HLD як стратегія IT та ІБ «на мінімалках»

У міру зростання бізнесу рано чи пізно постає потреба впорядкувати IT-господарство і перейти до планомірної побудови інфраструктури. Тут у пригоді стане високорівневий дизайн — HLD.

У більшості компаній, які не мали великого стартового капіталу, IT-інфраструктура формується не як результат єдиного архітектурного плану, а «еволюційним» шляхом — поступово, хаотично та під впливом поточних бізнес-потреб. На початкових етапах це виглядає логічним: компанія росте, з'являються нові співробітники, офіси, сервіси та задачі, а IT адаптується до них у міру необхідності. Проте з часом така модель розвитку починає створювати системні проблеми.

Очевидно, що на ранніх етапах розвитку компанії дуже складно передбачити, чи буде взагалі зростання, чи зможе керівництво виділяти відповідні ресурси на IT та інформаційну безпеку. В таких випадках керівництво часто намагається мінімізувати інвестиції в IT– та ІБ-інфраструктуру та живе за принципом «якщо можна не купувати, то краще не купувати». До певного часу така стратегія може працювати. Наступним етапом є «латання дірок», тобто впровадження рішень та технологій, які критично необхідні і без яких бізнес не може розвиватись або несе надто великі ризики.

Наприклад, у стартапі користуються тим, що в кого є, і кожен працює на власному ноутбуці. Наступний етап — розуміння, що якимось чином всіма такими системами потрібно керувати, перехід на певний корпоративний стандарт і початок видачі корпоративних пристроїв. І вже на останньому етапі, коли компанія має значний прибуток, вона переходить до використання преміальних систем на кшталт Dell Latitude або MacBook з централізованим управлінням через EMM.

Якщо перекласти такий реактивний підхід на всю інфраструктуру, то часто маємо, як приклад, наступні рішення:

- новий сервер «тимчасово» додається до існуючої мережі;
- додатковий VPN запускається без загальної концепції доступу;
- Wi-Fi, комутатори чи маршрутизатори закуповуються за принципом «що було доступно»;
- хмарні сервіси підключаються різними підрозділами незалежно один від одного;

● партнери рекомендують те, що їм вигідно продати, без розуміння загальної картини.

В результаті з часом інфраструктура перетворюється на набір слабко пов'язаних між собою компонентів, які важко адмініструвати та інтегрувати між собою, що згодом веде до необхідності часткової або повної зміни всього IT– та ІБ-ландшафту.

Створення стратегій

Класичний підхід до розвитку IT та інформаційної безпеки передбачає формування повноцінної довгострокової стратегії. Такі документи зазвичай включають детальний аналіз поточного стану, оцінку ризиків, фінансові моделі, дорожню карту (roadmap) розвитку на декілька років, governance-процеси, KPI, моделі зрілості та комплексну цільову архітектуру.

Подібні проєкти є нормою для великих компаній (enterprise), банків, телеком-операторів або міжнародних корпорацій, де над створенням стратегії можуть протягом декількох місяців працювати окремі команди консультантів, архітекторів та аудиторів.

В Україні для малого та середнього корпоративного сегменту (500–2000 співробітників) формування довгострокової стратегії, ще і в наш час, є занадто дорогою та тривалою справою, а результат виконується навіть менш ніж на 50% через постійні зміни в технологіях, трансформації у самому бізнесі, кризові ситуації та непевне майбутнє. Іноді складно планувати навіть на рік, не кажучи вже про три або п'ять. В таких умовах компанії часто взагалі відмовляються від будь-якого стратегічного планування IT, залишаючись у режимі «реактивного» розвитку інфраструктури, що, звісно, може вирішити деякі поточні завдання, але не майбутні.

HLD як ефективна заміна стратегії

Для швидкого формування загального бачення IT- та ІБ-інфраструктури можна використовувати документ під назвою HLD (High Level Design) або

