ЗАТВЕРДЖЕНО

Наказ Головного управління статистики у Миколаївській області

14 серпня 2024 року № 63

ПЛАН

дій працівників Головного управління статистики у Миколаївській області на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій

1. При виявленні ознак несанкціонованого доступу до персональних даних, володільцем або розпорядником яких є Головне управління статистики у Миколаївській області (далі – ГУС у Миколаївській області), шляхом несанкціонованого отримання логінів і паролів, підбору паролів та ключів, працівник, який виявив дані ознаки, зобов'язаний негайно:

припинити обробку персональних даних;

негайно повідомити безпосереднього керівника, відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці (далі – відповідальна особа) та управління інформаційних технологій з метою блокування доступу до облікового запису та зміни паролю.

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

негайно припинити обробку персональних даних;

повідомити начальника (за відсутності – заступника) управління інформаційних технологій;

повідомити безпосереднього керівника та відповідальну особу.

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

припинити обробку персональних даних;

про всі події та факти повідомити безпосереднього керівника та відповідальну особу.

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

припинити обробку персональних даних;

повідомити управління інформаційних технологій;

повідомити безпосереднього керівника та відповідальну особу.

5. При виявленні пошкодження, втрати, викрадення документа або іншого носія персональних даних невідкладно повідомити безпосереднього керівника та відповідальну особу.

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

вжити невідкладних заходів щодо оповіщення відповідних служб реагування;

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

повідомити безпосереднього керівника та відповідальну особу.

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, керівник структурного підрозділу, у якому виявлено даний факт, невідкладно письмово повідомляє відповідальну особу.

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

Акт підписується відповідальною особою та працівником, яким виявлено (вчинено) дане порушення та його безпосереднім керівником.

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 начальнику ГУС у Миколаївській області або, в разі його відсутності, - посадовій особі, на яку покладено виконання його повноважень для прийняття рішення про проведення службового розслідування, повідомлення правоохоронних органів про несанкціонований доступ до персональних даних та вжиття відповідних заходів реагування.

_____