури та мереж ***(45%).*** Водночас у частини таких підрозділів взагалі ***відсутні знання, навички і компетенції з відповідних питань, зокрема щодо політик і процедур (12%), основ кібербезпеки (11%) та загальної ІТ інфраструктури (17%).***

З метою підвищення кваліфікації ***30 підрозділів внутрішнього аудиту (або 28%)*** протягом останніх 2-х років проходили навчання з питань, пов'язаних з ІТ, у тому числі щодо ***цифрової грамотності, кібербезпеки, аналізу даних, роботи з ChatGPT, заходів ІТ контролю та ІТ інструментів***. Зазначені навчання були організовані Вищою школою публічного управління, НУ "Полтавська політехніка", КНЕУ ім. В. Гетьмана, Українським державним університетом ім. М. Драгоманова, Державним університетом економіки і технологій, Луцьким національним технічним університетом, Черкаським регіональним центром підвищення кваліфікації, компанією “Go IT”, організацією “CRDF Global в Україні”. Крім того, окремі навчання внутрішні аудитори проходили на онлайн-платформах Дія.Освіта, Prometheus, ВУМ online тощо.

Загальна кваліфікаційна спроможність підрозділів внутрішнього аудиту

Розуміння мети використання загальних заходів контролю:

48% підрозділів внутрішнього аудиту, які взяли участь в опитуванні, добре розуміють мету використання загальних заходів контролю (управління доступом, управління змінами, управління інцидентами тощо). Водночас 44 % підрозділів внутрішнього аудиту мають лише базовий рівень розуміння, а у 8% - взагалі відсутні знання щодо таких питань

Розуміння ключових заходів контролю:

41% підрозділів внутрішнього аудиту у відповідях на опитувальник зазначили, що мають добре розуміння ключових заходів контролю, розроблених для впливу на ризики, пов'язані з ІТ. Водночас 42 % підрозділів внутрішнього аудиту мають лише базовий рівень розуміння, а у 17% - взагалі відсутні знання щодо таких питань

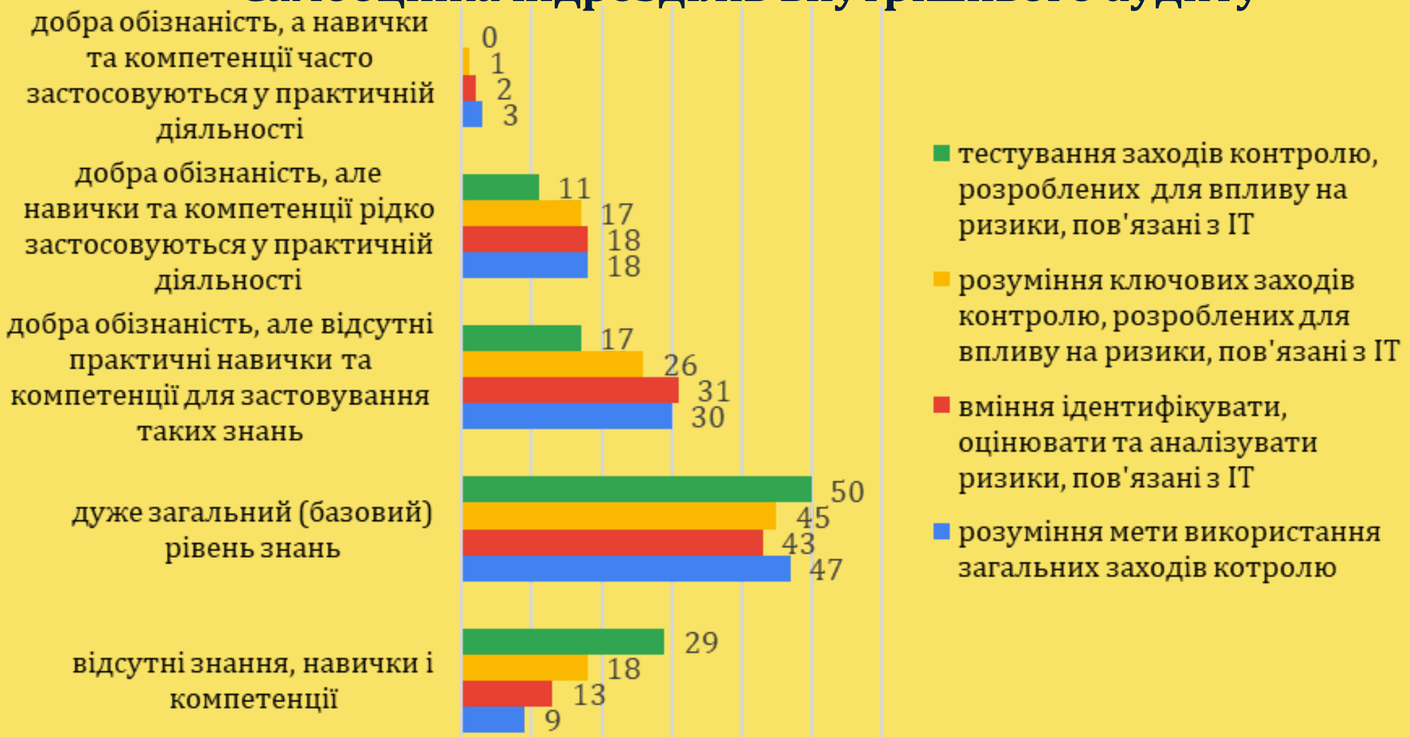
Вміння ідентифікувати, оцінювати та аналізувати ризики:

