ЗАТВЕРДЖЕНО

Розпорядження голови

обласної державної адміністрації

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_\_\_

**ПЛАН**

**дій працівників апарату обласної державної адміністрації на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій**

1. При виявленні ознак несанкціонованого доступу до персональних даних, володільцем яких є апарат облдержадміністрації, таких як несанкціоноване отримання логінів і паролів, підбір паролів та ключів, працівник, який виявив ці ознаки, зобов'язаний негайно:

1.1. Припинити обробку персональних даних;

1.2. Повідомити відповідальних осіб, які організовують роботу, пов'язану із захистом персональних даних при їхній обробці в апараті облдержадміністрації (далі − відповідальні особи);

1.3. Звернутися до відповідної особи, на яку покладено функції з впровадження в апараті облдержадміністрації інформаційних технологій з метою блокування доступу до облікового запису;

1.4. Змінити паролі доступу (за наявності технічної можливості).

2. При виявленні зараження програмного забезпечення та носіїв інформації комп'ютерними вірусами працівник зобов'язаний:

2.1. Негайно припинити обробку персональних даних;

2.2. Вимкнути комп'ютерну техніку від електроживлення;

2.3. Повідомити керівника, який організує роботу, пов'язану із захистом персональних даних;

2.4. Повідомити відповідну особу, на яку покладено функції з впровадження в апараті облдержадміністрації інформаційних технологій.

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

3.1. Припинити обробку персональних даних;

3.2. Про всі події та факти повідомити керівника, який організує роботу, пов'язану із захистом персональних даних.

4. При відмові та/або збої програмного забезпечення, за допомогою якого здійснюється обробка персональних даних, працівник зобов'язаний:

4.1. Припинити обробку персональних даних;

4.2. Повідомити керівника, який організує роботу, пов'язану із захистом персональних даних;

4.3. Повідомити відповідну особу, на яку покладено функції з впровадження програмного забезпечення в апараті облдержадміністрації інформаційних технологій.

5. При виявленні пошкодження, втрати, викрадення документа або іншого носія персональних даних невідкладно повідомити керівника, який організує роботу, пов'язану із захистом персональних даних.

6. У разі виникнення надзвичайних ситуацій (пожежа, повінь, стихійні лиха тощо):

6.1. Вжити невідкладних заходів щодо оповіщення відповідних служб реагування;

6.2. Забезпечити збереження носіїв персональних даних осіб від втрати та пошкодження (за наявної можливості та у спосіб, що не загрожує життю та здоров'ю працівників);

6.3. Повідомити відповідальних осіб, які організовують роботу, пов'язану із захистом персональних даних.

7. Про всі випадки несанкціонованого доступу до персональних даних, передбачені пунктами 1−6 цього Плану, та/або інші випадки, що призвели до пошкодження, псування, несанкціонованого доступу, знищення, поширення тощо персональних даних, працівник, який виявив цей факт, та безпосередній керівник невідкладно письмово повідомляють про подію відповідальну особу.

7.1. Повідомлення реєструється відповідно до вимог Інструкції з діловодства у Львівській облдержадміністрації.

8. Після отримання повідомлення відповідальна особа складає акт про факт порушення процесу обробки та захисту персональних даних (далі − Акт).

8.1. Акт підписується відповідальною особою та працівником, яким виявлено (вчинено) це порушення.

8.2. Відмова від підпису працівника фіксується відповідно до вимог чинного законодавства.

8.3. Організація роботи, пов'язаної із захистом персональних даних при їхній обробці, тих володільців/розпорядників, на яких не поширюються вимоги частини другої статті 24 Закону України «Про захист персональних даних», покладається безпосередньо на тих осіб, які здійснюють обробку персональних даних.

8.4. Вимоги відповідальної особи до заходів щодо забезпечення безпеки обробки персональних даних є обов'язковими для всіх працівників, які здійснюють обробку персональних даних.

9. Підписаний Акт надається керівникові апарату облдержадміністрації або, в разі його відсутності, − посадовій особі, на яку покладено виконання його повноважень для прийняття рішення та повідомлення правоохоронних органів про несанкціонований доступ до персональних даних та вжиття відповідних заходів реагування.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_