ЗАТВЕРДЖЕНО

наказ Державного агентства України з питань мистецтв та мистецької освіти

від 30.11 2021 р. № 118

ПЛАН

Дій працівників Держмистецтв 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 Держмистецтв, таких як: несанкціоноване отримання логінів і паролів, підбір та паролів та ключів, працівник, який виявив дані ознаки, зобов'язаний негайно:

1.1 припинити обробку персональних даних;

1.2 повідомити безпосереднього керівника та відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їхній обробці в Держмистецтв (далі – відповідальна особа);

1.3 звернутись до відповідальної особи, на яку покладено функції з впровадження в Держмистецтв 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 безпосереднього керівника та відповідальну особу;

2.4 повідомити відповідальну особу, на яку покладено функції з впровадження в Дермистецтв інформаційних технологій;

3. При вчинені 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 безпосереднього керівника та відповідальну особу;

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 безпосереднього керівника та відповідальну особу,

4.3 повідомити відповідальну особу, на яку покладено функції з впровадження в Держмистецтв інформаційних технологій.

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):

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 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, працівник, який виявив даний факт, та безпосередній керівник невідкладно письмово повідомляють про подію відповідальну особу.

7.1. Повідомлення реєструються відповідно до вимог діловодства у Держмистецтв.

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) дане порушення.

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

8.3. Підписаний Акт надається Голові Держмистецтв 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.

9. Організація роботи, пов'язаної із захистом персональних даних при їхній обробці, тих володільців/розпорядників, на яких не поширюється вимоги частини другої статті 24 Закону, покладається безпосередньо на тих осіб, які здійснюють обробку персональних даних.

Головний спеціаліст
сектору правового забезпечення Алла ТЕРЕХОВА