ПОРЯДОК
взаємодії суб'єктів забезпечення кібербезпеки
під час реагування на кіберінциденти/кібератаки

І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1. Цей Порядок встановлює вимоги до інформаційного обміну, координації та спільних дій суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки.

2. Терміни, що використовуються у цьому Порядку:

подія кібербезпеки – ідентифікована подія на об'єкті кіберзахисту, яка вказує на можливе порушення політики безпеки або відмову засобів захисту чи раніше невідому ситуацію, що може стосуватися безпеки;

рівень критичності кіберінциденту/кібератаки – рівень негативних наслідків для інформаційної інфраструктури країни, що можуть відбутися в результаті настання (реалізації) кіберінциденту/кібератаки.

Інші терміни вживаються у значенні, наведеному в Законах України «Про основні засади забезпечення кібербезпеки України», «Про національну безпеку України», «Про захист інформації в інформаційно-комунікаційних системах», «Про критичну інфраструктуру».

3. Застосування суб'єктами забезпечення кібербезпеки цього Порядку ґрунтується на таких принципах:

Спільна мета. Приватний сектор і державні органи мають спільний життєво важливий інтерес і взаємодоповнювальні ролі й обов'язки щодо забезпечення безпеки функціонування власних інформаційно-комунікаційних систем та кібербезпеки держави в цілому. Характер кіберзагроз унеможливлює ефективну протидію ним відособлено, потребує побудови стійких та ефективних механізмів співпраці.

Реагування з урахуванням ризиків. Під час реагування на кіберінциденти/кібератаки як держава, так і атаковані об'єкти за можливості максимально застосовують механізми оцінки ризиків, щоб забезпечити найбільш швидкий та ефективний шлях реагування, а також раціональне використання наявних ресурсів.

Повага до підприємств, установ та організацій, на яких стався кіберінцидент/кібератака. Основний суб'єкт національної системи кібербезпеки, який надає допомогу постраждалому від кіберінциденту/кібератаки суб'єкту, з повагою ставиться до збереження приватності тих даних, які могли йому стати відомі під час заходів реагування. Якщо інше не визначено спільними рішеннями учасників реагування або вимогами законодавства, інформація про інцидент може бути повідомлена громадськості в обсязі, що унеможливлює розголошення даних щодо постраждалої сторони але сприятиме підвищенню обізнаності громадськості про кіберзагрозу. Факт надання допомоги суб'єкту забезпечення кібербезпеки не свідчить про його неспроможність виконувати відповідні завдання в межах своєї компетенції.

Єдність зусиль. Кожен суб'єкт забезпечення кібербезпеки має власну роль, обов'язки, повноваження та можливості, які можуть бути задіяні під час реагування на кіберінцидент/кібератаку. Для швидкого досягнення необхідного результату зусилля суб'єктів забезпечення кібербезпеки мають бути скоординовані. Основний суб'єкт національної системи кібербезпеки, якому надійшла інформація про кіберінцидент/кібератаку, невідкладно інформує Національний координаційний центр кібербезпеки з метою сприяння уніфікованому реагуванню та поєднанню зусиль (залучення інших суб'єктів забезпечення кібербезпеки у разі необхідності). Якщо така потреба є – до заходів реагування можуть долучатись міжнародні партнери, а самі заходи координуватись з ними.

Пріоритетність заходів відновлення діяльності. Заходи з реагування на кіберінцидент проводитимуться таким чином, щоб передусім сприяти процесу відновлення надання суб'єктом забезпечення кібербезпеки послуг та/або забезпеченню його сталого функціонування, унеможливленню повторної реалізації виявленої загрози, зокрема на інших об'єктах, а щодо кібератак – також додатково забезпечення збереження можливих джерел доказування для подальшого притягнення винних до відповідальності.

4. Залежно від ступеня негативних наслідків, що можуть настати в результаті реалізації кіберінциденту/кібератаки, встановлюються такі рівні критичності кіберінцидентів/кібератак:

Некритичний (білий) – кіберінцидент/кібератака не загрожує сталому функціонуванню системи електронних комунікацій, системи управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів.

Низький (зелений) – кіберінцидент/кібератака безпосередньо загрожує сталому функціонуванню системи електронних комунікацій, системи управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів, інших об'єктів кіберзахисту, але не загрожує порушенню конфіденційності, цілісності та доступності державних інформаційних ресурсів або персональних даних громадян.

