

## **ЗАХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СЕРВЕРНИХ ПРИМІЩЕНЬ**

На сьогоднішній день актуальним є питання забезпечення захисту серверних приміщень, так як вони містять важливу інформацію, і її втрата цієї інформації може понести за собою великі втрати.

Безпека серверної кімнати починається з контролю доступу до неї. Картки доступу, біометричні і навіть звукові методи - це загальноприйняті методи, які використовують для обмеження доступу, однак ці методи є первинними і не можуть стовідсотково гарантувати безпеку. Картки, паролі можуть потрапити не в ті руки, а біометричні пристрої досить дорогі і можуть помилково не спрацювати на доступ в серверну навіть для тих осіб, яким він дозволений.

Ці заходи можна значно підсилити: наприклад, встановити камери відеоспостереження, фізичну охорону або контактні сенсори. За допомогою комбінування різних методів можна досягнути максимізацію безпеки.

З моменту планування фізична інфраструктура об'єкта повинна сприяти безпеці всього комплексу. Непогано, якщо матеріал стін, стель і підлоги добре захищає приміщення. Якщо вікна чи двері не дозволяють гарантувати безпеку від крадіжок або диверсії конкурентів, потрібно терміново вирішити цю проблему.

На додаток до заходів щодо забезпечення безпеки внутрішньої мережі, необхідно забезпечити фізичний захист і захист мережевого устаткування. Навіть всередині серверної кімнати безпека серверної стійки і встановленого в юнітах обладнання повинна бути максимально можливою. Замки на стійці обмежать доступ сторонніх осіб, захистять від навмисних або випадкових дотиків.

Кожен об'єкт характеризується своїми власними вимогами щодо безпеки. Розробляючи план безпеки для свого серверного приміщення потрібно уважно оцінити всі ризики. Потрібно знайти прийнятний компроміс між безпекою та її вартістю. Комбінуючи можливі ризики з аналізом доступних технологій і вимогам до доступу, цілком реально знайти прийнятне, ефективне рішення.

*Науковий керівник – д.т.н., проф., В.В. Козловський*