ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 15 березня 2024 р. № 301

ПОРЯДОК
проведення моніторингу стану дотримання норм міжнародного гуманітарного права у зв’язку із збройною агресією проти України

1. Цей Порядок визначає механізм підготовки та проведення моніторингу стану дотримання норм міжнародного гуманітарного права у зв’язку із збройною агресією проти України.

2. У цьому Порядку поняття “моніторинг стану дотримання норм міжнародного гуманітарного права у зв’язку із збройною агресією проти України” (далі — моніторинг) означає комплекс взаємозв’язаних заходів організаційного та технічного характеру щодо отримання, узагальнення, оброблення, збереження та проведення аналізу інформації про фактичний стан дотримання прав і свобод людини і громадянина та міжнародного гуманітарного права у зв’язку із збройною агресією проти України.

3. Моніторинг проводиться відповідно до Закону України “Про забезпечення прав і свобод громадян та правовий режим на тимчасово окупованій території України”, Положення про Міністерство з питань реінтеграції тимчасово окупованих територій України, затвердженого постановою Кабінету Міністрів України від 8 червня 2016 р. № 376 (Офіційний вісник України, 2016 р., № 51, ст. 1802; 2020 р., № 41, ст. 1320), цього Порядку, інших актів законодавства.

4. Моніторинг проводиться з метою отримання та узагальнення інформації про стан дотримання норм міжнародного гуманітарного права у зв’язку із збройною агресією проти України, за результатами якого відповідна інформація оприлюднюється та надсилається МЗС для подальшого надання міжнародним організаціям у сфері захисту прав і свобод людини і громадянина.

5. Основними завданнями моніторингу є збір та аналіз отриманої інформації, зокрема про порушення норм міжнародного гуманітарного права.

6. Моніторинг проводиться відповідно до таких принципів:

систематичності та системності;

доцільності;

прозорості моніторингових процедур та відкритості;

безпеки персональних даних;

об’єктивності одержання та аналізу інформації під час проведення моніторингу;

відповідального ставлення до своєї діяльності суб’єктів, які беруть участь у підготовці та проведенні моніторингу.

7. Суб’єктами моніторингу є центральні органи виконавчої влади, органи місцевого самоврядування, міжурядові та неурядові міжнародні організації та їх органи, громадські об’єднання, які забезпечують збір та аналіз інформації про стан дотримання норм міжнародного гуманітарного права у зв’язку із збройною агресією проти України.

8. Ініціатором проведення моніторингу є Мінреінтеграції.

9. Суб’єкти моніторингу інформують щомісяця до 5 числа наступного періоду (у разі наявності відповідної інформації) Мінреінтеграції про результати проведеного моніторингу (крім відомостей про кримінальні правопорушення, внесених в Єдиний реєстр досудових розслідувань, а також здобутих правоохоронними органами в ході досудового розслідування).

10. Об’єктом моніторингу може бути інформація про порушення норм міжнародного гуманітарного права, зокрема про серйозні порушення, передбачені Женевськими конвенціями про захист жертв війни від 12 серпня 1949 р., про порушення законів та звичаїв війни, серед яких є:

нелегальні ув’язнення;

захоплення полонених з числа цивільних осіб;

руйнування, не виправдане воєнною необхідністю;

примушення особи до служби в збройних силах ворожої держави;

нелегальна депортація осіб, що перебувають під захистом, зокрема дітей;

неналежне використання прапора, військових емблем, захисних емблем, військових відзнак або форменого одягу супротивних сторін;

застосування заборонених методів і засобів ведення війни.

Перелік зазначених порушень норм міжнародного гуманітарного права не є вичерпним.

11. Моніторинг проводиться шляхом збирання та фіксування суб’єктами моніторингу відповідно до їх компетенції всіх наявних випадків порушення норм міжнародного гуманітарного права у зв’язку із збройною агресією проти України.

12. Етапами проведення моніторингу є:

збір інформації;

аналіз отриманої інформації;

узагальнення результатів моніторингу;

оприлюднення результатів моніторингу.

13. Моніторинг проводитися у формі безпосереднього одержання інформації від суб’єктів моніторингу.

14. За результатами проведення моніторингу Мінреінтеграції складається щомісячний звіт, за підсумками якого формується річний звіт.

15. Щомісячний звіт надсилається МЗС для подальшого надання відповідної інформації міжнародним організаціям у сфері захисту прав і свобод людини, Офісу Генерального прокурора, СБУ, Уповноваженому Верховної Ради України з прав людини до відома.

16. Щомісячний та річний звіт публікується на офіційному веб-сайті Мінреінтеграції.