Середній (жовтий) – кіберінцидент/кібератака безпосередньо загрожує сталому функціонуванню системи електронних комунікацій, системи управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів, інших об'єктів кіберзахисту, внаслідок чого створюються передумови для порушення конфіденційності, цілісності та доступності державних інформаційних ресурсів або персональних даних громадян, виникають передумови для впливу на надання основних послуг населенню.

Високий (помаранчевий) – кіберінцидент/кібератака безпосередньо загрожує сталому функціонуванню системи електронних комунікацій, системи управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів, інших об'єктів кіберзахисту, внаслідок чого прогнозується помітній вплив на національну безпеку,

обороноздатність, економічну безпеку, зовнішні відносини, основоположні свободи чи суспільну довіру або створюється потенційна загроза обмеження у наданні основних послуг населенню. Реагування на цьому рівні може потребувати залучення ресурсів більше ніж одного основного суб'єкта національної системи кібербезпеки.

Критичний (червоний) – кіберінцидент/кібератака безпосередньо загрожує сталому функціонуванню декількох систем електронних комунікацій, систем управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів, інших об'єктів кіберзахисту, внаслідок чого прогнозується значній вплив на національну безпеку, обороноздатність, економічну безпеку, зовнішні відносини, здоров'я чи безпеку громадян або створюється реальна загроза обмеження у наданні основних послуг населенню. Реагування на цьому рівні потребує залучення ресурсів усіх основних суб'єктів національної системи кібербезпеки.

Надзвичайний (чорний) – кіберінцидент/кібератака безпосередньо загрожує сталому функціонуванню значної кількості систем електронних комунікацій, систем управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів, інших об'єктів кіберзахисту, внаслідок чого відбувається невідворотній вплив на повноцінне функціонування держави або створюється загроза життю громадян України. Реагування на цьому рівні потребує максимальної державної участі, повного залучення всіх ресурсів основних та інших суб'єктів національної системи кібербезпеки.

5. Рівень критичності кіберінциденту/кібератаки попередньо визначається суб'єктом забезпечення кібербезпеки, який зафіксував кіберінцидент/кібератаку та обов'язково підтверджується (уточнюється за необхідності) суб'єктом, відповідальним за реагування на кіберінцидент/кібератаку, з урахуванням отримання додаткової інформації про кіберінцидент/кібератаку.

6. Під час реагування на кіберінциденти/кібератаки «білого» рівня критичності цей Порядок не застосовується.

7. Взаємодія суб'єктів забезпечення кібербезпеки за цим Порядком розпочинається з настанням однієї з таких подій:

Інформування. Суб'єкт забезпечення кібербезпеки незалежно від форми власності інформує Національний координаційний центр кібербезпеки через профільну службу Апарату РНБО України та визначеного законодавством та цим Порядком основного суб'єкта національної системи кібербезпеки про зафіксований ним кіберінцидент/кібератаку щодо власної системи електронних комунікацій або системи управління технологічними процесами.

Дистанційне виявлення. Один з основних суб'єктів національної системи кібербезпеки власними силами і засобами в автоматизованому режимі виявляє події кібербезпеки в системі електронних комунікацій або системі управління технологічними процесами суб'єкта забезпечення

кібербезпеки, які містять ознаки кіберінциденту/кібератаки.

Інше джерело. Один з основних суб'єктів національної системи кібербезпеки під час моніторингу кіберпростору виявляє інформацію щодо кіберінциденту/кібератаки, у тому числі щодо державних електронних інформаційних ресурсів та/або критичної інформаційної інфраструктури, або інформація про такий факт надійшла йому іншим шляхом (від іноземних партнерів, юридичних або фізичних осіб тощо).

ІІ. РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ/КІБЕРАТАКИ «ЗЕЛЕНОГО», «ЖОВТОГО» ТА «ПОМАРАНЧЕВОГО» РІВНЯ КРИТИЧНОСТІ

1. При Національному координаційному центрі кібербезпеки створюється постійна Об'єднана група реагування на кіберінциденти/кібератаки (далі – Група). За посадою Групу очолює заступник керівника Національного координаційного центру кібербезпеки.

