АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАКАЗ

15.01.2016 № 20

Зареєстровано в Міністерстві юстиції України 05 лютого 2016 р. за № 196/28326

Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті

{Із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації № 640 від 28.10.2021}

Відповідно до пункту 41 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», підпункту 30 пункту 4 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, та абзацу другого пункту 5 Плану заходів щодо захисту державних інформаційних ресурсів, затвердженого розпорядженням Кабінету Міністрів України від 05 листопада 2014 року № 1135-р, **НАКАЗУЮ:**

1. Затвердити Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті, що додається.

2. Директору Департаменту спеціальних інформаційно-телекомунікаційних систем Адміністрації Державної служби спеціального зв'язку та захисту інформації України забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України відповідно до Указу Президента України від 03 жовтня 1992 року № 493 «Про державну реєстрацію нормативно-правових актів міністерств та інших органів виконавчої влади».

3. Цей наказ набирає чинності з дня його офіційного опублікування.

4. Контроль за виконанням цього наказу покласти на першого заступника Голови Державної служби спеціального зв'язку та захисту інформації України.

Голова Служби
генерал-майор
Держспецзв'язку **Л.О. Євдоченко**

ПОГОДЖЕНО:

Голова Національної комісії,
що здійснює державне регулювання
у сфері зв'язку та інформатизації О.М. Животовський

Т. в. о. Голови Служби безпеки України В.В. Маліков

Голова Державного агентства
з питань електронного урядування О.В. Риженко

ЗАТВЕРДЖЕНО
Наказ Адміністрації
Державної служби

спеціального зв'язку
та захисту інформації України
15 січня 2016 року № 20
(у редакції наказу Адміністрації
Державної служби
спеціального зв'язку
та захисту інформації України
від 28 жовтня 2021 року № 640)

Зареєстровано в Міністерстві
юстиції України
05 лютого 2016 р.
за № 196/28326

ПОРЯДОК
сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті

I. Загальні положення

1. Цей Порядок визначає організаційні засади проведення сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті (далі - сканування).

2. Терміни у цьому Порядку вживаються у значеннях, наведених у Законах України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про телекомунікації», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про основні засади забезпечення кібербезпеки України».

3. Сканування є однією з форм проведення оцінки стану захищеності інформації в інформаційно-телекомунікаційних системах (далі - ІТС) і полягає у дистанційній перевірці ІТС, яка забезпечує розміщення державних інформаційних ресурсів у мережі Інтернет (далі - розміщені в Інтернеті ДІР), на предмет виявлення в ній вразливостей, які створюють передумови до порушення конфіденційності, цілісності та доступності інформації та державних інформаційних ресурсів, що обробляються ІТС, або спостережності самої ІТС.

4. Об'єктами сканування є ІТС, в якій обробляються розміщені в Інтернеті ДІР, її окремі елементи, програмні і програмно-апаратні засоби, що застосовані в ІТС, незалежно від наявності побудованої комплексної системи захисту інформації та/або системи управління інформаційною безпекою з підтвердженою відповідністю.

5. Сканування проводиться згідно зі встановленим Порядком оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженим наказом Адміністрації Держспецзв'язку від 02 грудня 2014 року № 660, зареєстрованим в Міністерстві юстиції України 28 січня 2015 року за № 90/26535 (далі - Порядок оцінки).

6. Сканування проводиться Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (далі - ДЦКЗ Держспецзв'язку) відповідно до Порядку оцінки:

за письмовим зверненням державного органу, органу місцевого самоврядування, військового формування, підприємства, установи і організації державної форми власності (далі - розпорядник розміщених в Інтернеті ДІР);

в автоматичному режимі відповідно до переліку об'єктів сканування, який формується у рамках планування проведення оцінки стану захищеності в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності (далі - Перелік об'єктів сканування).

7. Посадовим особам ДЦКЗ Держспецзв'язку, що безпосередньо проводять сканування, забороняється розголошувати його результати третім сторонам, крім випадків, передбачених законодавством та цим Порядком, а також використовувати виявлені вразливості для проведення дій, що можуть призвести до порушення штатного режиму функціонування ІТС, що сканується, порушення цілісності, конфіденційності та доступності інформації та розміщених в Інтернеті ДІР, а також для отримання доступу до персональних даних, що можуть оброблятися в ІТС.

8. У разі виявлення під час сканування випадків порушення правил обробки та захисту інформації, що може спричинити розголошення службової інформації або інформації, що становить державну таємницю, Держспецзв'язку інформує Службу безпеки України про факти порушень протягом п'яти календарних днів з моменту їх виявлення.

II. Сканування за письмовим зверненням

1. Власник ІТС, в якій обробляються [illegible]

1. Власник ІТС, у якій обробляються державні інформаційні ресурси, у разі потреби проведення сканування власної ІТС на предмет виявлення у ній вразливостей ініціює перед розпорядником розміщених в Інтернеті ДІР, що обробляються у цій ІТС, питання звернення до Держспецзв'язку для проведення сканування власної ІТС.