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 15 березня 2024 р. № 301

ПОРЯДОК
функціонування, ведення та доступу до відомостей електронної інформаційної системи порушень норм міжнародного гуманітарного права внаслідок збройної агресії проти України

1. Цей Порядок визначає механізм функціонування, ведення та доступу до відомостей електронної інформаційної системи порушень норм міжнародного гуманітарного права внаслідок збройної агресії проти України (далі — інформаційна система) та використання таких відомостей.

Метою створення інформаційної системи є формування єдиної системи накопичення, обліку, зберігання та захисту даних про порушення норм міжнародного гуманітарного права внаслідок збройної агресії проти України, а також створення аналітичних матеріалів.

2. Терміни, що вживаються у цьому Порядку, мають таке значення:

авторизація користувача — процедура отримання користувачем повноважень на доступ до інформаційної системи за допомогою його власного кваліфікованого електронного підпису;

авторизований доступ — розширений або повний доступ до відомостей інформаційної системи, який надається авторизованим користувачам в установленому порядку;

авторизований користувач — користувач, що є посадовою або службовою особою органів державної влади та органів місцевого самоврядування, Секретаріату Уповноваженого Верховної Ради України з прав людини, якому надано авторизований доступ до інформаційної системи відповідно до положень цього Порядку;

знеособлення — процедура маскування в тексті інформації, оприлюднених з інформаційної системи відомостей, що не можуть бути розголошені відповідно до вимог законодавства, за допомогою спеціалізованого програмного забезпечення з подальшою вибірковою візуальною перевіркою результатів такого маскування. Результатом процедури знеособлення є створення образу електронного документа;

інформаційна система — державна інформаційно-комунікаційна система, призначена для накопичення, обліку, зберігання та захисту даних про порушення норм міжнародного гуманітарного права внаслідок збройної агресії проти України;

міжнародне гуманітарне право — система міжнародно визнаних правових норм і принципів, що застосовуються під час збройних

конфліктів, встановлюють права і обов’язки суб’єктів міжнародного права, зокрема щодо заборони чи обмеження використання певних засобів і методів ведення збройної боротьби, забезпечення захисту жертв конфлікту тощо;

неавторизований користувач — користувач, що не пройшов авторизацію в інформаційній системі з використанням кваліфікованого електронного підпису;

порушення норм міжнародного гуманітарного права — дія або бездіяльність, результатом якої є порушення норм міжнародного гуманітарного права, включаючи міжнародні злочини (воєнні злочини, злочини проти людяності, злочин геноциду) та інші порушення, що не є злочинами та суперечать відповідним міжнародним зобов’язанням;

суб’єкти документування — органи державної влади та органи місцевого самоврядування, міжнародна організація та її органи, юридична особа незалежно від форми власності або посадова особа, повноваженнями та/або завданням яких є діяльність, пов’язана із фіксуванням та/або обробкою інформації про порушення норм міжнародного гуманітарного права.

Інші терміни у цьому Порядку вживаються у значенні, наведеному в Законах України “Про інформацію”, “Про доступ до публічної інформації”, “Про захист персональних даних”, “Про Національну програму інформатизації”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про електронні комунікації”, “Про електронні документи та електронний документообіг”, “Про електронну ідентифікацію та електронні довірчі послуги”, Женевських конвенціях від 12 серпня 1949 р. та Додатковому протоколі до Женевських конвенцій від 12 серпня 1949 р., що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року.

3. Власником інформаційної системи та виключних майнових прав інтелектуальної власності на її програмне забезпечення є держава в особі Мінреінтеграції. Держателем інформаційної системи та володільцем інформації, що обробляється в такій системі, є Мінреінтеграції.

4. Адміністратором інформаційної системи є державне підприємство “Український національний центр розбудови миру”, що належить до сфери управління Мінреінтеграції.

5. Адміністратор інформаційної системи здійснює внесення відомостей до інформаційної системи шляхом створення в інформаційній системі відповідних записів, внесення до них змін, а також забезпечує функціонування та здійснює адміністрування інформаційної системи.

6. До інформаційної системи включається інформація про порушення норм міжнародного гуманітарного права внаслідок збройної агресії проти України.

7. Ведення інформаційної системи здійснюється державною мовою. Власні назви та імена у разі потреби можуть додатково наводитися іншою мовою.

8. Захист інформації в інформаційній системі здійснюється відповідно до законодавства у сфері захисту інформації в інформаційно-комунікаційних системах та законодавства про захист персональних даних.

9. Доступ до інформаційної системи надається безкоштовно у вигляді загального або авторизованого доступу.

10. Загальний доступ надається неавторизованим користувачам через офіційний веб-портал інформаційної системи після його створення та введення в експлуатацію.

11. У межах загального доступу надається інформація з інформаційної системи, яка визначена як відкрита або дозвіл на оприлюднення якої отримано в установленому законом порядку.