48% підрозділів внутрішнього аудиту мають добре вміють ідентифікувати, оцінювати та аналізувати ризики, пов’язані з ІТ, однак ***лише 2% підрозділів внутрішнього аудиту часто застосовують ці знання та вміння у практичній діяльності***

Тестування заходів контролю:

26% підрозділів внутрішнього аудиту мають добру обізнаність щодо тестування заходів контролю, розроблених для впливу на ризики, пов'язані з ІТ, ***при цьому жоден з таких підрозділів не застосовує такі знання у своїй практичній діяльності часто.***

Самооцінка підрозділів внутрішнього аудиту



Загальна кваліфікаційна спроможність підрозділів внутрішнього аудиту

38% підрозділів внутрішнього аудиту добре володіють техніками та інструментами аналізу та візуалізації даних, ***однак лише 5% таких підрозділів часто застосовують такі вміння та навички у своїй практичній діяльності;***

24% підрозділів внутрішнього аудиту не володіють техніками та інструментами аналізу та візуалізації даних;

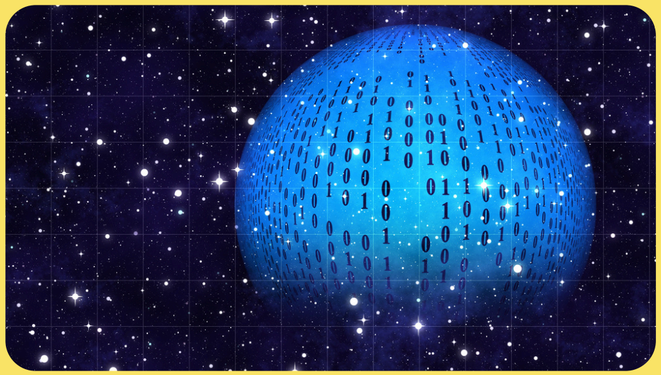
38% підрозділів внутрішнього аудиту у відповідях на опитувальник зазначили, що мають дуже загальний (базовий) рівень знань щодо технік та інструментів аналізу та візуалізації даних.

Самооцінка підрозділів внутрішнього аудиту

84 керівники підрозділів внутрішнього внутрішнього аудиту **(або майже 79% респондентів)** не навели жодного прикладу IT інструментів, які їх підрозділ у використовує в практичній діяльності.

Лише невелика частина респондентів зазначила про використання текстових редакторів, електронних таблиць, системи управління базами даних, графічних пакетів і програм створення презентацій, а решта учасників замість IT інструментів навели назви веб-сайтів, які вони використовують як джерела інформації під час планування і виконання аудиторських завдань.

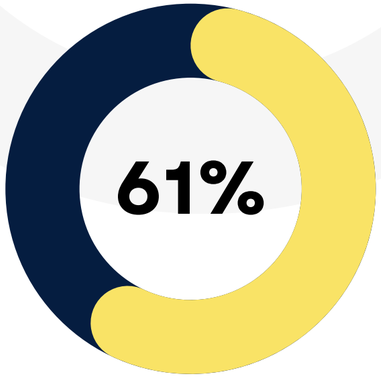
ОБ’ЄКТИ ВНУТРІШНЬОГО АУДИТУ



Приклади підходів до формування простору внутрішнього аудиту (в частині ІТ) наведено в розділі 3 посібника з ІТ аудиту, розробленого Практикуючим спітовариством з внутрішнього аудиту PEM PAL. Зокрема, на думку авторів посібника, з метою впливу на важливі та стратегічні ІТ ризики до простору внутрішнього аудиту завжди потрібно включати 3 головні процеси:

- управління інформаційними технологіями;
- інформаційна безпека;
- кіберстійкість.