2. ДЦКЗ Держспецзв'язку організовує заходи зі сканування на підставі письмового звернення розпорядника розміщеного в Інтернеті ДІР та за рішенням Голови Держспецзв'язку або його заступника відповідно до розподілу функціональних обов'язків.

3. ДЦКЗ Держспецзв'язку:

письмово інформує розпорядника розміщеного в Інтернеті ДІР та власника ІТС (якщо розпорядник розміщеного в Інтернеті ДІР не є власником ІТС, у якій обробляється відповідний ресурс) про строки, обсяг та зміст заходів, які будуть проведені у процесі сканування;

не пізніше ніж за три робочих дні інформує Службу безпеки України про об'єкт, строки та методи проведення сканування. Для термінового інформування також використовується електронна пошта.

4. За результатами сканування посадові особи ДЦКЗ Держспецзв'язку, що безпосередньо здійснювали сканування, складають акт сканування на предмет вразливості розміщених в Інтернеті державних інформаційних ресурсів (далі - Акт) за формою, що наведена у додатку до цього Порядку, в якому викладають результати сканування, висновки та відповідні рекомендації.

5. Акт складається у двох примірниках, його затверджує Голова Держспецзв'язку або його заступник відповідно до розподілу обов'язків.

6. Примірники Акта не пізніше ніж за десять днів після його затвердження надсилаються розпоряднику розміщених в Інтернеті ДІР для ознайомлення з ним керівника або уповноваженої особи державного органу, що звертався.

7. Розпорядник розміщених в Інтернеті ДІР повертає другий примірник Акта у десятиденний строк з дати його отримання. До усунення причин, що зумовлюють віднайдені вразливості, розпоряднику розміщеного в Інтернеті ДІР або власнику ІТС, в якій обробляються державні інформаційні ресурси, забороняється публічно оголошувати результати сканування.

8. У місячний строк з дня отримання Акта розпорядник розміщеного в Інтернеті ДІР або власник ІТС письмово інформує Держспецзв'язку про врахування рекомендацій, викладених в Акті. У разі відсутності такого інформування або надходження повідомлення про неможливість врахування рекомендацій Держспецзв'язку протягом десяти робочих днів інформує Службу безпеки України про виявлені під час сканування вразливості.

III. Автоматизоване дистанційне сканування

1. ДЦКЗ Держспецзв'язку на початку кожного календарного року з урахуванням даних, що містяться в Реєстрі інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, складає Перелік об'єктів сканування, який містить відомості про об'єкти і дати проведення сканування. Перелік об'єктів сканування є частиною річного плану проведення оцінки стану захищеності в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності, який формується відповідно до встановленого Порядку оцінки.

2. ДЦКЗ Держспецзв'язку протягом п'яти робочих днів після затвердження Переліку об'єктів сканування надсилає його до Служби безпеки України.

3. За результатами проведення автоматизованого дистанційного сканування ДЦКЗ Держспецзв'язку інформує:

розпорядників розміщених в Інтернеті ДІР - якщо під час автоматизованого дистанційного сканування виявлено вразливості та недоліки у налаштуванні ІТС, в якій обробляються державні інформаційні ресурси, згідно з процедурою, встановленою пунктами 4-8 розділу II цього Порядку;

Національний координаційний центр кібербезпеки Ради національної безпеки і оборони України - щотижня про виявлені у ході автоматизованого дистанційного сканування вразливості і недоліки функціонування ІТС.

4. Після отримання від розпорядника розміщених в Інтернет ДІР або власника ІТС, в якій вони обробляються, інформації щодо усунення виявлених вразливостей та недоліків ДЦКЗ Держспецзв'язку у разі потреби з метою перевірки ефективності впроваджених заходів із захисту проводить повторне автоматизоване дистанційне сканування в порядку, встановленому розділом II цього Порядку.

Заступник Голови
Державної служби
спеціального зв'язку
та захисту інформації України

**з питань цифрового розвитку,
цифрових трансформацій
і цифровізації** **В. Жора**

{Порядок в редакції Наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації № 640 від 28.10.2021}

Додаток
до Порядку сканування на предмет
вразливості державних інформаційних
ресурсів, розміщених в Інтернеті
(пункт 4 розділу II)

АКТ
сканування на предмет вразливості розміщених в Інтернеті державних інформаційних ресурсів

{Додаток в редакції Наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації № 640 від 28.10.2021}

Документи та файли

Сигнальний документ — f453437n75.doc

Публікації документа

- **Офіційний вісник України** від 09.03.2016 — 2016 р., № 17, стор. 198, стаття 695, код акта 80874/2016