

The background of the slide is a dark grey color with a light grey circuit board pattern. The pattern consists of vertical lines on the left side that branch out into various paths, ending in small circles, resembling a printed circuit board (PCB) layout.


# **ПРАКТИЧНІ ПИТАННЯ ЗАКОНОДАВСТВА З КІБЕРБЕЗПЕКИ ТА ДІДЖИТАЛІЗАЦІЇ**

**ЧОМУ БЕЗ ВЗАЄМОПОВ'ЯЗАНИХ ЗАКОНІВ ТА МЕТОДОЛОГІЙ  
ПОБУДУВАТИ ЦИФРОВУ ДЕРЖАВУ НЕМОЖЛИВО**



## КЛЮЧОВІ ПРОБЛЕМИ

- Відсутність єдиної методології цифровізації органів державної влади
- Невизначеність та конфлікт повноважень та інтересів ключових стейкхолдерів
- Неузгодженість законів та НПД вищого рівня
- Невизначеність ключових термінів інформаційної безпеки та кібербезпеки
- Застарілі НД ТЗІ



# МЕТОДОЛОГІЇ ЦИФРОВІЗАЦІЇ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ

Для побудови ефективної ІТ-архітектури органів державної влади та державних послуг головним є використання єдиного стандарту та підходу до виконання таких робіт.

На даний момент в Україні відсутній такий документ, однак у світі існує мінімум два варіанти такого стандарту:

1. TOGAF
2. Методологія Зерде



# TOGAF

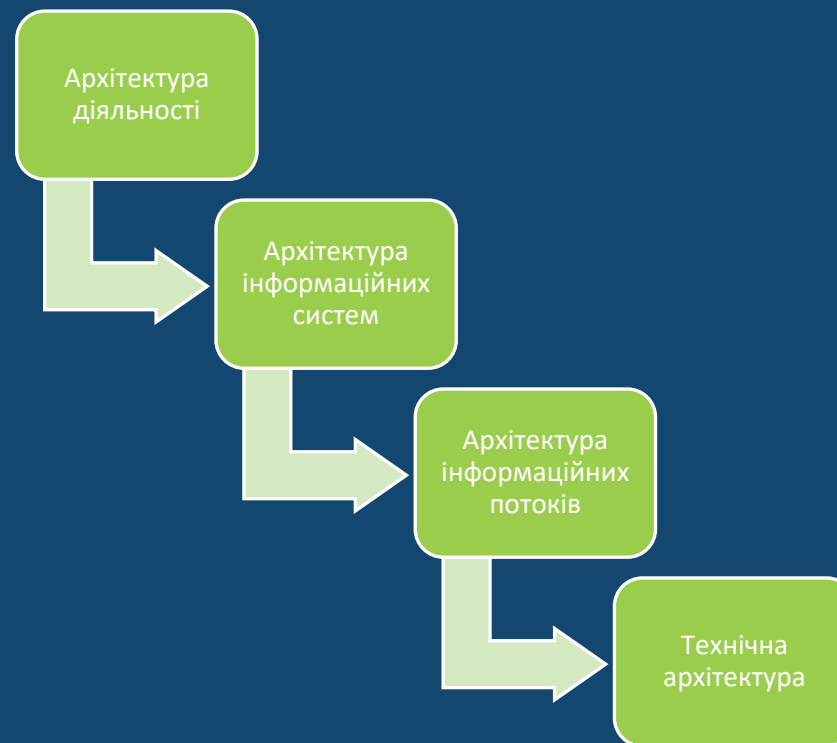
Структура архітектури Open Group (TOGAF) є найбільш часто використовуваною структурою для архітектури підприємства на сьогоднішній день, що забезпечує підхід до проектування, планування, впровадження та управління архітектурою інформаційних технологій підприємства. TOGAF - це підхід високого рівня до дизайну. Зазвичай він моделюється на чотирьох рівнях: бізнес, додатки, дані та технологія. Він значною мірою покладається на модуляризацію, стандартизацію та вже існуючі, перевірені технології та продукти.


TOGAF був розроблений з 1995 року Open Group на базі стандартів Міністерства оборони Сполучених Штатів та Інтегрованої архітектурної системи Капгеміні (IAF). Станом на 2016 рік The Open Group стверджує, що в TOGAF працюють 80% компаній Global 50 та 60% компаній Fortune 500.



# МЕТОДОЛОГІЯ ЗЕРДЕ

На базі TOGAF національним телекомунікаційним холдингом Зерде в Республіці Казахстан була створена відповідна методологія цифрової трансформації, що стала обов'язковим елементом проведення цифровізації органів державної влади.