За погодженням керівника Національного координаційного центру кібербезпеки або його заступника обов'язки керівника Групи можуть бути покладені на іншого члена Національного координаційного центру кібербезпеки.

2. Члени Національного координаційного центру кібербезпеки визначають для діяльності Групи щонайменше одного свого співробітника, діяльність якого під час реагування на кіберінцидент/кібератаку скеровується керівником Групи.

3. В умовах правового режиму воєнного стану заходи реагування на кіберінциденти/кібератаки здійснюються з урахуванням заходів стримування та відсічі збройної агресії проти України, визначених для основних суб'єктів національної системи кібербезпеки директивами, бойовими наказами (розпорядженнями) Головнокомандувача Збройних Сил України. Вказаними рішеннями військового командування може бути встановлено інший порядок взаємодії.

4. Суб'єкт забезпечення кібербезпеки, який зафіксував кіберінцидент/кібератаку, невідкладно (протягом години) інформує через офіційну електронну поштову скриньку або іншим офіційно визначеним шляхом:

Урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA (далі – CERT-UA) – в обов'язковому порядку (окрім суб'єктів банківської системи та суб'єктів переказу коштів);

Команду реагування на кіберінциденти в банківській системі Центру кіберзахисту Національного банку України (далі – CSIRT-NBU) – якщо суб'єкт належить до банківської системи, здійснює діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю якого здійснює Національний банк, є оператором платіжних систем та/або учасником платіжних систем, технологічним оператором платіжних послуг;

Службу безпеки України – обов'язково, якщо

кіберінцидент/кібератака відбувається стосовно державних електронних інформаційних ресурсів або об’єктів критичної інфраструктури.

Департамент кіберполіції Національної поліції України (далі – ДКП) – у випадку вчинення правопорушення стосовно об’єкта приватного сектору, який не належить до об’єктів критичної інфраструктури;

відомчий або галузевий (секторальний) центр кібербезпеки (кіберзахисту) – у разі наявності відповідного центру, до сфери відповідальності якого належить суб’єкт забезпечення кібербезпеки.

5. Порядок взаємодії суб’єкта забезпечення кібербезпеки, який зафіксував кіберінцидент/кібератаку, з відомчим або галузевим (секторальним) центром кібербезпеки (кіберзахисту) визначається відомчими розпорядчими документами.

Суб’єкт забезпечення кібербезпеки, який зафіксував кіберінцидент/кібератаку, може здійснювати інформування, передбачене пунктом 4 розділу ІІ цього Порядку, через відомчий або галузевий (секторальний) центр кібербезпеки (кіберзахисту). Такий алгоритм взаємодії (інформування) необхідно додатково врегулювати відомчим розпорядчим документом.

6. Повідомлення про кіберінцидент/кібератаку щонайменше має містити таку інформацію:

Тип кіберінциденту/кібератаки (відповідно до таксономії кіберінцидентів).

Рівень критичності кіберінциденту/кібератаки.

Короткий опис (контекст).

Попередня оцінка: кібератака чи кіберінцидент?

Хто виявив (підрозділ, посадова особа, контактні дані)?

Перелік суб’єктів, яких поінформовано про кіберінцидент/кібератаку.

Позначка «Потрібна допомога в реагуванні» або «Допомога в реагуванні не потрібна».

7. Відповідальними за реагування на конкретний кіберінцидент/кібератаку визначаються:

1) у випадку, якщо кіберінцидент/кібератака відбувається стосовно державних електронних інформаційних ресурсів або об’єктів критичної інформаційної інфраструктури – CERT-UA та ДЦКЗ Держспецзв’язку (за необхідності), які разом з представниками СБУ (за згодою) надають допомогу та здійснюють координацію щодо локалізації кіберінциденту/кібератаки, здійснюють їх технічний аналіз, документування, встановлення джерел та збереження доказової бази в інтересах можливого розслідування правопорушення, надають власникам об’єктів кіберзахисту методичну та практичну допомогу з метою запобігання, виявлення та усунення наслідків кіберінцидентів та кібератак щодо цих об’єктів;

2) у випадку, якщо кіберінцидент/кібератака відбувається стосовно об’єкта приватного сектору, який не належить до об’єктів критичної інформаційної інфраструктури – CERT-UA та ДЦКЗ Держспецзв’язку (за