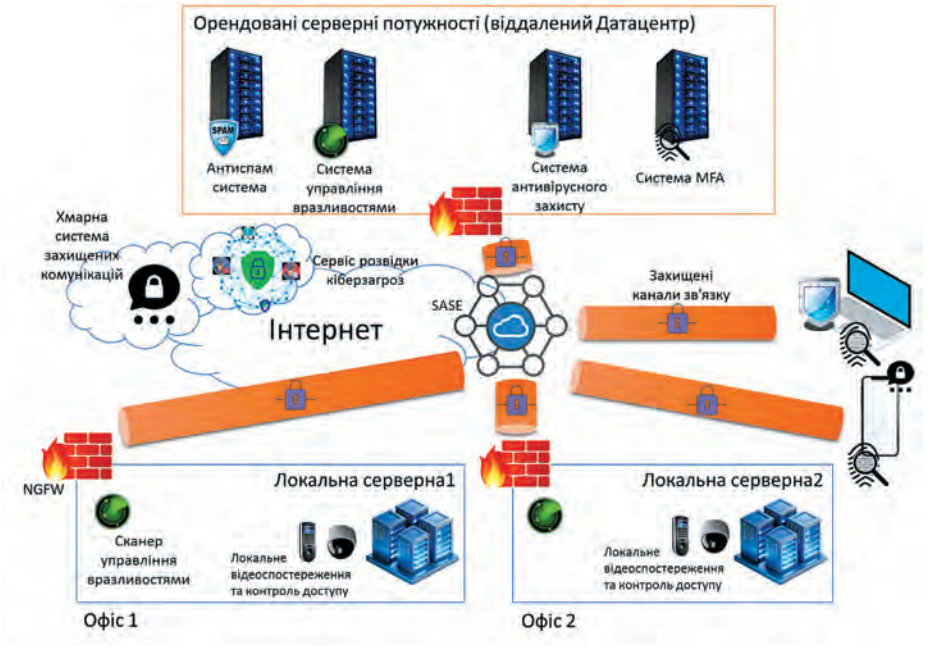

Рис. Приклад HLD з інформаційної безпеки

високорівневий дизайн інфраструктури. HLD — це опис архітектури інфраструктури IT та інформаційної безпеки, систем та сервісів, який визначає загальну концепцію побудови IT-ландшафту, його основні компоненти, взаємозв'язки та напрямок розвитку (**рис.**).

Простими словами, HLD — це «карта» або «стратегічний план» IT та ІБ, який містить відповіді на такі питання:
- що є зараз;
- що саме будується;
- як це повинно виглядати в цілому;
- які компоненти використовуються;
- як вони взаємодіють між собою;
- куди рухатиметься інфраструктура в майбутньому.

Основна користь HLD в тому, що документ описує можливий розвиток інфраструктури як єдиного організму з урахуванням взаємодії різних систем IT та безпеки, починаючи з критичної фізичної інфраструктури та закінчуючи процесами управління.

Стратегія vs HLD

Попри схожість, HLD та повноцінна IT-стратегія виконують різні завдання та мають різний рівень деталізації. IT-стратегія зазвичай фокусується на бізнес-рівні та описує довгострокові цілі розвитку компанії, цифрову трансформацію, фінансове планування, підходи до управління IT, організаційні зміни та показники ефективності. Такий документ часто формується на рівні топменеджменту та має прямий зв'язок із загальною бізнес-стратегією компанії.

HLD, у свою чергу, більше концентрується на технічній та архітектурній частині. Він описує, як саме повинна виглядати інфраструктура, які технології та сервіси використовуються, як взаємодіють між собою системи, яким чином забезпечується інформаційна безпека та в якому напрямку повинна розвиватися IT-архітектура.

Фактично HLD можна розглядати як технічний фундамент або практичний рівень реалізації IT-стратегії. Якщо остання відповідає на питання «навіщо компанії потрібні певні зміни», то HLD пояснює, «як це повинно бути реалізовано на рівні інфраструктури та систем».

Для компаній середнього бізнесу та невеликих державних організацій базовий HLD часто стає реалістичною альтернативою складній та дорогій IT-стратегії, дозволяючи отримати керовану модель розвитку без багатомісячних консалтингових проєктів.

Приклади реальних проєктів:
- стратегія розвитку IT для Національного Банку Казахстану (разом з Маккензі) — 500+ сторінок тексту,

$2 млн вартості для замовника та півроку роботи команди. Розрахована на 5 років з детальним описом бізнес-процесів;
- створення HLD до 100 сторінок залежно від складності може коштувати максимум пару десятків тисяч доларів та потребувати до місяця роботи команди. Результат — документ, розрахований на 2 роки, з загальним описом проєктів, систем, пріоритетів та вартості.

Симптоми того, що компанії вже потрібен HLD

У більшості випадків компанії замислюються над HLD не на етапі активного зростання, а тоді, коли інфраструктура вже починає створювати проблеми для бізнесу. Найчастіше це відбувається поступово: окремі «тимчасові» рішення накопичуються роками, IT-середовище ускладнюється, а керованість інфраструктури знижується.

1. Відсутність цілісного розуміння поточного стану IT
Компанія не має актуальних схем мережі, інвентаризації систем або документації, а значна частина знань існує лише «в голові» окремих адміністраторів чи підрядників. Будь-які зміни починають супроводжуватися ризиком простою або непередбачуваних наслідків.

