Міністерство освіти і науки України

ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

імені Юрія Федьковича

НАКАЗ

«30» 12 2024 р. м. Чернівці № 477

Про затвердження плану дій
на випадок несанкціонованого доступу
до персональних даних у
Чернівецькому національному університеті
імені Юрія Федьковича

На виконання пунктів 2, 3 Припису № 72-24 про усунення порушення вимог законодавства у сфері захисту персональних даних, виявленого під час перевірки Представника Уповноваженого Верховної Ради України з прав людини від 03.12.2024 р.,

НАКАЗУЮ:

1. Затвердити «План дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання або виникнення надзвичайних ситуацій у Чернівецькому національному університеті імені Юрія Федьковича».
2. Довести цей наказ до відома проректорів, деканів факультетів, директорів інститутів, керівників структурних підрозділів університету.
3. Контроль за виконанням цього наказу залишаю за собою.

Ректор **Руслан БІЛОСКУРСЬКИЙ**

Проєкт наказу внесла:
Ганна ПОКЛІТАР, 871

ЗАТВЕРДЖЕНО
наказом ректора Чернівецького національного університету імені Юрія Федьковича
№ 771 від «28» 12 2024 р.

ПЛАН ДІЙ
на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання або виникнення надзвичайних ситуацій у Чернівецькому національному університеті імені Юрія Федьковича

Плані дій складається з комплексних заходів, спрямований на захист інформації, швидке реагування, мінімізацію можливих втрат та включає:

1. Реагування на несанкціонований доступ до персональних даних

1.1 Виявлення інциденту:

- моніторинг системи безпеки (виявлення підозрілих активностей у логах (журналах) доступу та повідомлення адміністратора безпеки);
- аналіз активності (визначення масштабу інциденту та ідентифікація джерела несанкціонованого доступу).

1.2 Оцінка та ізоляція:

- ізоляція уражених систем (негайне відключення скомпрометованих облікових записів або сервісів, щоб запобігти поширенню інциденту);
- перегляд доступу користувачів (аналіз рівнів доступу і тимчасове призупинення доступу до даних для користувачів, які можуть бути пов'язані з інцидентом).

1.3 Інформування та усунення:

- повідомлення зацікавлених осіб (ЦЦТ, юридичний відділ) та зовнішніх органів згідно з вимогами законодавства);
- усунення вразливостей (виправлення виявлених уразливостей, таких як слабкі паролі, відсутні оновлення, незахищені API тощо).

2. Реагування на пошкодження технічного обладнання

2.1 Виявлення та оцінка пошкодження:

- оцінка рівня пошкодження: (визначення впливу на роботу інформаційних систем та обсягів пошкоджених даних);

– ідентифікація пошкоджених компонентів.

2.2 Активізація резервних засобів

– активація резервних серверів або хмарних рішень;
– використання резервних копій (відновлення даних з резервних копій, якщо це необхідно.

2.3 Відновлення обладнання

– ремонт або заміна техніки (залучення технічної підтримки для ремонту чи заміни пошкодженого обладнання);
– перевірка відновлення системи (тестування відновленого обладнання на відповідність вимогам безпеки та функціональності).

3. Звітність та оновлення плану дій

– документування інциденту;
– внесення змін до плану дій для покращення готовності до подібних ситуацій у майбутньому.