ЗАТВЕРДЖЕНО

Розпорядження начальника
Чернігівської обласної
військової адміністрації
23 травня 2025 року № 707

План
дій на випадок несанкціонованого доступу до персональних даних,
пошкодження технічного обладнання, виникнення надзвичайних ситуацій

1. При виявленні ознак несанкціонованого доступу до автоматизованих систем Чернігівської обласної державної адміністрації (далі – обласна державна адміністрація), де обробляються персональні дані, таких як: несанкціоноване отримання даних про облікові записи користувачів, підбір паролів з застосуванням атак грубої сили необхідно:

*користувачам*

1) припинити обробку персональних даних в інформаційно-комунікаційній системі обласної державної адміністрації;

2) повідомити адміністратора безпеки в автоматизованих системах та особу, відповідальну за організацію роботи, пов’язаної із захистом персональних даних при їх обробці, володільцем яких є обласна державна адміністрація (далі – відповідальна особа);

*адміністратору безпеки* змінити паролі скомпрометованих облікових записів.

2. При виявленні зараження автоматизованих систем обласної державної адміністрації шкідливим програмним забезпеченням необхідно:

*користувачам*

1) припинити обробку інформації в автоматизованих системах;

2) повідомити адміністратора безпеки в автоматизованих системах обласної державної адміністрації;

3) повідомити безпосереднього керівника та відповідальну особу;

*адміністратору безпеки*

1) визначити тип та масштаб компрометації систем / мереж, що були уражені;

2) повідомити основних суб’єктів забезпечення кібербезпеки України;

3) ізолювати уражені системи, мережі, мережеві сегменти та пристрої;

4) забезпечити повне технічне усунення загрози та пов’язаної з нею зловмисної активності.

3. При відмові та/або збої програмного забезпечення, за допомогою якого здійснюється обробка персональних даних, необхідно:

1) припинити обробку персональних даних;

2) повідомити адміністратора безпеки в автоматизованих системах обласної державної адміністрації;

3) повідомити безпосереднього керівника та відповідальну особу.

4. У випадку виявлення несанкціонованого доступу до паперових баз персональних даних (справ, журналів) необхідно:

1) негайно припинити будь-яку роботу з документами;

2) обмежити доступ до паперових даних до отримання інструкцій від відповідальної особи щодо подальших дій;

3) повідомити безпосереднього керівника та відповідальну особу.

5. При вчиненні випадкових та/або помилкових дій, що можуть призвести до втрати, зміни, поширення, розголошення персональних даних тощо, необхідно:

1) припинити обробку персональних даних;

2) повідомити безпосереднього керівника та відповідальну особу.

6. У випадку виникнення надзвичайних ситуацій (пожежі, повені, стихійного лиха, воєнних дій тощо):

1) вжити невідкладних заходів щодо оповіщення відповідних служб реагування;

2) забезпечити збереження носіїв персональних даних від втрати та пошкодження (за наявної можливості та у спосіб, що не загрожує життю та здоров’ю);

3) повідомити безпосереднього керівника та відповідальну особу.

7. Відповідальна особа у разі загрози безпеці персональних даних та у разі виявлення порушення законодавства повідомляє про це голову Чернігівської обласної державної адміністрації (начальника Чернігівської обласної військової адміністрації) з метою вжиття необхідних заходів, зокрема, повідомлення правоохоронних органів за потреби.

Начальник організаційного відділу
апарату Чернігівської обласної
державної адміністрації Оксана СЕРДЮК