ЗАТВЕРДЖЕНО

Наказ Державної судової
адміністрації України
04.09.2025 № 343

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

1. ДСА України вживає заходів щодо забезпечення захисту персональних даних суб'єктів персональних даних у паперовому та/або електронному вигляді на всіх етапах їх обробки, за допомогою організаційних та технічних заходів. Такі заходи спрямовані на запобігання випадкових втраті або знищення персональних даних, їх витоку, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

2. У випадку виявлення несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій техногенного, природного, соціально-політичного, військового характеру (далі – виникнення надзвичайних ситуацій), посадові особи ДСА України, які відповідно до своїх посадових обов'язків мають доступ до персональних даних та обробляють персональні дані, володільцем яких є ДСА України (далі – посадові особи ДСА України), у разі відсутності загрози їхньому життю, мають вчинити усі необхідні дії для збереження інформації в паперовому та/або електронному вигляді, що містить персональні дані, та унеможливити доступ сторонніх осіб та/або програмних засобів до такої інформації.

3. Загальна організація та координація дій у випадку несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій покладається на управління з питань персоналом (далі – відповідальний структурний підрозділ) та адміністратора Єдиної судової інформаційно-телекомунікаційної системи та інших інформаційних систем і сервісів судової влади, Державне підприємство «Інформаційні судові системи» (далі – адміністратор).

Безпосередня організація дій у випадку несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій покладається на керівників самостійних структурних підрозділів ДСА України та головних спеціалістів, які виконують окремі функції ДСА України.

4. Загальний опис дій посадових осіб ДСА України при виявленні ознак несанкціонованого доступу до персональних даних в інформаційно-

телекомунікаційних системах ДСА України, пошкодження технічного обладнання, виникнення надзвичайних ситуацій:

1) несанкціоноване отримання логінів і паролів, підбір паролів та ключів:
припинити обробку персональних даних;
повідомити безпосереднього керівника та відповідальний структурний підрозділ;
відповідальний структурний підрозділ повідомляє адміністратора, з метою блокування доступу до облікового запису;
змінити паролі доступу (за наявності технічної можливості);

2) зараження програмного забезпечення та носіїв інформації комп'ютерними вірусами:
припинити обробку персональних даних;
вимкнути робочий комп'ютер від електроживлення;
повідомити безпосереднього керівника та відповідальний структурний підрозділ;
відповідальний структурний підрозділ повідомляє адміністратора, з метою блокування доступу до облікового запису;

3) вчинення випадкових та/або помилкових дій, що можуть призвести до втрати, зміни, поширення, розголошення персональних даних тощо:
припинити обробку персональних даних;
про всі події та факти повідомити безпосереднього керівника та відповідальний структурний підрозділ;

4) відмова та/або технічний збій програмного забезпечення, за допомогою якого здійснюється обробка персональних даних:
припинити обробку персональних даних;
повідомити безпосереднього керівника та відповідальний структурний підрозділ;
відповідальний структурний підрозділ повідомляє адміністратора, з метою блокування доступу до облікового запису;

5) виникнення надзвичайних ситуацій техногенного, природного, соціально-політичного, військового характеру:
негайно припинити роботу з персональними даними та вимкнути робочі комп'ютери, зачинити паперові носії інформації у сховища;
покинути приміщення згідно з планом евакуації;
унеможливити неконтрольований доступ до приміщень, де зберігаються носії персональних даних;
відповідальний структурний підрозділ повідомляє головного спеціаліста з питань планування і реалізації планів заходів ДСА України та адміністратора з метою вжиття невідкладних заходів щодо оповіщення відповідних груп реагування та забезпечення збереження носіїв персональних даних від втрати та

пошкодження (за наявної можливості та у спосіб, що не загрожує життю за здоров'ю працівників).

5. Про всі випадки несанкціонованого доступу до персональних даних в паперовому та/або електронному вигляді, що призвели до пошкодження, псування, знищення, поширення тощо персональних даних, посадові особи ДСА України або їх безпосередні керівники мають невідкладно письмово повідомити відповідальний структурний підрозділ, відповідальний структурний підрозділ в свою чергу повідомляє адміністратора.

6. При виявленні пошкодження, втрати, викрадення документа або іншого носія персональних даних в паперовому та/або електронному вигляді посадові особи ДСА України мають невідкладно повідомити безпосереднього керівника та відповідальний структурний підрозділ, відповідальний структурний підрозділ в свою чергу повідомляє адміністратора.

7. Після отримання повідомлення відповідальний структурний підрозділ складає Акт про факт порушення процесу обробки та захисту персональних даних (далі – Акт).

8. Акт підписується відповідальним структурним підрозділом, адміністратором, Посадовою особою ДСА України, якою виявлено (вчинено) дане порушення, та його безпосереднім керівником.

9. Відмова Посадової особи ДСА України або її безпосереднього керівника від підписання Акта фіксується відповідно до вимог чинного законодавства.

10. Підписаний Акт подається Голові ДСА України (особі, яка виконує його обв'язки) для прийняття рішення про реагування відповідно до чинного законодавства.

Начальник управління
з питань персоналу **Наталя МІСЬКО**