Одеська національна музична академія імені А.В. Нежданової

ЗАТВЕРДЖЕНО
Вченою радою ОНМА
імені А.В. Нежданової
від 31 серпня 2023 року № 1

Голова Вченої ради, ректор

_____Олександр ОЛІЙНИК

План захисту інформаційних систем

Введено в дію Наказом
№84а від 11.09.2023 року

1 Адміністративний рівень забезпечення безпеки

- процедура доведення до відома співробітників основних положень концепції інформаційної безпеки, вимог із навчання персоналу правил інформаційної безпеки;
- система контролю за реалізацією прийнятих рішень та відповідальні особи.

2 Організаційний рівень забезпечення інформаційної безпеки

- організаційна структура служби, відповідальної за забезпечення режиму інформаційної безпеки, розподіл обов'язків;
- комплекс профілактичних заходів (попередження появи вірусів, попередження ненавмисних дій, що ведуть до порушення інформаційної безпеки);
- організація доступу співробітників сторонніх організацій до ресурсів інформаційних систем;
- організація доступу користувачів і персоналу до конкретних ресурсів інформаційних систем;

3 Технічний рівень забезпечення інформаційної безпеки

При розгляді різних варіантів рекомендується враховувати наступні аспекти:

- керування доступом до інформації й сервісів, включаючи вимоги до поділу обов'язків і ресурсів;
- перевірка й забезпечення цілісності критично важливих даних на всіх стадіях їхньої обробки;
- захист конфіденційних даних від несанкціонованого доступу, у тому числі використання засобів шифрування;
- резервне копіювання критично важливих даних;
- відновлення роботи інформаційних систем після відмов, особливо для систем з підвищеними вимогами до доступності;
- забезпечення засобів контролю, наприклад, за допомогою використання програми для вибіркового контролю й альтернативні варіанти програмного забезпечення для повторення критично важливих обчислень.

4 Забезпечення безперебійної роботи організації

У процесі планування безперебійної роботи організації розглядаються наступні питання:

- виявлення критично важливих процесів у роботі інформаційних систем;

- визначення можливого впливу аварій різних типів на роботу інформаційних систем;
- визначення й узгодження всіх обов'язків і планів дій у надзвичайних ситуаціях;
- планування підготовки персоналу до роботи в надзвичайних ситуаціях.

План забезпечення безперебійної роботи організації повинен включати:

- процедури реагування на надзвичайні ситуації, що описують заходи, які слід вжити відразу після збою в інформаційних системах, що може викликати небезпеку у роботі організації й/або порушення інформаційної безпеки;
- процедури переходу на аварійний режим, що описують заходи, які слід вжити для забезпечення безперебійної роботи закладу чи перенесення сервісів в інші місця;
- процедури поновлення роботи організації, що описують заходи, які слід вжити для поновлення нормальної виробничої діяльності організації;

Плани забезпечення безперебійної роботи організації необхідно обновляти при виникненні істотних змін. Такими змінами є:

- установка нового обладнання або модернізація функціонуючих систем;
- організаційні зміни;
- зміни у виробничих процесах;
- зміни в програмному забезпеченні.