12. Надання авторизованого доступу до інформаційної системи здійснюється адміністратором інформаційної системи за погодженням з Мінреінтеграції. Обсяг інформації з інформаційної системи, доступної в межах авторизованого доступу, визначається власником інформаційної системи та надається адміністратором інформаційної системи за рівнями доступу.

13. Для авторизованих користувачів створюється електронний кабінет користувача.

14. З метою унеможливлення несанкціонованого втручання в роботу інформаційної системи адміністратор визначає для авторизованих та неавторизованих користувачів моделі захисту від загроз витоку інформації та застосовує засоби забезпечення цілісності бази даних інформаційної системи, запобігання спробам несанкціонованих дій щодо інформаційної системи, а також вчиняє інші необхідні дії.

15. Об’єктами інформаційної системи є інформація про порушення норм міжнародного гуманітарного права та окремо про суб’єктів документування.

16. Сукупність відомостей та даних (включаючи персональні дані) щодо потерпілих осіб, свідків та осіб, стосовно яких є дані про можливе вчинення ними порушень норм міжнародного гуманітарного права, технічна інформація, інформація, яка надійшла лише з одного джерела, яке не є суб’єктом документування, а також інша інформація з обмеженим доступом становлять службову та конфіденційну інформацію, яка не публікується в загальному доступі.

17. Інформація із інформаційної системи, доступна в межах загального доступу, оприлюднюється на офіційному веб-порталі

інформаційної системи знеособлено відповідно до положень цього Порядку.

18. Внесення інформації до інформаційної системи забезпечується адміністратором на підставі відомостей, отриманих від:

органів державної влади та органів місцевого самоврядування, міжнародних організацій та їх органів;

іноземних держав і міжнародних організацій та їх органів; фізичних та юридичних осіб, які володіють інформацією, необхідною для формування інформаційної системи;

інших джерел.

19. До інформаційної системи вносяться такі відомості:

1) обставини порушення (місце, дата і час, в які порушення вчинилося, у проміжку між якими продовжувалося або продовжується, опис обставин);

2) вид порушення;

3) кваліфікація порушення відповідно до норм міжнародних договорів (за наявності);

4) інформація про осіб, пов’язаних з порушенням (прізвище (за наявності), власне ім’я та по батькові (за наявності), дата народження, стать, громадянство, фото, інші ідентифікаційні дані, контактні дані (за наявності);

5) про джерело інформації;

6) інша інформація, пов’язана з порушенням.

До інформаційної системи може вноситися така інформація про суб’єктів документування:

прізвище (за наявності), власне ім’я та по батькові (за наявності) фізичної особи або найменування юридичної особи;

місцезнаходження (для юридичної особи) або адреса задекларованого (зареєстрованого) місця проживання (перебування) (для фізичної особи);

ідентифікаційний код юридичної особи згідно з ЄДРПОУ (для юридичної особи) або реєстраційний номер облікової картки платника податків (для фізичної особи);

відомості про керівника (для юридичної особи);

контактні дані;

інформація про діяльність.

20. Інформація щодо кожного порушення в інформаційній системі є унікальним записом. Допускається створення альтернативних записів у разі надходження інформації щодо порушення з різних джерел, яка не

узгоджується між собою. Кожен запис має реєстровий номер, містить дату внесення, джерело отримання відомостей та інформацію про особу, яка створила запис.

21. У разі надходження додаткової інформації про порушення норм міжнародного гуманітарного права дані вносяться до існуючого запису із зазначенням дати та джерела отримання відомостей. Новий запис при цьому не створюється.

22. Адміністратор інформаційної системи вносить інформацію в інформаційну систему за допомогою існуючих прикладних програмних інтерфейсів інформаційної системи.

23. Внесення відомостей до інформаційної системи здійснюється адміністратором невідкладно, але не пізніше ніж протягом п’яти робочих днів з моменту їх отримання.

24. Авторизований користувач інформаційної системи отримує право доступу до інформаційної системи після його надання адміністратором інформаційної системи та проходження авторизації.

25. Адміністратор інформаційної системи невідкладно вживає заходів до блокування доступу користувачів інформаційної системи, які порушують установлені законодавством умови користування інформаційною системою або політику безпеки, якою встановлюються права доступу до інформації, що міститься в інформаційній системі.

26. Обсяг та структура даних, якими обмінюються суб’єкти електронної взаємодії через програмні інтерфейси електронних інформаційних ресурсів (сервіси), визначаються договорами про інформаційну взаємодію, укладеними відповідно до законодавства.

27. Обробка отриманої інформації в інформаційній системі здійснюється з дотриманням законодавства про захист персональних даних. Доступ до інформації, що міститься в інформаційній системі, здійснюється з дотриманням вимог законодавства щодо захисту інформації з обмеженим доступом.

