ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від \_\_\_\_\_\_\_\_\_\_\_ 2022 р. № \_\_\_\_\_

**ПОРЯДОК**

**передачі, збереження, функціонування та доступу до державних інформаційних ресурсів (публічних електронних реєстрів) та їх резервних копій, розміщених на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України**

1. Цей Порядок визначає механізм передачі (переміщення), збереження, функціонування та доступу до державних інформаційних ресурсів (публічних електронних реєстрів) (далі – ДІР) та їх резервних копій, розміщених на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України (зокрема в закордонних дипломатичних установах України), протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування, володільцями інформації – власниками, держателями ДІР (далі – замовники), які виявили бажання (намір) розмістити ДІР та їх резервні копії на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України з метою захисту інформації.

2. У цьому Порядку терміни вживаються у значенні, наведеному в Законах України «Про захист інформації в інформаційно-комунікаційних системах», «Про публічні електронні реєстри», «Про Державну службу спеціального зв’язку та захисту інформації України», «Про основні засади забезпечення кібербезпеки України», «Про електронні довірчі послуги», «Про інформацію», «Про хмарні послуги»та «Про електронні комунікації».

3. Розміщення замовниками ДІР та їх резервних копій на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України, здійснюється на підставі договору.

4. Замовники погоджують з Службою безпеки України питання використання хмарних ресурсів та/або центрів обробки даних, що розташовані за межами України, для розміщення ДІР та їх резервних копій.

Служба безпеки України повідомляє замовників про прийняте рішення протягом п’яти робочих днів.

У разі коли Служба безпеки України у зазначений строк не надала своє погодження, вважається, що питання використання хмарних ресурсів та/або центрів обробки даних, що розташовані за межами України, для розміщення ДІР та їх резервних копій погоджено.

Замовники повідомляють Адміністрацію Держспецзв’язку та Мінцифри про використання хмарних ресурсів та/або центрів обробки даних, що розташовані за межами України, для розміщення ДІР та їх резервних копій.

5. Замовники для забезпечення належного функціонування систем та захисту інформації, що обробляється в них забезпечують створення резервних копій ДІР на окремих фізичних носіях у зашифрованому вигляді та їх подальшу передачу (переміщення) для зберігання в установленому законодавством порядку, у тому числі за межами України (зокрема в закордонних дипломатичних установах України)

6. ДІР та їх резервні копії, які не містять службової інформації та інформації, що становить державну таємницю, можуть бути розміщені на хмарних ресурсах та центрах обробки даних, що розташовані за межами України.

7. Розміщення та обробка ДІР та їх резервних копій, що містять службову інформацію та інформацію, що становить державну таємницю, за межами України здійснюються виключно в закордонних дипломатичних установах України.

Замовники забезпечують створення на окремих фізичних носіях у зашифрованому вигляді резервних копій ДІР, що містять службову інформацію та інформацію, що становить державну таємницю, і забезпечують їх передачу (переміщення) для зберігання до закордонних дипломатичних установ України.

Ключі шифрування повинні бути доступні виключно власнику (держателю), адміністратору або технічному адміністратору ДІР відповідно до законодавства.

8. Замовники є відповідальними за цілісність і конфіденційність ДІР та їх резервних копій у разі передачі (переміщення) ДІР до хмарних ресурсів та/або в центри обробки даних, що розташовані за межами України, а також до закордонних дипломатичних установ України.

9. Постачальник послуг (надавач хмарних послуг або ресурсів у центрах обробки даних), до якого переміщуються ДІР або їх резервні копії, повинен мати документ про відповідність впровадження системи інформаційної безпеки міжнародним стандартам.

10. Замовник обробляє ДІР, розміщені в хмарному ресурсі та/або в центрі обробки даних, розташованому за межами України, із застосуванням системи управління інформаційною безпекою або комплексної системи захисту інформації (далі – КСЗІ).

11. При переміщенні до хмарних ресурсів та/або центрів обробки даних, розташованих за межами України, інформаційно-комунікаційної системи (далі – ІКС), яка має чинний атестат відповідності КСЗІ з підтвердженою відповідністю, атестат відповідності КСЗІ такої ІКС не втрачає чинності за таких умов:

технологія обробки інформації не змінилася;

програмний склад ІКС, що реалізує функції захисту інформації, відповідає оціненим проектним рішенням КСЗІ;

постачальник послуг має документ про відповідність впровадження системи інформаційної безпеки міжнародним стандартам.

В інших випадках проводяться заходи з модернізації КСЗІ відповідно до законодавства.

При переміщенні ІКС, що не мають КСЗІ з підтвердженою відповідністю, власник системи вживає заходів з її побудови або впровадження щодо ІКС системи управління інформаційною безпекою.

12. Переміщення ДІР до хмарних ресурсів та/або центрів обробки даних, що розташовані за межами України, здійснюється з використанням фізичних носіїв або електронних комунікаційних мереж.

