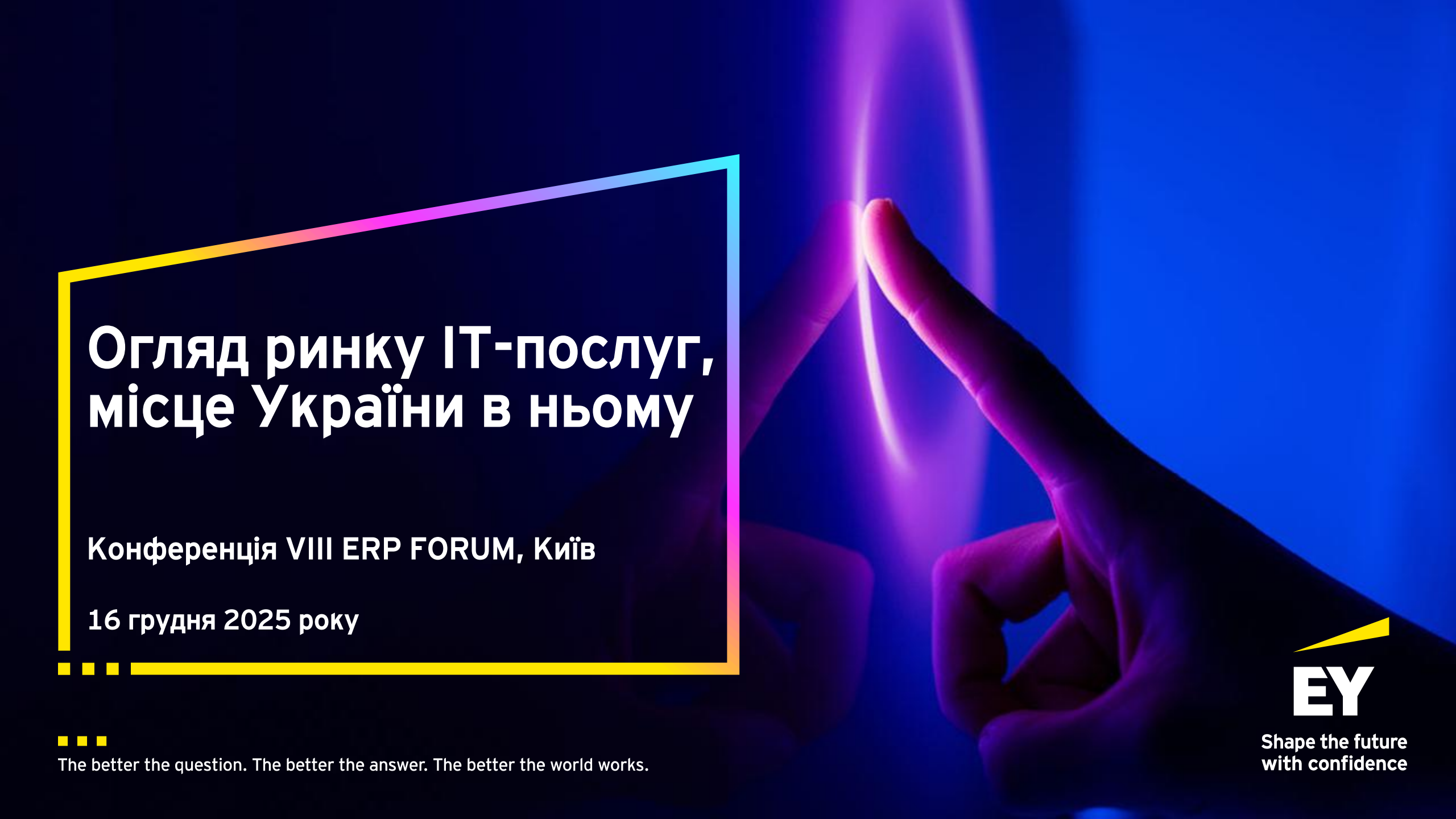




Огляд ринку ІТ-послуг, місце України в ньому

Конференція VIII ERP FORUM, Київ

16 грудня 2025 року



The better the question. The better the answer. The better the world works.



