

Микола Трофименко

ЗАХИСТ СЕРВЕРІВ І ДАНИХ - ЯК ЗАБЕЗПЕЧИТИ БЕЗПЕРЕРВНІСТЬ НАВЧАННЯ В УНІВЕРСИТЕТАХ

Звертаюся до керівників закладів вищої освіти: захист серверів, університетських даних і навчальних платформ має бути нині серед першочергових завдань підготовки до осінньо-зимового періоду.

Російські обстріли та перебої з електропостачанням загрожують роботі цифрової інфраструктури університетів. Пошкодження серверного обладнання може позбавити тисячі студентів доступу до навчальних матеріалів, завдань і результатів оцінювання, а викладачів – можливості проводити заняття та підтримувати зв'язок зі студентами.

Прошу керівників ЗВО разом з ІТ-командами перевірити готовність закладів до таких ситуацій і визначити, що необхідно зробити насамперед.

Захистити обладнання. Оцінити розміщення серверів, систем зберігання даних і мережевого обладнання. Де це технічно можливо – організувати їх перенесення до придатних підземних або інших захищених приміщень. Таке рішення потребує належного електроживлення, охолодження, вентиляції, захисту від вологи та пожежної безпеки. Обладнання не повинно займати місця, призначені для укриття людей, або перешкоджати евакуації.

Забезпечити резервування даних і сервісів. Актуальні копії навчальних матеріалів, баз даних, результатів оцінювання та налаштувань систем потрібно зберігати окремо від основних серверів. Резервна копія в тому самому приміщенні залишається вразливою до того самого удару чи аварії. Варто передбачити інший майданчик або захищене хмарне середовище, а для критичних сервісів – резервні ресурси, на яких можна відновити їхню роботу.

Підготувати автономне живлення та зв'язок. Визначити, які системи мають працювати першочергово під час знеструмлення, на скільки часу вистачає резервного живлення та як заклад діятиме після його вичерпання. Передбачити резервний доступ до інтернету для критичних сервісів.

Зберегти доступ до навчання. Перевірити, чи можуть викладачі завчасно завантажити лекції, завдання та інші матеріали, а студенти – працювати з ними без постійного підключення до мережі. Підготувати порядок продовження онлайн- та асинхронного навчання у разі недоступності основної платформи. Викладачі й студенти мають знати, де отримати матеріали, як передати виконані роботи та до кого звернутися по допомогу.

Перевірити план відновлення на практиці. Визначити відповідальних, порядок перемикавання на резервні ресурси та канали інформування університетської спільноти. Провести тестове відновлення даних: наявність копії ще не підтверджує, що з неї можна швидко відновити роботу.

Провести спеціальне навчання для студентів, викладачів та адміністративного персоналу щодо альтернативних способів доступу та використання цифрової інфраструктури університетів.

Це спільна робота керівництва, IT-підрозділів і команд, які організовують освітній процес. Прошу оцінити потреби в обладнанні та ресурсах, визначити строки виконання й завчасно повідомити засновника про питання, які заклад не може вирішити самостійно.

Наше завдання – зберегти університетські дані та забезпечити студентам можливість продовжувати навчання навіть у разі пошкодження окремих корпусів або тривалих відключень світла чи інтернету. До цього потрібно підготуватися завчасно.