необхідності), які разом з ДКП надають допомогу та здійснюють координацію щодо локалізації кіберінциденту/кібератаки, здійснюють їх технічний аналіз, документування, встановлення джерел та збереження доказової бази в інтересах можливого розслідування правопорушення, надають власникам об'єктів кіберзахисту методичну та практичну допомогу з метою запобігання, виявлення та усунення наслідків кіберінцидентів та кібератак щодо цих об'єктів;

3) у випадку кіберінциденту/кібератаки в банку, іншому суб'єкті, що здійснює діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю якого здійснює Національний банк, є оператором платіжних систем та/або учасником платіжних систем, технологічним оператором платіжних послуг – CSIRT-NBU, до того ж у разі наявності ознак кібератаки «помаранчевого» рівня критичності CSIRT-NBU інформує СБУ та ДКП (з метою встановлення джерел та збереження доказової бази в інтересах можливого розслідування правопорушення), а також CERT-UA.

Під час виконання заходів з реагування обов'язково забезпечується унеможливлення порушення цілісності доказової бази.

8. У випадку відсутності у відповідального за заходи з реагування основного суб'єкта національної системи кібербезпеки ресурсів для проведення значених вище заходів, за його ініціативи рішенням Групи порядок реагування на конкретний кіберінцидент/кібератаку (зокрема перелік суб'єктів, які є відповідальними за реагування на кіберінцидент/кібератаку) може бути змінений.

9. CERT-UA, CSIRT-NBU, СБУ та ДКП за результатами первинної перевірки отриманих даних про кіберінциденти/кібератаки інформують в узгодженому порядку Службу з питань інформаційної безпеки та кібербезпеки Апарату РНБО України для інформаційно-аналітичного забезпечення діяльності Національного координаційного центру кібербезпеки та Групи.

Інформування має містити такі відомості:

назва суб'єкта забезпечення кібербезпеки, в інформаційно-комунікаційних системах якого зафіксовано кіберінцидент/кібератаку, контактні дані відповідальної за кіберзахист посадової особи;

тип кіберінциденту/кібератаки (відповідно до таксономії кіберінцидентів);

рівень критичності кіберінциденту/кібератаки;

короткий опис (контекст);

час виявлення кіберінциденту/кібератаки та час початку реагування на нього;

пропозиції щодо необхідності залучення інших суб'єктів забезпечення кібербезпеки.

10. Національний координаційний центр кібербезпеки веде облік таких повідомлень та координує дії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки відповідно до отриманої

інформації та з урахуванням надходження додаткової інформації про зміни в безпековому середовищі.

11. Суб'єкти, які є відповідальними за реагування на кіберінцидент/кібератаку, через наявну мережу вузлів MISP (Malware Information Sharing Platform) забезпечують обмін інформацією про кіберінцидент/кібератаку з усіма суб'єктами забезпечення кібербезпеки, представники яких входять до складу Національного координаційного центру кібербезпеки, а також з іншими суб'єктами забезпечення кібербезпеки, що є користувачами MISP, з дотриманням протоколу TLP (Traffic Light Protocol).

12. Національний координаційний центр кібербезпеки, CERT-UA та СБУ відповідають за інформування громадськості про кіберінцидент/кібератаку. Оприлюднення відповідної інформації здійснюється з урахуванням інтересів суб'єкта забезпечення кібербезпеки (атакованого об'єкта) та, у визначених законом випадках, після отримання дозволу слідчого (прокурора).

У разі необхідності таке інформування може здійснюватись іншими суб'єктами забезпечення кібербезпеки (як самостійно, так і додатково) за погодженням із суб'єктом, який є відповідальним за реагування на кіберінцидент/кібератаку та/або Національним координаційним центром кібербезпеки.

13. Суб'єкти, які є відповідальними за реагування на кіберінцидент/кібератаку, з урахуванням наявних сил і засобів визначають заходи реагування та порядок надання допомоги суб'єкту забезпечення кібербезпеки (атакованому об'єкту).

У разі необхідності, під час реагування можуть бути залучені додаткові ресурси (кадрові та/або технічні) інших основних суб'єктів національної системи кібербезпеки, міжнародних партнерів, приватних компаній (або окремих експертів), що провадять свою діяльність у сфері кібербезпеки.