13. Переміщення ДІР або їх резервних копій на фізичних носіях може здійснюватись шляхом використання фізичного носія із резервною копією або шляхом переміщення ІКС в цілому. Якщо у складі ІКС є криптомодулі чи інші засоби криптографічного захисту інформації, які підпадають під визначення товарів подвійного використання, погодження їх вивезення здійснюється відповідно до Порядку здійснення державного контролю за міжнародними передачами товарів подвійного використання, затвердженого постановою Кабінету Міністрів України від 28 січня 2004 р. № 86 (Офіційний вісник України, 2004 р., № 4, ст. 167).

14. При переміщенні ІКС в цілому залучаються уповноважені фахівці власника (держателя), адміністратора або технічного адміністратора ДІР.

15. Переміщення ДІР, що містять конфіденційну інформацію, з використанням електронних комунікаційних мереж повинно здійснюватись із використанням засобів криптографічного захисту інформації.

У засобах криптографічного захисту інформації, які використовуються для переміщення ДІР, використовуються криптоалгоритми та криптопротоколи, які визначені національними стандартами, зокрема наведені у переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації, визначеному Адміністрацією Держспецзв’язку, та/або ті, на які за результатами експертних досліджень Адміністрацією Держспецзв’язку видано позитивний експертний висновок.

Ключі шифрування повинні бути доступні виключно власнику (держателю), адміністратору або технічному адміністратору ДІР відповідно до законодавства.

16. Про результати проведених заходів щодо переміщення ІКС замовник повідомляє Адміністрацію Держспецзв’язку та надає такі відомості:

1) найменування переміщеної ІКС;

2) номер і дата реєстрації документа про відповідність;

3) декларація у довільній формі щодо відповідності програмного складу ІКС, що реалізує функції захисту інформації, оціненим проектним рішенням КСЗІ (для ІКС, які мали КСЗІ з підтвердженою відповідністю);

4) найменування постачальника послуг, організації (надавача хмарних послуг або ресурсів у центрах обробки даних), найменування хмарного ресурсу та/або центру обробки даних, адреса розміщення центру обробки даних;

5) документ про відповідність впровадженої у постачальника послуг системи інформаційної безпеки міжнародним стандартам.

17. Періодичність створення резервних копій ДІР визначає замовник.

Протягом трьох робочих днів з дати укладання договору щодо переміщення резервної копії ДІР замовник повідомляє Адміністрацію Держспецзв’язку та надає такі відомості:

1) перелік ДІР, резервні копії яких створені та переміщені;

2) найменування ІКС, з якої здійснювалося копіювання;

3) інформація щодо засобу криптографічного захисту інформації (за наявності), яким здійснювалося шифрування резервної копії ДІР;

4) найменування постачальника послуг, організації (надавача хмарних послуг або ресурсів у центрах обробки даних), найменування хмарного ресурсу та/або центру обробки даних, адреса розміщення центру обробки даних;

5) документ про відповідність впровадженої у постачальника послуг системи інформаційної безпеки міжнародним стандартам.

18. Конфіденційна інформація, яка міститься у резервних копіях ДІР, зберігається у хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України, у зашифрованому вигляді. Ключі шифрування повинні бути доступні виключно власнику (держателю), адміністратору або технічному адміністратору ДІР, резервної копії ДІР.

19. Доступ для адміністрування ДІР, що розміщуються на хмарних ресурсах та центрах обробки даних, що розташовані за межами України, повинен здійснюватись із використанням засобів криптографічного захисту інформації.

У засобах криптографічного захисту інформації, які використовуються для захисту/доступу для адміністрування ДІР, використовуються криптоалгоритми та криптопротоколи, які визначені національними стандартами, зокрема наведені у переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації, визначеному Адміністрацією Держспецзв’язку, та/або ті, на які за результатами експертних досліджень Адміністрацією Держспецзв’язку видано позитивний експертний висновок.

Ключі шифрування повинні бути доступні виключно власнику (держателю), адміністратору або технічному адміністратору ДІР відповідно до законодавства.

20. Забезпечення функціонування (в тому числі адміністрування) ДІР здійснюється за участю представників власника (держателя), або адміністратора або технічного адміністратора ДІР відповідно до законодавства України у сфері захисту інформації.

21. Організацію заходів з резервування ДІР замовники здійснюють самостійно.

Замовники призначають відповідальних посадових осіб, які залучаються до організації робіт з резервування ДІР, та визначають їхні обов’язки.

Резервування ДІР здійснюється з дотриманням установлених для таких ресурсів та ДІР вимог щодо цілісності, конфіденційності та доступності.

22. Періодичність створення резервних копій ДІР визначає замовник.

23. Протягом шести місяців після припинення чи скасування правового режиму воєнного стану в Україні замовники, з якими укладено договір відповідно до пункту 3 цього Порядку, повинні забезпечити:

припинення використання відповідних хмарних сховищ та центрів обробки даних за межами України, на яких функціонують та зберігаються ДІР та їх резервні копії;

функціонування ДІР та зберігання їх резервних копій на території України.

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