28. Електронна інформаційна взаємодія між інформаційною системою та іншими електронними інформаційними ресурсами здійснюється засобами системи електронної взаємодії державних електронних інформаційних ресурсів “Трембіта” з дотриманням положень Законів України “Про електронну ідентифікацію та електронні довірчі послуги”, “Про захист персональних даних”, “Про захист інформації в інформаційно-комунікаційних системах”. У разі відсутності технічної можливості передачі даних засобами системи електронної взаємодії державних електронних інформаційних ресурсів електронна інформаційна взаємодія може здійснюватися з використанням інших інформаційно-комунікаційних систем із застосуванням в них відповідних комплексних систем захисту

інформації з підтвердженою відповідністю за результатами державної експертизи в порядку, встановленому законодавством.

29. Під час обміну інформацією суб'єкти інформаційного обміну впроваджують організаційно-технічні заходи, які забезпечують захист інформації з обмеженим доступом, що передається, та побудову комплексної системи захисту інформації з підтвердженою відповідністю згідно із статтею 8 Закону України "Про захист інформації в інформаційно-комунікаційних системах".

30. Комплексна система захисту інформації з підтвердженою в установленому законодавством порядку відповідністю забезпечує захист інформації в інформаційній системі шляхом здійснення комплексу технічних, криптографічних, організаційних та інших заходів і використання засобів захисту інформації, спрямованих на недопущення блокування доступу до інформації, несанкціонованого доступу до інформації та/або її модифікації, а також недокументованих функцій у програмному забезпеченні.

31. З метою забезпечення достовірності, точності даних, їх внесення/зміни/уточнення в інформаційній системі адміністратор інформаційної системи здійснює комплекс організаційно-технічних заходів, спрямованих на забезпечення здійснення контролю та верифікації даних інформаційної системи, моніторингу змін індивідуальних відомостей.

32. Інформація в інформаційній системі зберігається 75 років, якщо інше не встановлено законом.

33. Доступ працівникам адміністратора інформаційної системи до відомостей, що містяться в інформаційній системі, надається відповідно до їх посадових обов'язків на підставі персональних автентифікаційних даних: логіна та пароля, присвоєння яких кожному працівнику контролюється уповноваженою особою адміністратора інформаційної системи.

34. Адміністратор інформаційної системи:

1) забезпечує:

адміністрування, технічну підтримку та безперебійне функціонування інформаційної системи;

здійснення заходів з інформаційного, технічного, програмно-технологічного функціонування інформаційної системи;

визначення порядку або правил управління інформаційною безпекою, політики та підходів до управління ризиками;

здійснення заходів щодо забезпечення захисту інформаційної системи та інформації, що міститься в ній;

збереження інформації, що міститься в інформаційній системі;

проведення аналізу та діагностики збоїв або припинення роботи апаратно-програмних ресурсів інформаційної системи;

2) здійснює:

облік дій користувачів щодо обробки інформації в інформаційній системі у спеціальних електронних журналах;

облік дій працівників адміністратора інформаційної системи під час внесення додаткової інформації або змін до відомостей, що містяться в інформаційній системі;

створення та розподіл рівнів авторизованого доступу до інформаційної системи;

постійний моніторинг технічного стану інформаційної системи та захищеності інформації, що міститься в ній;

запровадження механізму електронної ідентифікації особи для підключення авторизованих користувачів до інформаційної системи;

надання/припинення підключення користувачів інформаційної системи;

ведення обліку авторизованих користувачів інформаційної системи, яким надано доступ до інформаційної системи з використанням засобів електронної ідентифікації особи;

технічну та інформаційну підтримку користувачів інформаційної системи;

внесення відомостей до інформаційної системи;

3) проводить:

навчання авторизованих користувачів інформаційної системи під час її впровадження та функціонування;

інші дії, пов’язані з роботою інформаційної системи.

35. Органи державної влади та органи місцевого самоврядування:

1) визначають уповноважених осіб, які діятимуть від їх імені як авторизовані користувачі інформаційної системи;

2) забезпечують:

здійснення контролю за доступом до інформаційної системи авторизованих користувачів, які діють від їх імені;

авторизованих користувачів, які діють від їх імені, шляхом надання діючого кваліфікованого сертифіката відкритого ключа, його скасування, блокування та поновлення для авторизації в інформаційній системі;

3) звертаються до власника інформаційної системи з пропозиціями (зауваженнями) щодо його роботи.

36. Авторизовані користувачі інформаційної системи несуть передбачену законодавством відповідальність за розголошення відомостей з інформаційної системи, які становлять службову та конфіденційну інформацію.