Shape the future
with confidence

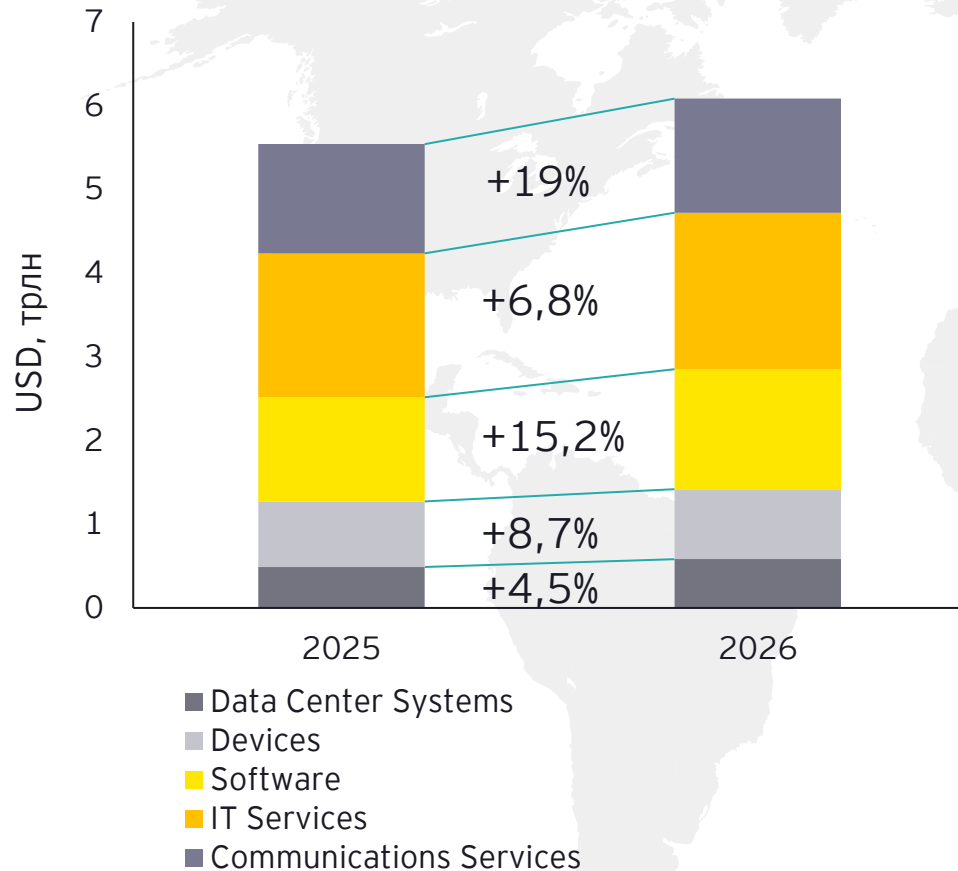
Про що поговоримо сьогодні

- Огляд глобального ринку ІТ
- Ключові драйвери зростання
- Український ІТ-сектор
- Виклики та можливості



Світовий ринок ІТ послуг: розмір та динаміка

Прогноз витрат на ІТ*



Топ 15 споживачів ІТ:

- США
- Китай
- Японія
- Німеччина
- Велика Британія
- Франція
- Індія
- Канада
- Бразилія
- Південна Корея
- Італія
- Австралія
- Іспанія
- Нідерланди
- ОАЕ

Попит за галузями:

- Фінансові послуги
- Виробництво
- Охорона здоров'я
- Торгівля та e-commerce
- Телекомунікації
- Енергетика
- Державний сектор
- Транспорт і логістика
- Освіта
- Медіа та розваги

Глобальні тренди зростання попиту на ІТ-послуги



Generative AI



AI-програмне забезпечення



Консалтинг та інтеграція AI



Хмарні технології



Потужні сервери та ЦОД



Edge-обчислення та IoT



Кібербезпека та регуляції



Прозорість та захист даних



SaaS та керовані сервіси



Екологічність ІТ

Стрибок можливостей, ROI, конкуренція

Інтеграція з CRM/ERP, готові модулі

Складність інтеграції, брак внутрішніх компетенцій

Потреба в потужностях, гнучкість та безпека

Попит на GPU, зростання обсягів даних, енергоефективність

Обробка даних в реальному часі, використання IoT, економія трафіку та швидкість

Зростання кількості атак, нові регуляції та стандарти, дефіцит кадрів

Вимоги AI Act/Data Act, прозорість алгоритмів, аудит та контроль якості даних

Прогнозовані витрати та SLA, OPEX vs CAPEX

ESG-вимоги, оптимізація енергоспоживання

Кібербезпека як стратегічний пріоритет для компаній у світі

Кібербезпека стає ключовим елементом корпоративного врядування

- Компанії суттєво підвищують зрілість кібербезпеки через інтеграцію у політики, стандарти та практичні заходи