14. Суб'єкти, які є відповідальними за реагування на кіберінцидент/кібератаку, регулярно інформують Національний координаційний центр кібербезпеки (через Службу з питань інформаційної безпеки та кібербезпеки Апарату РНБО України) про хід реагування на кіберінцидент/кібератаку, а також про завершення заходів з реагування на кіберінцидент/кібератаку протягом доби після такого завершення.

15. Суб'єкт забезпечення кібербезпеки, в системах якого зафіксовано кіберінцидент/кібератаку, вживає заходів щодо виконання рекомендацій, наданих суб'єктами забезпечення кібербезпеки, що здійснювали реагування на кіберінцидент/кібератаку.

ІІІ. РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ/КІБЕРАТАКИ «ЧЕРВОНОГО» ТА «ЧОРНОГО» РІВНЯ КРИТИЧНОСТІ

1. Суб'єкт, який є відповідальним за реагування на

кіберінцидент/кібератаку і визначив рівень критичності кіберінциденту/кібератаки як «червоний», невідкладно (не пізніше ніж за 30 хвилин з моменту фіксації) інформує про це керівника Групи через Службу з питань інформаційної безпеки та кібербезпеки Апарату РНБО України, яка визначає канали, способи та інструменти здійснення такого інформування.

2. Керівник Групи невідкладно інформує про ситуацію, що склалася, членів Національного координаційного центру кібербезпеки та членів Групи.

Не пізніше ніж через 2 години (у робочий час) або 4 години (поза робочим часом) з моменту такого інформування члени Групи прибувають у розпорядження керівника Групи.

До роботи Групи за рішенням її керівника можуть бути залучені представники центральних органів виконавчої влади, які відповідають за формування та реалізацію політики у сфері, до якої віднесено суб'єкт (суб'єкти) забезпечення кібербезпеки, в інформаційно-комунікаційних системах яких зафіксовано кіберінцидент/кібератаку.

3. Керівник Групи здійснює розподіл наявних сил і засобів реагування, а також об'єктів кіберзахисту, визначає завдання для членів Групи та особисто здійснює контроль за їх виконанням.

4. У випадку кіберінцидентів/кібератак «червоного» рівня критичності може здійснюватись комунікація з міжнародними партнерами.

Заходи з комунікації на політичному рівні (зокрема щодо загального інформування про ситуацію та опрацювання можливої допомоги щодо подолання наслідків) забезпечує МЗС, готуючи спільно з членами Групи офіційну заяву. Вказана комунікація може носити двосторонній або багатосторонній характер.

За дорученням керівника Групи така комунікація здійснюється протягом всього часу реагування на кіберінцидент/кібератаку за цим Порядком.

Основні суб'єкти національної системи кібербезпеки, до яких звертаються міжнародні партнери щодо кіберінциденту/кібератаки, інформують про це керівника Групи для організації відповідної комунікації (окрім комунікації за напрямом спеціальних та розвідувальних служб іноземних держав).

5. Інформування громадськості про кіберінциденти/кібератаки «червоного» рівня критичності здійснюється у формі спільних прес-релізів, що погоджуються керівником Групи та оприлюднюються (за можливості – одночасно) на інформаційних ресурсах Національного координаційного центру кібербезпеки, CERT-UA, СБУ та інших суб'єктів забезпечення кібербезпеки, що делегували своїх представників до Групи.

6. За результатами роботи Групи складається звіт, який розглядається та затверджується на засіданні Національного координаційного центру кібербезпеки, а також який є основою для посткризової комунікації членів Національного координаційного центру кібербезпеки з громадськістю.

Особливості реагування на кіберінциденти/кібератаки «чорного» рівня критичності

7. Для всіх випадків, які стосуються кіберінцидентів/кібератак «чорного» рівня критичності здійснюються заходи, аналогічні реагуванню на кіберінциденти/кібератаки «червоного» рівня критичності.

Додатково вживаються наступні заходи:

вивчається необхідність ініціювання введення режиму надзвичайної ситуації або надзвичайного стану для своєчасного подолання наслідків кіберінциденту/кібератаки;

здійснюється аналіз кібератаки на предмет наявності наслідків, які відповідно до норм міжнародного права досягають рівня, що прирівнюється до збройної агресії, невідкладно організовується робота з її атрибуції.

Керівник Групи за згодою членів Національного координаційного центру кібербезпеки може ініціювати проведення екстреного засідання Ради національної безпеки і оборони України.