2. Хаотичне впровадження нових рішень
Системи купуються під окремі завдання або інциденти без єдиного бачення архітектури. У результаті з'являється велика кількість слабо інтегрованих між собою сервісів, систем з дублюванням функцій або, навпаки, з їх нестачею.

3. Проблеми в інформаційній безпеці
Організація може мати окремі засоби захисту — наприклад, антивірус та мережеві екрани, — але не розуміти, як саме вони повинні працювати разом. Відсутність сегментації, централізованого управління доступами, резервування, інтеграції та стандартизації поступово збільшує ризики компрометації та ускладнює підтримку інфраструктури.

4. Складність масштабування бізнесу
Безкоштовне або дешеве добре працює для десятка людей, але не завжди добре — для тисячі з розподіленою інфраструктурою та складними процесами. Мережа на «домашніх» маршрутизаторах Wi-Fi може якось працювати для п'яти локацій, але вже для двадцяти вона перетворюється на некеровану інфраструктуру, яку потрібно постійно підтримувати вручну з критичними ризиками безпеки. Використовуючи підходи стартапу, IT-команда починає докладати непропорційно великих зусиль для відкриття нового офісу чи підрозділу. Принцип «давайте тут ще причепимо на скотч» в перспективі призводить до абсолютної неконтрольованості та неоптимальності.

5. Постійний «режим пожежогасіння»
Замість планового розвитку IT-команда переважно займається вирішенням поточних проблем. У такій ситуації більшість ресурсів витрачається на підтримку історично накопичених рішень, а не на побудову стабільної та прогнозованої архітектури.

На практиці HLD стає потрібним саме в той момент, коли компанія усвідомлює, що подальший хаотичний розвиток інфраструктури починає коштувати дорожче, ніж створення системного підходу до IT та інформаційної безпеки.

Що повинно входити в HLD

Склад HLD може суттєво відрізнятися залежно від масштабу компанії, галузі, рівня зрілості IT та вимог до інформаційної безпеки, а також цілей самої компанії. Наприклад, отримання ISO27001 або прагнення виходу на західні ринки суттєво вплинуть на майбутню інфраструктуру та дорожню карту проєктів. Навіть у спрощеному форматі HLD повинен формувати цілісне бачення інфраструктури, її поточного стану, цільової моделі та напрямків розвитку.

Фактично HLD можна розділити на три основні частини:
1. Як є зараз.
2. Як має бути.
3. Як потрапити в це «світле майбутнє».

Основою створення бачення на перспективу завжди є аналіз поточної ситуації. Отже, перший головний розділ — це опис поточної інфраструктури і її проблем. Відповідно до бажання або необхідності замовника додається опис певних рівнів «піраміди інфраструктури». Ось перелік можливих рівнів:
- критична фізична інфраструктура (живлення, серверні кімнати, кабельна мережа);
- фізична цифрова безпека (відеонагляд, системи контролю доступу);
- мережева інфраструктура;
- кінцеві пристрої (робочі станції, смартфони, серверна інфраструктура);
- системи друку та мультимедіа;
- операційні системи та віртуалізація;
- хмарна інфраструктура;
- додатки (застосунки);
- додаткові рівні інфраструктури (написання коду, ОТ, інші);
- дані та процеси;
- інформаційна безпека.

Інформаційна безпека є важливим і великим підрозділом, але вона іде як останній шар інфраструктури, як «ковдра», що накриває IT-інфраструктуру. Очевидно, що інформаційна безпека залежить від IT-інфраструктури, процесів та цілей організації і не може в рамках HLD розглядатися окремо. Саме тому HLD в повному обсязі настільки корисний: він дає повну картину безпеки з прив'язкою до IT-інфраструктури.

Другим великим розділом є відповідно бачення цільової архітектури. Він майже дублює попередній по підрозділах і описує, яким чином має бути оптимально побудована вся інфраструктура як єдиний механізм для виконання поставлених бізнес-завдань та з можливістю легкого масштабування.

Саме цей розділ описує, як виглядатиме IT-ландшафт в майбутньому: які технології використовуються, які системи централізуються, що переноситься у хмару, що докуповується, які системи мають працювати та як зміняться процеси.

Наступною важливою частиною HLD є архітектура інформаційної безпеки. У цьому блоці описуються основні

підходи до захисту інфраструктури: фізична цифрова безпека, захист мережі, захист кінцевих точок, MFA, резервне копіювання, логування, управління вразливостями, PAM, захист пошти, віддалений доступ та інші компоненти архітектури безпеки. При цьому HLD зазвичай не описує детальні налаштування рішень, а визначає їхню роль та місце в загальній архітектурі. Всі технології та компоненти безпеки підібрані таким чином, щоб максимально спростити управління та автоматизувати адміністрування, враховуючи всі переваги та недоліки рішень й максимально посилюючи ефект «симбіозу» в інфраструктурі.