Включення об'єктів внутрішнього аудиту, пов'язаних з ІТ, до бази даних



більшість респондентів (61%) зазначили, що в їх підрозділах внутрішнього аудиту, до ***бази даних включені, об'єкти внутрішнього аудиту, пов’язані з інформаційними системами і технологіями***, та навели відповідні приклади таких об’єктів. При цьому, ***13 респондентів (або 12%) у наведених прикладах все ще невірно трактують “об'єкт внутрішнього аудиту”*** як установу (або структурний підрозділ), як завдання або тему внутрішнього аудиту.

водночас досить значна частка респондентів (39%) не навели прикладів таких об’єктів (25 керівників підрозділів внутрішнього аудиту (або 23%)) або зазначили про відсутність у ***базі даних об'єктів внутрішнього аудиту, пов’язаних з інформаційними системами і технологіями***, (17 керівників підрозділів внутрішнього аудиту (або 16%)). Однак ця частина респондентів не врахувала, що такими об’єктами можуть бути діяльність щодо інформаційної безпеки, забезпечення функціонування технічних засобів для інформаційних систем в установі тощо.

IT ІНСТРУМЕНТИ

ІНСТРУМЕНТИ ДЛЯ АНАЛІЗУ ДАНИХ

В міжнародній практиці внутрішні аудитори використовують різні інструменти для полегшення, пришвидшення та оптимізації своєї роботи.

Нові технології дають змогу аудиторам збирати дані з ширшим охопленням, швидше їх передавати та обробляти, а це в свою чергу покращує результати роботи та дозволяє оптимізувати ресурси.

Існує багато інструментів, які можуть допогти внутрішнім аудиторам провести аналіз даних і структуровано візуалізувати його результати. Приклади деяких з цих інструментів наведено на цьому слайді.

Microsoft Excel

Популярний і широко використовуваний аналітичний інструмент, який дозволяє збирати, узагальнювати, аналізувати та візуалізувати дані завдяки низці аналітичних, логічних, фінансових та інших функцій, а також формувати зведені таблиці та діаграми, відфільтрувати дані відповідно до потреб.

Knime

Безкоштовна аналітична платформа, яка дозволяє агрегувати, сортувати, фільтрувати, об’єднувати дані, а також досліджувати їх за допомогою інтерактивних діаграм і візуалізацій, автоматизувати електронні таблиці тощо.

Microsoft Power BI

Комплексне програмне забезпечення бізнес аналітики від Microsoft, яке дає можливість отримувати дані з різних джерел, створювати моделі даних, проводити обчислення за допомогою різноманітних функцій, налаштовувати категорії й формати даних, щоб поглибити та деталізувати аналіз, а також створювати сучасні інтерактивні візуалізації та звіти.

IT ІНСТРУМЕНТИ

ІНСТРУМЕНТИ ДЛЯ АНАЛІЗУ ДАНИХ

Перелік аналітичних інструментів є досить широким і постійно розширюється. Можливості їх використання залежать не лише від наявності фінансових ресурсів (використання деяких інструментів (або принаймні їх окремих функцій) є безкоштовним), але й від знань, вмінь і навичок аудиторів стосовно їх використання.

Водночас слід зазначити, що в загальному доступі в мережі інтернет є досить багато матеріалів, за допомогою яких внутрішні аудитори можуть ознайомитися із основними функціями та можливостями інструментів для аналізу даних.

IDEA

Комплексний інструмент аналізу даних, що дозволяє визначати тенденції, закономірності та винятки, взаємозв'язки між даними, а також створювати різноманітні візуалізації. Наявна можливість імпорту даних IDEA із інших програм, таких як Tableau, Power BI, MS Excel тощо.

Audit Command Language (ACL) analytics

Програмне забезпечення, за допомогою якого можна витягнути та аналізувати дані для виявлення та запобігання шахрайству, а також управління ризиками. Цей інструмент відбирає великі набори даних, щоб виявити порушення або закономірності в операціях, які можуть вказувати на слабкість заходів контролю або шахрайство.