# ПЕРЕВАГИ ВІД ВПРОВАДЖЕН НЯ ЄДИНОГО АРХІТЕКТУРНО ГО ПІДХОДУ

---

Можливість вертикального прослідковування будь-яких потреб ІТ та інформаційної безпеки з рівня законодавства

---

Системний опис та оптимізація ключових бізнес-процесів

---

Наявність єдиних державних вимог

---

Горизонт планування до 30 років

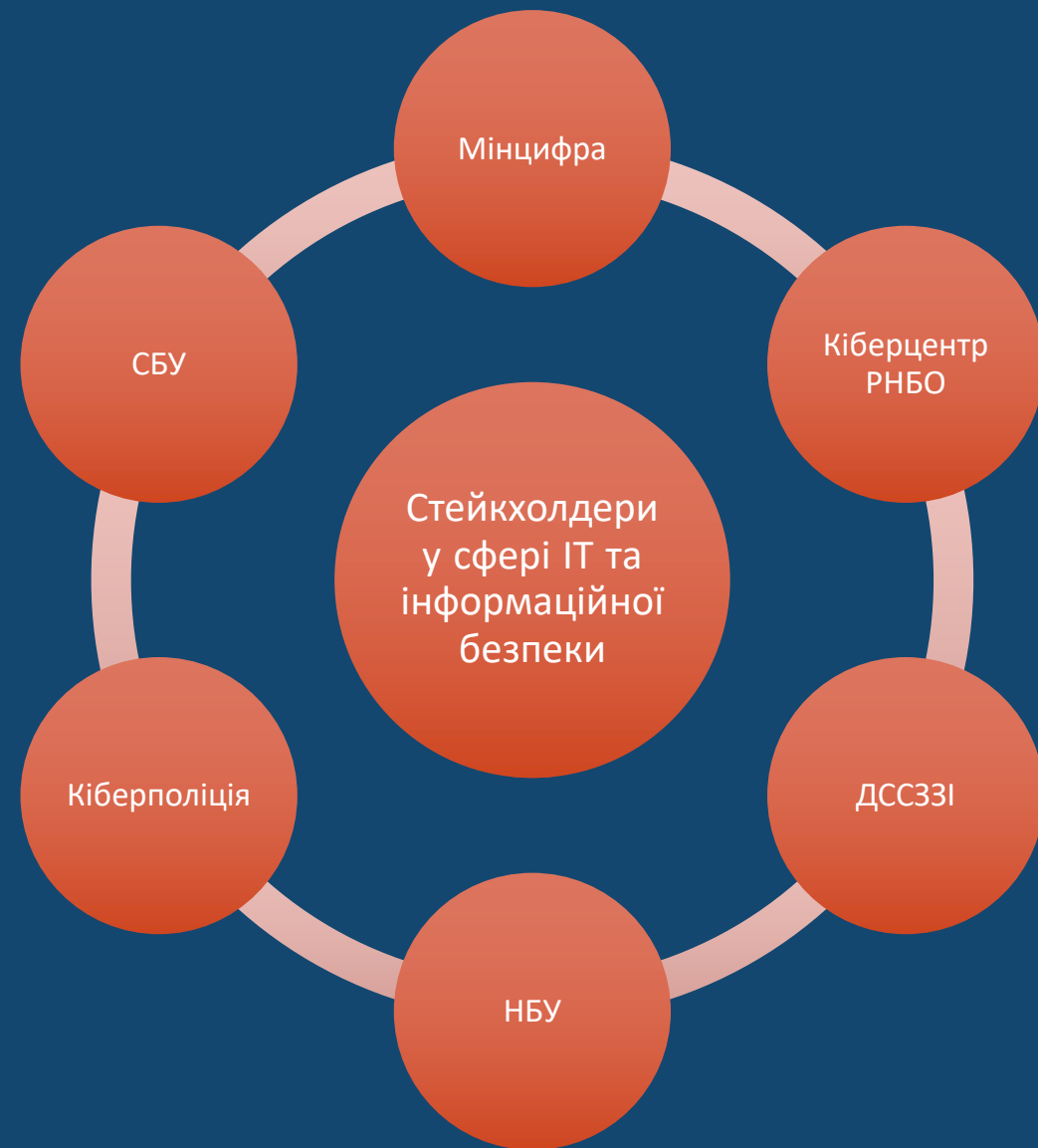
---


Виключення дублювання будь-яких дій та процесів

---

Комплексний погляд на потреби державних органів

# КЛЮЧОВІ СТЕЙКХОЛДЕРИ УПОВНОВАЖЕН І ДЕРЖАВОЮ






## НЕВИЗНАЧЕННІСТЬ ТА НЕУЗГОДЖЕННІСТЬ ОСНОВНИХ ТЕРМІНІВ

Не визначено такі терміни (перелік не повний):