Розмір глобального ринку

- Ринок зростає: 2025 ~\$177 млрд -> 2030 ~\$500 млрд
- Фактори зростання: збільшення кіберзагроз, перехід в хмару, посилення регуляторних вимог, критична нестача кадрів

Використання AI в кібербезпеці

- Моніторинг загроз та автоматизоване реагування
- Прогнозування ризиків та оптимізація роботи SOC

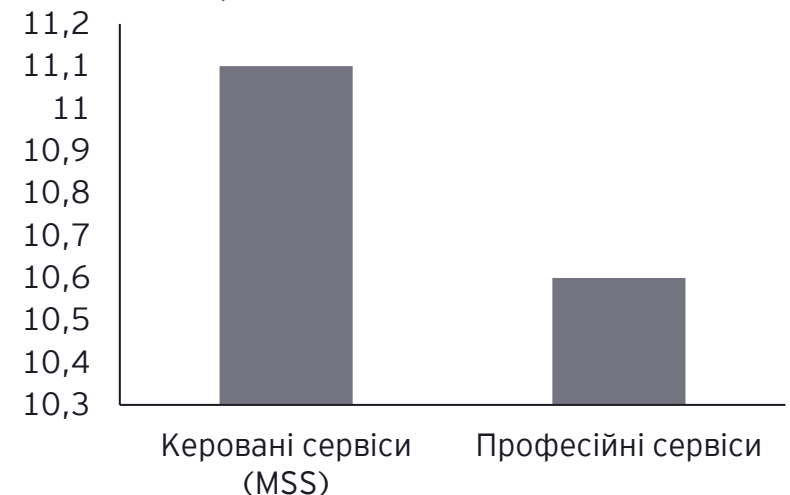
86% рад директорів мають або шукають кіберекспертизу

Аудиторський комітет відповідає за кібербезпеку у 78% компаній

73% компаній декларують відповідність зовнішнім стандартам

58% компаній включають в заходи кібербезпеки практичні інструменти

Порівняння за сегментами



CAGR, % (2025-2030)

Україна на мапі ІТ послуг

Експорт ІТ послуг стабільний попри війну

- Розмір: 2022 ~\$7,3 млрд, 2023 ~\$6,8 млрд, 2024 ~\$6,45 млрд, 2025 I пів ~\$3,28
- Географія: США ~35%, Велика Британія ~9%, Мальта ~8,5, %Кіпр ~7%, Ізраїль ~4%, Швейцарія ~4%, Німеччина ~3,5%, Естонія ~3%, Польща ~3%, інші ~22%

Позиціювання України

- ТОП-3 серед країн Східної Європи за cost-efficiency та якістю сервісу
- Переваги: велика база спеціалістів у JavaScript, Cloud, AI/ML, стійкість та гнучкість, високий рівень технічної англійської, конкурентна вартість для високій експертизі, зручні часові зони



Тренди на ІТ послуги в Україні

■ Гармонізація з нормами ЄС

Впровадження NIS2, DORA, AI Act та Data Act стимулює комплаєнс-аудити, контроль та навчання персоналу

■ Розвиток е-уряду та цифрові послуги

Інтеграція реєстрів, безпека даних та омніканальні цифрові публічні сервіси покращують державні послуги

■ Фінтех та безготівкова економіка

Модернізація платіжної інфраструктури, AML/KYC та відповідність DORA підтримують цифрові фінанси

■ Кіберстійкість та відбудова

Цифрові двійники, IoT-моніторинг та плани відновлення забезпечують безпеку критичної інфраструктури

■ Дефіцит ІТ-кадрів

Перехід на керовані сервіси забезпечує 24/7 підтримку без розширення штату

■ Цифрова трансформація SMB

SMB активно переходять на онлайн-сервіси, автоматизацію та хмарні рішення для зниження витрат і підвищення ефективності

