

# Екранований МЦОД:



## максимальна безпека та мобільність для захисту інформації

Модульні дата-центри давно й успішно використовуються для розгортання та підтримки бізнес-критичних сервісів по всьому світу. Але, щоб МЦОД був дійсно надійним та захищеним, треба враховувати велику кількість деталей.

**В**перше концепцію дата-центру в контейнерному виконанні представила компанія Sun Microsystems, відбулося це ще 2006 року. Дуже швидко ідею підхопили й інші світові ІТ-виробники: зокрема Dell, IBM, HP тощо. Поступово з року в рік усе більше замовників, серед яких промислові підприємства і фінансові установи, віддавали перевагу МЦОДам. В результаті сьогодні рішення такого класу – це не просто контейнер з обладнанням, а високотехнологічний комплекс, зібраний і протестований на заводі-виробнику, який гарантує безперебійну роботу всіх інженерних систем і надійний захист інформації. На сьогодні в Україні розгорнуто вже понад два десятки модульних центрів обробки даних, але всі вони різні і побудовані під індивідуальні потреби замовників. Серед цих дата-центрів особливо вирізняються своєю специфікою екрановані МЦОДи. Експерти компанії IT-Solutions готові поділитися їх характерними відмінностями.

“ У поточних умовах, коли багато замовників повністю зупиняють проєкти з розвитку ІТ-інфраструктури, а деякі компанії концентрують зусилля лише на підтримці своїх систем та економлять бюджети, є й ті, хто дійсно думає про майбутнє, інвестуючи у безпечні захищені рішення, що відповідають вимогам часу”.

**Вікторія Чучина,**  
директор з маркетингу і продажів IT-Solutions

### Основні замовники, хто вони?

Банківські установи, державні структури, а також компанії, які відповідально працюють з конфіденційною і сенситивною інформацією, мають високі вимоги до систем безпеки своїх дата-центрів, які, серед іншого, регулюються нормативними документами Національного банку України, Мін'юсту або Держспецзв'язку. Всі вони покликані гарантувати цілісність і захищеність даних та обладнання інформаційних систем від руйнувань чи пошкоджень. Зокрема, серверні приміщення і дата-центри українських банків мають відповідати вимогам Національного банку України (Постанова №243 від 04.07.2007р.), а також відповідати міжнародним стандартам безпеки ISO 27001, PCI DSS та іншим.

### Від чого захищає екранований МЦОД?

В екранованих МЦОД конфіденційна інформація і обчислювальне обладнання захищені від зовнішнього деструктивного впливу електромагнітного випромінювання і полів, які можуть бути як природного, так і техногенного

походження. Крім того, не слід виключати ризики умисного впливу на працююче ІТ-обладнання потужним направленим імпульсним випромінюванням, яке може призвести до збоїв у його роботі і навіть виходу з ладу.

### Основні принципи захисту

Відомо, що безпека будь-якого об'єкта залежить від рівня захищеності його найслабшого місця. Тому концепція модульного дата-центру передбачає, що вже на етапі виробництва конструкції закладаються всі необхідні рівні захисту. Формфактор контейнера дозволяє реалізувати так звану клітку Фарадея – замкнену металеву конструкцію, яка виготовлена з електропровідного матеріалу. Така клітка не дозволяє потрапляти зовнішнім електричним і електромагнітним полям всередину конструкції.

Крім того, контейнерна конструкція є всепогодною і передбачає її транспортування і вуличне розміщення. В процесі облаштування екранованого МЦОД його конструкція оснащується обладнанням інженерних систем і засобами безпеки. Дата-центр підключається до зовнішніх мереж електроживлення і зв'язку. Відповідно всі комунікації вводяться в екранований МЦОД через фільтри і інші захисні елементи екрану (протизавадні і феромагнітні фільтри, екрановані двері, вентиляційні решітки тощо).

За результатами проведених робіт перед введенням в експлуатацію кожного екранованого МЦОДа проводиться приладова перевірка ефективності його екранування. Контроль параметрів здійснюється лабораторіями, які мають відповідну ліцензію Держспецзв'язку, потрібне обладнання і підготовлених фахівців. Періодичність такої перевірки складає раз на п'ять років.

### Відповідність стандартам

Екранування МЦОД відповідає вимогам комплексної системи захисту інформації (КСЗІ) НД ТЗІ 3.7-001-99, а саме створення комплексної системи безпеки інформації з урахуванням необхідності обробки інформації з обмеженим доступом. Валерій Яцківський, керівник відділу інформаційної безпеки, зазначає, що IT-Solutions здійснює супровід державної експертизи КСЗІ ІТС до моменту отримання Атестату відповідності. Зокрема, експертиза являє собою один із найважливіших етапів створення КСЗІ та передуює введенню КСЗІ в експлуатацію.



За матеріалами компанії **IT-Solutions**  
[www.it-solutions.ua](http://www.it-solutions.ua)