- Інформаційна безпека
- Кібербезпека (її співвідношення з інформаційною безпекою)
- Ризик інформаційної безпеки
- Конфіденційність, цілісність та доступність інформації
- Аудит інформаційної безпеки



# ОСНОВНІ ДОКУМЕНТИ

Перелік основних нормативно-правових документів, що регламентують питання у сфері інформаційної безпеки та ІТ(1/4):

- Законом України «Про інформацію»;
- Законом України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Законом України «Про захист персональних даних»
- Законом України «Про електронні довірчі послуги»
- Закон України «Про основні засади забезпечення кібербезпеки України»
- Закон України «Про НБУ»
- Закон України «Про банки і банківську діяльність»
- Указ Президента України від 7 червня 2016 року № 242 «Про Національний координаційний центр кібербезпеки»
- Указ Президента України від 22 травня 1998 року № 505 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні»

# ОСНОВНІ ДОКУМЕНТИ

Перелік основних нормативно-правових документів, що регламентують питання у сфері інформаційної безпеки та ІТ (2/4):

- ПКМУ №1772 від 16.11.2002 Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах
- ПКМУ №1433 від 10.09.2003 Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади
- ПКМУ №373 від 29.03.2006 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах
- Наказ Держспецзв'язку №288 від 19.10.2011 Про затвердження Порядку погодження призначення на посади керівників органів спеціального зв'язку, підрозділів з питань зв'язку, інформатизації та захисту інформації органів державної влади, Національного банку України і Генеральної прокуратури України
- Наказ Держспецзв'язку №45 від 26.03.2007 Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації
- ПКМУ №869 від 12.08.2009 Про затвердження загальних вимог до програмних продуктів, які закуповуються та створюються на замовлення державних органів
- ПКМУ від 04 лютого 1998 року № 121 «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації» (у редакції постанови Кабінету Міністрів України від 11 листопада 2009 р. № 1191)

# ОСНОВНІ ДОКУМЕНТИ

Перелік основних нормативно-правових документів, що регламентують питання у сфері інформаційної безпеки та ІТ (3/4):

- Наказ Мініюсту № 1886/5 від 11.11.2014 Про затвердження Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання
- ПКМУ №326 від 17.03.2004 Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів.03.2004
- ПКМУ №357 від 10.05.2018 Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів
- Наказ Держагенства з електронного урядування № 51 від 13.18.2018 Про затвердження форматів електронних повідомлень та обміну даними системи електронної взаємодії державних електронних інформаційних ресурсів
- ПКМУ №606 від 08.09.2016 Деякі питання електронної взаємодії державних електронних інформаційних ресурсів
- ПКМУ №522 від 12.04.2002 Про затвердження Порядку підключення до глобальних мереж передачі даних.
- УПУ №891/2001 від 24.09.2001 Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних
- Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 липня 2007 року № 141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації»

# ОСНОВНІ ДОКУМЕНТИ

Перелік основних нормативно-правових документів, що регламентують питання у сфері інформаційної безпеки та ІТ (4/4):

- Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19.06.2019 №518
- Наказ Держагенства з електронного урядування №35 від 14.05.2019 Про затвердження Методики визначення належності бюджетних програм до сфери інформатизації
- Закону України «Про санкції»;
- Наказ Адміністрації Держспецзв'язку від 10.04.2008 р. № 94 «Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»
- Наказ Адміністрації Держспецзв'язку від 17.03.2014 р. № 115 «Про затвердження Положення про порядок визначення переліку технічних засобів, які можуть застосовуватися в телекомунікаційних мережах загального користування України, та погодження застосування засобів телекомунікацій, не внесених до цього переліку»,
- Наказ Адміністрації Держспецзв'язку від 02.12.2014 р. № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»,
- Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14 «Про затвердження документів у сфері захисту персональних даних»





Ключовою проблемою в інформаційній безпеці держави є те, що відстуня відповідальність за невиконання вимог законодавства в сфері ІБ та неінформування про можливі кібератаки



Михайло Чайкін

+380931514514

[mchaikin@outlook.com](mailto:mchaikin@outlook.com)