|  |
| --- |
| Додаток до розпорядження Чорноморського міського голови |
| від 30.12.2022 № 378 |

**Обов’язки користувачів,**

**встановлені Порядком надання працівникам доступу до відомчої інформаційної системи Державної міграційної служби України**

1. Користувач зобов’язаний:

1.1. забезпечувати обробку інформації відповідно до своїх функціональних обов’язків та Регламенту технічної взаємодії;

1.2. не допускати розголошення у будь-який спосіб персональних даних, які йому було довірено або які стали відомі у зв’язку з виконанням професійних чи службових або трудових обов’язків, крім випадків, передбачених законодавством;

1.3. суворо дотримуватись вимог нормативно-правових актів з питань захисту інформації;

1.4. на час відсутності на робочому місці блокувати свій доступ до відомчої інформаційної системи шляхом виходу із системи та видаленням з автоматизованого робочого місця захищеного носія особистого електронного ключа;

1.5. у разі надзвичайних подій доступу до відомчої інформаційної системи (зокрема: несанкціонованого доступу до робочої станції, несанкціонованих дій з відомчою інформаційною системою або інформацією, блокування доступу, втрати або компрометації пароля доступу тощо) – негайно усно повідомити начальника УЗД ЦНАП у м. Чорноморську, який є відповідальною особою, і який, в свою чергу, зобов’язаний невідкладно проінформувати про подію адміністратора безпеки ДМС України та керуючу справами виконавчого комітету Чорноморської міської ради Одеської області;

після усного повідомлення про вищезазначену подію користувач та відповідальна особа зобов’язані в установленому порядку письмово поінформувати керуючу справами виконавчого комітету Чорноморської міської ради Одеської області та керівництво ДМС України;

1.6. виконувати вимоги законодавства, Порядку та договору щодо зберігання та використання отриманої інформації за призначенням;

1.7. здійснювати та відповідати за збереження змісту робочого пароля та дії, здійснені від імені його облікового запису, та дотримуватись вимог законодавства України про захист інформації в інформаційно-телекомунікаційних системах, захист персональних даних та електронний цифровий підпис;

1.8. використання різними користувачами одного облікового запису не допускається. Це правило діє і в тому разі, коли користувачі мають однакові повноваження на доступ до відомчої інформаційної системи.

2. Користувачам забороняється:

2.1. розголошувати персональні дані фізичних осіб, отриманих з БПД, доступ до яких надається користувачу відповідно до своїх функціональних обов’язків;

2.2. залишати носій особистого електронного ключа у автоматизованій робочій системі на час своєї відсутності;

2.3. передавати у будь-якому вигляді або повідомляти особисті логіни (ідентифікатори) і паролі доступу іншим особам, у тому числі й своїм керівникам;

2.3. зберігати пароль доступу на будь-яких носіях інформації та в загальнодоступних місцях, що дає змогу іншим особам отримати інформацію про цей пароль;

2.4. використовувати отриману інформацію в цілях, не передбачених посадовими (функціональними) обов’язками користувача;

2.5. встановлювати на автоматизоване робоче місце будь-яке програмне забезпечення або змінювати параметри конфігурації раніше встановлених програмних засобів, у тому числі спеціального програмного забезпечення та АВПЗ, для доступу до відомчої інформаційної системи та інформації, яка обробляється за допомогою відомчої інформаційної системи;

2.6. надавати доступ до автоматизованого робочого місця, з якого введені його ідентифікатори і паролі доступу, іншим особам, у тому числі керівникам;

2.7. розповсюджувати, поширювати та використовувати в особистих цілях або передавати іншим особам отриману за допомогою ВІС інформацію, крім випадків, передбачених законодавством.

Керуюча справами Наталя КУШНІРЕНКО