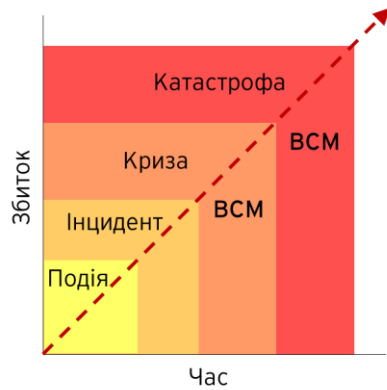
■ Розвиток кіберосвіти та up skill

Критичний дефіцит кадрів у кібербезпеці та AI на фоні вимог регуляцій ЄС до підготовлених фахівців

■ Оборонний сектор та безпека

Військові дії та потреба у стійкості стимулюють розвиток defense-tech та кіберзахисту, а також цифрових рішень для логістики та аналітики

Управління безперервністю бізнесу як ключовий компонент корпоративної стійкості



Управління безперервністю бізнесу (BCM) – це сукупність процесів, спрямованих на ефективне реагування на кризові ситуації, які

- Визначає та резервує ресурси, необхідні для функціонування критичних процесів
- Визначає дії відповідальних співробітників у разі недоступності одного або декількох ресурсів внаслідок виникнення кризових ситуацій

Статистика показує, що багато бізнесів не готові ефективно протистояти кризовим ситуаціям:



16%

Датацентрів вказали, що втрати через простій склали більше 1\$ мільйона доларів



49%

Респондентів вважають кібератаки найбільш деструктивними подіями



39%

Серед розглянутих компаній не мають плану забезпечення безперервності бізнесу (BCP)



73%

Компаній у зоні ризику матеріальних кібератак за оцінками експертів



43%

Малих бізнесів не зможуть відновитися після катастрофи або надзвичайної ситуації



88%

Кібератак у 2023 році були реалізовані через фішинг



44%

Випадків простою датацентрів виникає через збій постачання електроенергії



91%

Бізнесів стикаються зі збоями мережі принаймні раз на квартал

Попит на BCM послуги за галузями:

- Фінансовий сектор
- IT та телеком
- Енергетика та інфраструктура
- Державні установи та оборонні проєкти
- Виробничі та логістичні компанії

Безперервність бізнесу – окрім швидкого відновлення з мінімізацією втрат, це ще про захист людей та активів, збереження довіри, ділової репутації, постійне вдосконалення

ІТ як драйвер відновлення та сталого розвитку



Відновлення – це не тільки інфраструктура

- Соціальне відновлення
- Економічне відновлення
- Екологічне відновлення



Виклики щодо відновлення дають нові можливості

- Впровадження інновацій
- Доступ до фондів
- Енергетична незалежність
- Зелена трансформація
- Безпечне середовище



Цифровізація управління ресурсами

Автоматизація процесів знижує витрати, оптимізує енергоспоживання та скорочує викиди

Прозорість і контроль

Електронні платформи (Prozorro, DREAM) забезпечують відкритість, антикорупційні механізми та довіру донорів

Кіберстійкість та безпека даних

Захист критичної інфраструктури – основа економічної та соціальної стійкості

Енергоефективність та «зелена» трансформація

ІТ-рішення підтримують Smart Grid, моніторинг енергоспоживання, інтеграцію відновлюваних джерел