Qlik Sense

Платформа для аналітики даних, що дозволяє підключати і об'єднувати дані з різних джерел, має вбудовану технологію штучного інтелекту, який пропонує аналізи та ідеї, автоматизує процеси створення аналітики та підготовки даних.

В цій презентації наведені найбільш широко застосовані інструменти для аналізу та візуалізації даних. Крім того, існує дуже багато інших інструментів, які можуть використовувати як внутрішні, так і зовнішні аудитори. Наприклад, у "Вказівках щодо проведення аудиторської діяльності з аналітикою даних", підготовлених Робочою групою INTOSAI з великих даних, згадується досить багато прикладів інших інструментів.

IT ІНСТРУМЕНТИ

ІНСТРУМЕНТИ ДЛЯ АНАЛІЗУ ДАНИХ

Питання щодо інструментів, рішень, методів і програмного забезпечення для автоматизації роботи внутрішніх аудиторів є надзвичайно актуальним і часто обговорюється серед практикуючих внутрішніх аудиторів. Зокрема, у травні 2024 року на черговому засіданні Практикуючого співтовариства з внутрішнього аудиту PEM PAL внутрішні аудитори Федерального Міністерства Фінансів Австрії презентували свій досвід використання різних IT інструментів (деякі з них наведені на цьому слайді).

Microsoft Visio

Комплексний інструмент для візуалізації та моделювання процесів, створення схем процесів (“як є?” та “як повинно бути?”), організаційних структур, схем причинно-наслідкових зв’язків, SWOT-аналізу, мережевих схем тощо.

MaxQDA

Програмне забезпечення, за допомогою якого можна аналізувати якісні дані з використанням штучного інтелекту (узагальнювати текстові дані, підсумовувати результати інтерв’ю, зокрема аудіо- та відеофайли). MaxQDA також дозволяє поєднати аналіз якісних і кількісних даних з використанням змішаних методів і численних інструментів для оцінки обох типів даних

InfraNodus

Інструмент, що допомагає проводити візуальний аналіз тексту на основі штучного інтелекту. InfraNodus представляє текст як мережу та використовує алгоритми аналізу для визначення та візуалізації основних ключових слів, тем та їхніх взаємозв’язків. Цей інструмент дозволяє побачити шаблони, тематичні кластери, згенеровані штучним інтелектом, і, що більш важливо, структурні прогалини.

РИЗИКИ, ПОВ’ЯЗАНІ З ІНФОРМАЦІЙНИМИ ТЕХНОЛОГІЯМИ

Інформаційні технології постійно змінюються та удосконалюються. Такі зміни вимагають від внутрішніх аудиторів регулярного визначення та розуміння впливу ризиків, повязаних з інформаційними технологіями. В посібнику з IT аудиту, розробленому Практикуючим спітовариством з внутрішнього аудиту PEM PAL, наведені 4 основні кроки, які необхідно зробити аудиторам, щоб враховувати зазначені зміни в своїй роботі:

01 щороку проводити незалежну оцінку IT-ризиків, щоб визначити нові технології, які впливають на організацію

02 ознайомитися з річними короткостроковими планами IT підрозділу та проаналізувати, як вони впливають на оцінку IT-ризиків