Останнім важливим компонентом є roadmap розвитку — поетапний план реалізації цільової архітектури. У ньому визначаються пріоритети проєктів, послідовність впровадження рішень, залежності між компонентами та приблизні етапи розвитку інфраструктури. Саме roadmap дозволяє перетворити HLD із «теоретичного документа» на практичний інструмент розвитку IT.

Приклад: очевидно, що не можна побудувати мережу зв'язку, не маючи кросових приміщень або хоча б телекомунікаційних шаф та кабельної (бажано структурованої) системи.

Що HLD дає бізнесу

У багатьох компаніях HLD помилково сприймається виключно як «технічний документ для IT». Насправді його основна цінність полягає саме у бізнес-площині. HLD дозволяє компанії перейти від хаотичного розвитку інфраструктури до керованої та прогнозованої моделі розвитку IT та інформаційної безпеки.

1. Розуміння поточного стану IT
HLD дозволяє сформувати цілісне бачення існуючої інфраструктури, її компонентів, взаємозв'язків та критичних залежностей. Компанія починає краще розуміти, які системи є критичними для бізнесу, де знаходяться слабкі місця та які елементи інфраструктури вже створюють ризики або технічний борг.

2. Формування цільової моделі
HLD визначає, як повинна виглядати інфраструктура в майбутньому з урахуванням потреб бізнесу, масштабування та вимог безпеки. Це дозволяє перейти від хаотичного розвитку до системного підходу, де всі нові рішення впроваджуються в межах єдиної архітектурної концепції.

3. Планування розвитку інфраструктури
Наявність HLD дозволяє будувати roadmap розвитку IT та реалізовувати зміни поетапно, без постійного «гасіння пожеж». Компанія отримує розуміння, які проєкти необхідно виконувати першочергово, а які можуть бути реалізовані пізніше в рамках довгострокового розвитку.

4. Пріоритезація інвестицій
HLD допомагає інвестувати в ті компоненти інфраструктури, які дійсно мають найбільший вплив на стабільність, безпеку та розвиток бізнесу. Це дозволяє уникати хаотичних закупівель, дублювання рішень та витрат на технології, які не вписуються в цільову архітектуру.

5. Спрощення масштабування
Коли інфраструктура побудована за єдиними принципами, відкриття нових офісів, інтеграція нових сервісів та збільшення кількості користувачів стають значно простішими. HLD створює основу для прогнозованого зростання компанії без необхідності постійно перебудовувати IT «з нуля».

Компетенції, необхідні для створення HLD

Попри поширену думку, створення HLD — це не виключно технічна задача. Якісний HLD знаходиться на перетині архітектури, інформаційної безпеки, бізнес-аналізу та практичного досвіду експлуатації інфраструктури. Саме тому для його створення недостатньо лише знання окремих технологій або вміння малювати схеми.

Однією з ключових компетенцій є системне розуміння IT-інфраструктури. Архітектор повинен бачити не окремі компоненти, а взаємозв'язки між мережами, серверами, хмарними сервісами, користувачами, системами безпеки та бізнес-процесами. HLD завжди працює на рівні всієї екосистеми компанії, а не окремих технологій.

Не менш важливим є досвід у сфері інформаційної безпеки. Сучасну архітектуру вже не можна будувати без урахування підходу security-by-design. Спеціаліст, який створює HLD, повинен розуміти принципи інформаційної безпеки та добре орієнтуватися в рішеннях.

Нарешті, одна з найважливіших компетенцій — вміння знаходити баланс між «ідеальною архітектурою» та реальністю бізнесу. Хороший HLD не намагається побудувати преміум enterprise-рівень для кожної компанії. Його завдання — створити реалістичну, масштабовану та керовану модель розвитку IT та інформаційної безпеки в межах можливостей конкретного бізнесу.

Висновки

У сучасних умовах HLD поступово перестає бути атрибутом виключно великих компаній і стає практичним інструментом керованого розвитку IT та інформаційної безпеки для бізнесу будь-якого масштабу. Навіть базовий високорівневий опис архітектури дозволяє знизити хаос, краще контролювати ризики, планувати розвиток інфраструктури та впроваджувати безпеку системно, а не реактивно. У світі, де IT вже напряму впливає на стабільність, безперервність роботи та конкурентоспроможність компанії, HLD стає не «додатковою документацією», а фундаментом для прогнозованого та безпечного розвитку бізнесу.

Олексій ЗАЙОНЧКОВСЬКИЙ,
архітектор рішень
інформаційної безпеки та IT, vCISO
+380 (63) 585 7307,
Threema ID: B8X9K2NC