Інклюзія та доступність

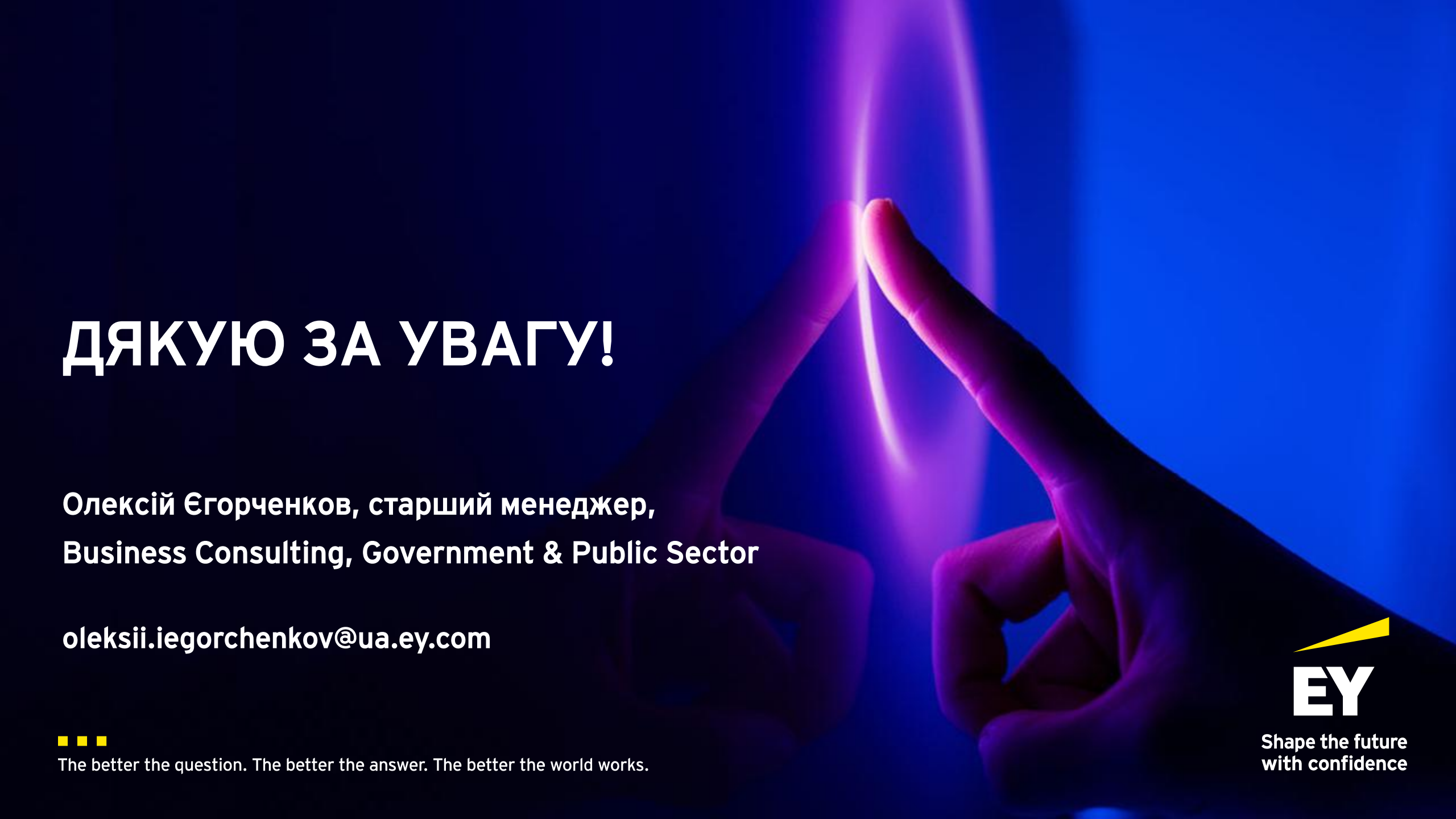
Хмарні сервіси та цифрові платформи дають рівний доступ громадам та бізнесу до послуг та фінансування

та багато іншого...

Ризики та виклики

- **Кіберзагрози і безпека даних**
Постійні атаки на держсектор і критичну інфраструктуру;
фрагментований SOC/NOC
- **Непослідовність архітектури та інтеграцій**
«Острови автоматизації», відсутність єдиного data governance,
дублювання рішень
- **Дефіцит кадрів і релокація талантів**
Конкуренція за спеціалістів, вигорання, «військові ризики»
- **Нерівномірна інфраструктура**
Пошкодження мережі/енергетики, різна якість підключення у
регіонах, перебої електропостачання
- **Регуляторні та процесні бар'єри**
Повільні зміни законодавства, складні процедури закупівель,
вимоги сумісності з міжнародними стандартами (EU Pillars, GDPR)
- **Фінансова стійкість продуктів**
Залежність від грантів і коротких бюджетних циклів; ризик
«пілотного кладовища»





ДЯКУЮ ЗА УВАГУ!

Олексій Єгорченков, старший менеджер,
Business Consulting, Government & Public Sector

oleksii.iegorchenkov@ua.ey.com



The better the question. The better the answer. The better the world works.



Shape the future
with confidence