03 починати кожен IT-аудит з перегляду та оцінки ризиків

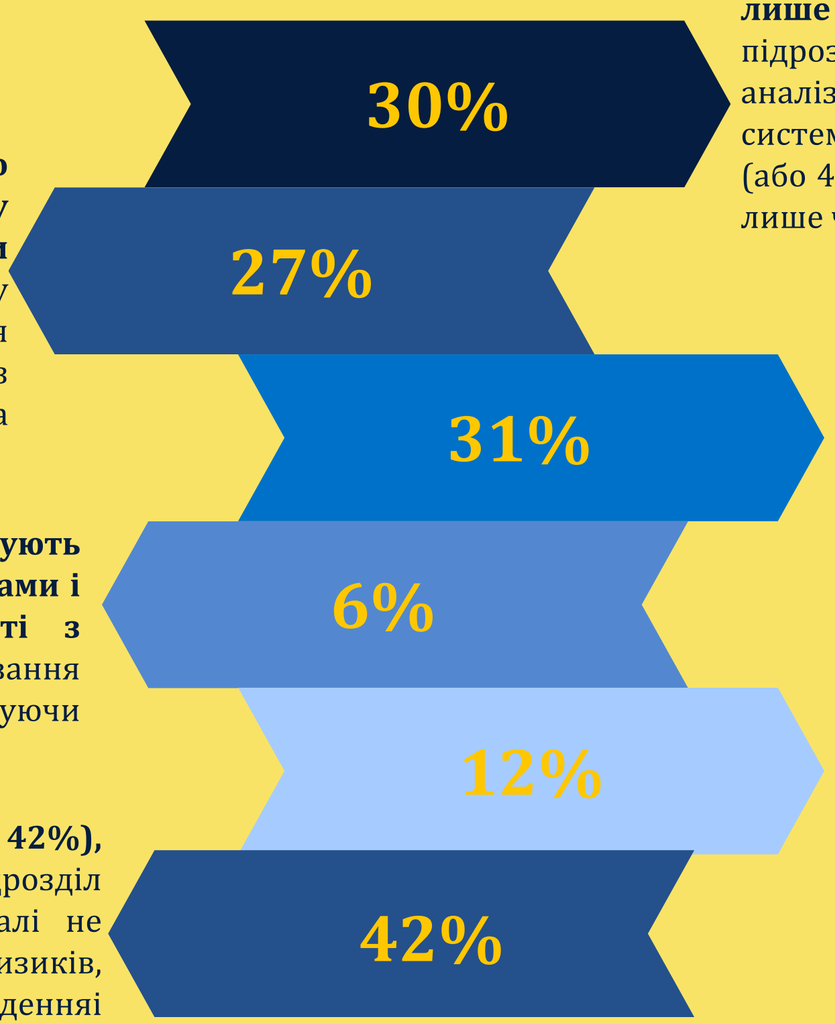
04 бути гнучкими у сфері IT-аудиту — відстежувати ризики в установі, пов’язані з IT, і запроваджувати процедури аудиту в міру їх зростання.

ІДЕНТИФІКАЦІЯ ТА ОЦІНКА РИЗИКІВ, ПОВ’ЯЗАНИХ З ІНФОРМАЦІЙНИМИ ТЕХНОЛОГІЯМИ

29 респондентів (або 27%) зауважили про нездійснення ідентифікації, оцінки та аналізу ризиків, пов'язаних з інформаційними системами і технологіями. Проте 6 з них у подальших відповідях зазначали про проведення оцінки таких ризиків при плануванні діяльності з внутрішнього аудиту, під час планування та виконання аудиторських завдань.

лише 6 респондентів (або 6%) враховують ризики, пов'язані з інформаційними системами і технологіями, на всіх етапах діяльності з внутрішнього аудиту, починаючи від планування діяльності з внутрішнього аудиту та закінчуючи звітуванням про її результати.

45 респондентів (або 42%), зазначили, що їх підрозділ внутрішнього аудиту взагалі не здійснює оцінку ризиків, пов'язаних з ІТ, при проведенняі внутрішніх аудитів.



лише 32 респонденти (або 30%), зазначили, що їх підрозділ внутрішнього аудиту ідентифікує, оцінює та аналізує ризики, пов'язані з інформаційними системами і технологіями. Крім того, 46 респондентів (або 43%) повідомили, що здійснюють таку діяльність лише частково.

33 респонденти (або 31%), зазначили, що їх підрозділ внутрішнього аудиту враховує ризики, пов'язані з інформаційними системами і технологіями, лише на етапі планування діяльності з внутрішнього аудиту.

лише 13 респондентів (або 12%), зауважили, що оцінка ризиків, пов'язаних з інформаційними системами і технологіями, здійснюється під час проведення всіх внутрішніх аудитів. Крім того, **49 респондентів (або 46%)** повідомили про те, що оцінка таких ризиків здійснюється у разі включення до програми внутрішнього аудиту питань, пов'язаних з ІТ.

Проведення IT аудитів

19 Протягом 2021-2023 років 1***9 підрозділів внутрішнього аудиту (або 18%) проводили IT аудити.*** Крім того, ще 19 респондентів (або 18%) зазначили, що IT аудити їх підрозділи не проводили, але під час проведення аудитів вони досліджували окремі питання, пов'язані з інформаційними системами і технологіями.

