КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 4 квітня 2023 р. № 299

Київ

Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі

Відповідно до пункту 37 Плану реалізації Стратегії кібербезпеки України, схваленого рішенням Ради національної безпеки і оборони України від 30 грудня 2021 р. “Про План реалізації Стратегії кібербезпеки України”, введеного в дію Указом Президента України від 1 лютого 2022 р. № 37, Кабінет Міністрів України **постановляє:**

1. Затвердити Порядок реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, що додається.

2. Рекомендувати враховувати вимоги Порядку, затвердженого згідно з пунктом 1 цієї постанови, під час проведення заходів із забезпечення кібербезпеки:

Апарату Ради національної безпеки і оборони України та органам місцевого самоврядування;

Національному банку, банкам, іншим суб’єктам, що провадять діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторам та/або учасникам платіжних систем, технологічним операторам платіжних послуг, у тому числі суб’єктам, віднесення яких до критичної інфраструктури здійснює Національний банк.

3. Адміністрації Державної служби спеціального зв’язку та захисту інформації затвердити у тримісячний строк методичні рекомендації щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі.

Прем’єр-міністр України **Д. ШМИГАЛЬ**

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 4 квітня 2023 р. № 299

ПОРЯДОК
реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі

1. Цей Порядок визначає процедури реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі (далі — кіберінциденти/кібератаки) та категорії (рівні) їх критичності.

2. У цьому Порядку терміни вживаються у значенні, наведеному в Законі України “Про основні засади забезпечення кібербезпеки України” та постанові Кабінету Міністрів України від 29 грудня 2021 р. № 1426 “Про затвердження Положення про організаційно-технічну модель кіберзахисту” (Офіційний вісник України, 2022 р., № 4, ст. 219).

3. Реагування на кіберінциденти/кібератаки здійснюється суб’єктами забезпечення кібербезпеки шляхом вжиття заходів до кіберзахисту, спрямованих на швидке виявлення та захист від кіберінцидентів/кібератак, належне інформування про них, запобігання негативним наслідкам, їх мінімізації та усунення, виправлення вразливостей, а також відновлення сталості і надійності функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем та інших об’єктів кіберзахисту.

Суб’єкти забезпечення кібербезпеки вживають заходів відповідно до методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених Адміністрацією Держспецзв’язку.

4. Реагування на кіберінциденти/кібератаки здійснюється суб’єктами забезпечення кібербезпеки послідовно такими етапами, як підготовка, виявлення та аналіз, стримування, усунення, відновлення, аналіз ефективності заходів з реагування на кіберінциденти/кібератаки.

5. Реагування суб’єктами забезпечення кібербезпеки на кіберінциденти/кібератаки розпочинається з етапу підготовки, під час якого здійснюються заходи з вивчення та дослідження сучасних видів кіберінцидентів/кібератак, розроблення методів і механізмів запобігання та протидії можливим кіберінцидентам/кібератакам.

6. На етапі виявлення та аналізу суб’єкти забезпечення кібербезпеки здійснюють виявлення кіберінциденту/кібератаки та визначають їх критичність для забезпечення пропорційності та/або співрозмірності подальших заходів з кіберзахисту реальним та потенційним ризикам.

Суб’єкти забезпечення кібербезпеки визначають критичність кіберінциденту/кібератаки відповідно до методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених Адміністрацією Держспецзв’язку, за такими категоріями (рівнями):

рівень 0, некритичний (білий) — кіберінцидент/кібератака не загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем;

рівень 1, низький (зелений) — кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, але не загрожує захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються;

рівень 2, середній (жовтий) — кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, внаслідок чого створюються передумови для порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються, виникають передумови для припинення виконання функцій та/або надання послуг критичною інфраструктурою;

рівень 3, високий (помаранчевий) — кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають потенційні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Реагування на цьому рівні може потребувати залучення сил та засобів більше ніж одного основного суб’єкта національної системи кібербезпеки;

рівень 4, критичний (червоний) — кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування кількох інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають реальні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих

галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Кіберінцидент/кібератака може мати транскордонний вплив. Реагування на цьому рівні потребує залучення сил та засобів основних суб'єктів національної системи кібербезпеки;

рівень 5, надзвичайний (чорний) — кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування значної кількості інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають невідворотні загрози для повноцінного функціонування держави або загроза життю громадян України. Кіберінцидент/кібератака може мати транскордонний вплив. Реагування на цьому рівні потребує максимального залучення сил та засобів основних суб'єктів національної системи кібербезпеки та інших суб'єктів забезпечення кібербезпеки.

7. Під час етапу стримування суб'єктами забезпечення кібербезпеки вживаються заходи до зниження негативного впливу кіберінциденту/кібератаки, запобігання порушенню безпеки, забезпечення сталого, надійного та штатного режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, несанкціонованого втручання в їх роботу, захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються.

8. Під час етапу усунення суб'єкти забезпечення кібербезпеки вживають заходів до ліквідації наслідків кіберінциденту/кібератаки для інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, інформації та даних, що ними обробляються.

9. На етапі відновлення суб'єктами забезпечення кібербезпеки вживаються заходи до відновлення безпеки, сталого, надійного, штатного та захищеного від несанкціонованого втручання в роботу режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються.

10. За результатами вжиття заходів до кіберзахисту суб'єкти забезпечення кібербезпеки проводять аналіз ефективності реагування на кіберінциденти/кібератаки.

Під час цього етапу забезпечується вивчення задокументованих даних щодо кіберінциденту/кібератаки, інформування керівництва суб'єкта забезпечення кібербезпеки, узагальнення та проведення аналізу досвіду реагування для подальшого підвищення ефективності вжиття заходів до кіберзахисту у разі можливих кіберінцидентів/кібератак у подальшому.

_____