ГНУЧКІ СКЛАДОВІ НАДІЙНОСТІ ІТ-СИСТЕМИ

Добровольський Ю.Г., Прохоров Г.В., Ганжело Д.В.
Чернівецький національний університет імені Юрія Федьковича, м. Чернівці

Надійність ІТ-системи – це здатність системи адаптуватися і відновлюватися після деструктивних подій, таких як апаратні або програмні збої, кібератаки, перебої в подачі електроенергії або стихійні лиха без порушення нормальної роботи бізнесу. Вона включає проектування, впровадження та обслуговування ІТ-систем, щоб гарантувати, що вони можуть витримувати збої та відновлюватися після них, а також продовжувати надавати основні послуги клієнтам та зацікавленим сторонам.

Структура надійності ІТ-систем включає кілька рівнів захисту, зокрема надмірність, механізми аварійного перемикання, процеси резервного копіювання і відновлення, а також планування аварійного відновлення. Забезпечуючи стійкість ІТ-систем, організації можуть знизити ризик простоїв, втрати даних та шкоди репутації, зберігаючи при цьому безперервність бізнесу та задовольняючи вимоги клієнтів.

Стійкість ІТ-системи складається з різних компонентів, які працюють разом для забезпечення здатності системи відновлюватись після руйнівних подій. Деякі з ключових компонентів стійкості ІТ-системи включають:

1. Надмірність: наявність кількох систем, пристроїв або мереж, які можуть взяти на себе керування у разі відмови одного або кількох компонентів.

2. Механізми аварійного перемикання: автоматизовані процеси, які перемикаються на резервну систему або пристрій у разі збою основної системи або пристрою.

3. Процеси резервного копіювання та відновлення: регулярне резервне копіювання даних та систем, а також процедури їх швидкого та точного відновлення у разі збою чи збою.

4. Планування аварійного відновлення: стратегії, процедури та ресурси для реагування та відновлення після великих збоїв, таких як стихійні лиха чи кібератаки.

5. Моніторинг та оповіщення: інструменти та процеси, які відстежують продуктивність та доступність ІТ-систем та попереджають ІТ-персонал про потенційні проблеми чи збої.

6. Безпека та відповідність: заходи щодо захисту ІТ-систем від кіберзагроз та забезпечення відповідності нормативним вимогам.

7. Тестування та перевірка: регулярне тестування механізмів стійкості, щоб переконатися, що вони працюють належним чином та можуть забезпечити необхідний рівень захисту.

Кожен з вищезгаданих компонентів має свою вагу, ціну і конфігурацію. Гнучко комбінуючи ці компоненти, організації можуть створювати стійкі до відмови ІТ-системи, здатні протистояти збоям і продовжувати надавати необхідні послуги клієнтам.