16 респондентів залучали до проведення IT аудитів експертів з інших структурних підрозділів, інших державних органів, консалтингових компаній

9 респондентів при проведенні IT аудитів використовували рамкові основи, стандарти, вказівки

Ключові аспекти, які досліджено внутрішніми аудиторами при проведенні IT аудитів, та кількість підрозділів внутрішнього аудиту, що їх досліджувала

Рамкові основи (стандарти, вказівки), які використовуються під час проведення ІТаудиту

Під час проведення ІТ аудитів зазвичай використовуються різні рамкові основи, стандарти або вказівки залежно від об’єкта та цілей аудиту. У відповідях на опитувальник ***9 респондентів, які у 2021-2023 роках проводили ІТ аудити або досліджували окремі питання, пов'язані з інформаційними системами і технологіями***, зазначили про використання різних рамкових основ і навели їх приклади (ISO/IEC 27001, COBIT 5, GTAG-8, PRINCE 2, ITIL 4).

Крім того, ще ***13 респондентів зауважили, що частково використовували такі рамкові основи.*** Нижче наведено приклади цих рамкових основ.

ISO/IEC 2700x

Стандарти ISO серії 2700X стосуються різних тем у сфері інформаційної безпеки, в тому числі: системи управління інформаційною безпекою та управління захистом даних, рекомендації щодо управління ризиками інформаційної безпеки, тощо.

COBIT

Стандарт, розроблений Асоціацією з аудиту та контролю інформаційних систем (ISACA) , який містить кращі практики з управління інформаційними технологіями, зокрема: цілі, принципи та об'єкти управління, опис ІТ-процесів (завдань), практичні рекомендації по управлінню ІТ-безпекою. Зазначені стандарти постійно оновлюються та актуалізуються (українською мовою доступна версія COBIT 4.1: http://www.isaca.org.ua/index.php/standards/cobit).

GTAG

Глобальні вказівки з аудиту технологій, розроблені Міжнародним інститутом внутрішніх аудиторів, які включають низку вказівок щодо аудиту управління інформаційними технологіями, контролю та безпеки.

Рамкові основи (стандарти, вказівки), які використовуються під час проведення IT аудиту

ITIL	PRINCE	ITAF
Бібліотека інфраструктури інформаційних технологій, яка містить кращі світові практики і рекомендації стосовно надання IT-послуг, документування процесів, функцій та ролей, Управління IT-службою тощо.	Методологія управління IT проєктами, розроблена британською Урядовою організацією OGC, яка містить 7 основних принципів управління проєктом (запуск, ініціювання, керування, контроль стадій, керування розробкою та межами стадій, завершення проєкту), а також основні предметні теми та опис ролей у проєкті.	Збірник настанов для фахівців з IT аудиту, який розроблений Асоціацією з аудиту та контролю інформаційних систем (ISACA), що містить основні положення професійної практики аудиту та підтвердження довіри до інформаційних систем. Ці настанови постійно оновлюються та актуалізуються (українською мовою доступна версія ITAF 3: http://www.isaca.org.ua/index.php/standards/cobit).

Приклади використання різних рамкових основ, стандартів і вказівок наведено в розділі 2 посібника з IT аудиту, розробленого Практикуючим спітовариством з внутрішнього аудиту PEM PAL.

ВИКОРИСТАННЯ CHATGPT ПРИ ПРОВЕДЕННІ ВНУТРІШНІХ АУДИТІВ

В міжнародній практиці досить часто обговорюють можливості використання штучного інтелекту для удосконалення та оптимізації роботи. Такі тенденції характерні й для діяльності з внутрішнього аудиту.

Нещодавно була опублікована стаття, в якій детально описано приклади використання ChatGPT для покращення процесу внутрішнього аудиту на прикладі великої міжнародної компанії Uniper. Автори статті дослідили переваги та виклики інтеграції ChatGPT у процес внутрішнього аудиту (на прикладі аудиту фізичної безпеки). Зокрема публікація містить приклади його застосування на ***3-х етапах аудиту (підготовка до аудиту, робота на місці, звітування)***, які також наведені на цьому слайді.

Для використання в роботі ChatGPT внутрішні аудитори компанії Uniper визначили ключові практики та правила, які також містяться в статті.

За результатами проведеного аудиту працівники підрозділу внутрішнього аудиту цієї компанії оцінюють ***підвищення ефективності від 50 до 80% для різних процесів внутрішнього аудиту.***

Важливо відмітити, що з урахуванням ризиків і потенційних обмежень використання ChatGPT, ***внутрішні аудитори компанії Uniper не використовували персональні або корпоративні дані з метою збереження конфіденційності, а також не вводили повні тексти документів, а лише певні фрагменти або твердження*** (у додатках до статті містяться відповідні приклади запитів у ChatGPT).

01 Підготовка до аудиту:

Внутрішні аудитори компанії Uniper почали використовувати ChatGPT для ***виявлення потенційних ризиків фізичної безпеки*** (близько 80% ризиків були згенеровані ChatGPT). Надалі ідентифіковані ризики були обговорені із замовником, який підтвердив, що такі ризики є обгрунтованими та актуальними.

Також за допомогою цього інструменту аудитори ***визначили обсяг аудиту***, що містив 7 сфер і 3 підпункти в кожній сфері, які пізніше було обговорено із замовником і уточнено.

У додатках до статті містяться відповідні приклади запитів у ChatGPT.

02 Робота на місці

На наступному етапі аудитори використовували ChatGPT ***для підготовки питань до інтерв'ю, структурування та узагальнення протоколів зустрічей за результатами інтерв'ю, дослідження нормативних документів, стандартів і публікацій та узагальнення їх основних ідей*** (у додатках до статті містяться відповідні приклади запитів у ChatGPT).

03 Звітування

Під час підготовки звіту за результатами аудиту внутрішні аудитори з метою ***покращення його читабельності*** вводили в ChatGPT короткі частини висновків і створювали їх альтернативні варіанти (у додатках до статті містяться відповідні приклади запитів у ChatGPT).

Результати IT аудитів, проведених респондентами

35 респондентів (або 33%) навели приклади найбільш значущих недоліків і проблем, пов'язаних з використанням інформаційних систем і технологій, виявлених у 2021-2023 роках. Серед них найбільш типовими були:

- вісутність загальної стратегії розвитку IT інфраструктури;
- невизначеність політик і процедур щодо резервного копіювання інформації та щодо реагування на кіберінциденти;
- проблеми із захистом інформації, даних та їх цілісністю;
- несанкціонований доступ до інформаційних систем;
- несвоєчасне здійснення резервного копіювання тощо.

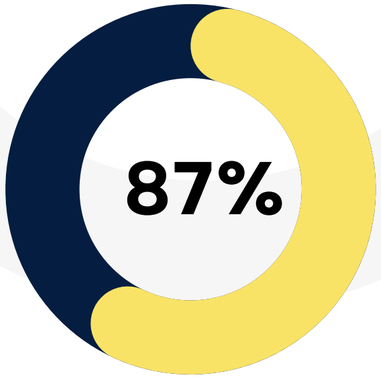
Кількість підрозділів внутрішнього аудиту, які надавали рекомендації, направлені на зменшення/уникнення ризиків, пов'язаних з інформаційними системами і технологіями

8 респондентів (або 7%) протягом останніх трьох років за результатами проведених внутрішніх аудитів надали більше 10-ти рекомендацій, направлених на зменшення/ уникнення ризиків, пов'язаних з інформаційними системами і технологіями.

30 респондентів (або 28%) навели приклади наданих рекомендацій, які стосувалися:

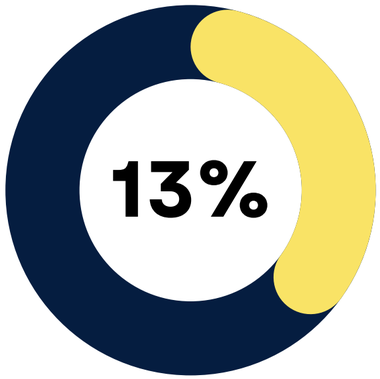
- визначення структури ролей користувачів, рівня їх доступу та повноважень користувачів;
- розробки порядку резервного копіювання інформації, проведення такого копіювання, перевірки та здійснення його моніторингу;
- проходження навчання з відповідних питань тощо.

ДОСТУП ДО ІНФОРМАЦІЙНИХ СИСТЕМ І БАЗ ДАНИХ



переважна більшість респондентів (87%) зазначили, що в їх підрозділах внутрішнього аудиту, ***наявний доступ до інформаційних систем і баз даних***, необхідних для проведення внутрішніх аудитів, в тому числі:

- 17 підрозділів внутрішнього аудиту (або 16%) має доступ до всіх інформаційних систем і баз даних;
- в 19-ти підрозділах внутрішнього аудиту (або 18%) наявний доступ до окремих інформаційних систем і баз даних установи;
- 57 підрозділів внутрішнього аудиту (або 53%) зазначили, що доступ до таких систем і баз даних надається за окремим рішенням керівника установи (у разі наявності обгрунтованої потреби).



водночас 14 респондентів (або 13%) зазначили, що в їхніх підрозділах внутрішнього аудиту відсутній доступ до інформаційних систем і баз даних, необхідних для проведення внутрішніх аудитів, і навели приклади таких систем і баз даних (зокрема, до систем для автоматизації бухгалтерського обліку та звітності (наприклад, Is-pro, M.E.Doc), управління людськими ресурсами та нарахування заробітної плати (HRMIS), до окремих державних реєстрів (наприклад, Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, Єдиного реєстру судових рішень) тощо).

МОЖЛИВІ ШЛЯХИ УДОСКОНАЛЕННЯ ДІЯЛЬНОСТІ З ВНУТРІШНЬОГО АУДИТУ

73 керівники підрозділів внутрішнього аудиту (або 68% респондентів) у відповідях на опитувальник зазначили можливі шляхи удосконалення діяльності з внутрішнього аудиту з урахуванням сучасного рівня розвитку інформаційних технологій. Набільш поширеними серед респондентів були наступні пропозиції:

проведення навчання

організація та проведення різних навчальних заходів для підвищення компетентності внутрішніх аудиторів, зокрема у сфері IT, а також отримання практичних навичок у даній сфері

автоматизація роботи

впровадження програмного продукту, який забезпечить комплексне покриття процесів внутрішнього аудиту (планування, здійснення внутрішніх аудитів, звітування)

добір персоналу

залучення або прийняття на роботу в підрозділи внутрішнього аудиту фахівців/спеціалістів, які володіють знаннями, навичками і компетенціями у сфері IT

методологічна підтримка

удосконалення методології проведення IT аудиту, в тому числі розробка типових форм робочих документів з використанням практичних прикладів

Слід зазначити, що Мінфін у межах співпраці з міжнародними проєктами запланував низку заходів з метою підвищення кваліфікаційної спроможності підрозділів внутрішнього аудиту в сфері IT, у тому числі: проведення навчальних заходів, оновлення методології. Крім того, в рамках проєкту EU4PFM здійснюється підготовка специфікацій IT-рішення для ДВФК порталу, який дозволить частково автоматизувати окремі напрями роботи підрозділів внутрішнього аудиту.

Рекомендовані заходи для удосконалення діяльності з внутрішнього аудиту

01

Переглянути та оновити простір внутрішнього аудиту з урахуванням наявних об’єктів внутрішнього аудиту, в тому числі згідно з прикладом, наведеним у методичному посібнику “Ризик-орієнтоване планування діяльності з внутрішнього аудиту”

02

Налагодити співпрацю і регулярну взаємодію із структурними підрозділами інформаційних технологій та інформаційної безпеки з метою обміну інформацією щодо наявних в установі інформаційних систем і технологій, а також проведення ідентифікації та оцінки ризиків, пов’язаних з ними

03

Розробити (або оновити) Модель загальних компетенцій, навиків і знань, до якої включити пов’язані ІТ сфери, зокрема: розуміння мети використання загальних заходів контролю (управління доступом, управління змінами, управління інцидентами тощо); знання політик і процедур щодо інформаційної безпеки та інших питань, пов'язаних з використанням ІТ; розуміння основ кібербезпеки; вміння ідентифікувати, оцінювати та аналізувати ризики, пов'язані з ІТ; розуміння ключових заходів контролю, розроблених для впливу на ці ризики, та їх тестування; володіння техніками та інструментами аналізу даних тощо.

Застосовувати розроблену Модель загальних компетенцій, навиків і знань під час пошуку персоналу в підрозділ внутрішнього аудиту, а також при плануванні заходів з підвищення кваліфікації працівників підрозділу внутрішнього аудиту

04

На періодичній основі відслідковувати доступні на Порталі управління знаннями НАДС, а також на інших ресурсах (наприклад, на онлайн-платформах Дія.Освіта, Prometheus, ВУМ online) навчальні заходи, програми яких містять питання, пов’язані з інформаційними системами і технологіями

05

Опрацювати Рамкові основи (стандарти, вказівки), які використовуються під час проведення ІТ аудиту, та у разі доцільності використовувати їх під час проведення ІТ аудитів або дослідження питань, пов’язаних з інформаційними системами і технологіями

06

Продовжувати змінювати пріоритети під час проведення внутрішніх аудитів, зокрема планувати та проводити ІТ аудити (в тому числі й на ранніх стадіях запровадження нових ІТ систем та / або проєктів), з огляду на пов’язані з ними ризики, а також враховуючи наявну кваліфікаційну спроможність підрозділів внутрішнього аудиту