ЗАТВЕРДЖЕНО
Розпорядження начальника
районної військової адміністрації
_____ № _____

ПОРЯДОК
реагування на різні види подій у кіберпросторі районної військової адміністрації

1. Цей порядок визначає процедури реагування відповідальними за кіберзахист працівниками районної військової адміністрації (далі – відповідальні за кіберзахист) на різні види подій у кіберпросторі районної військової адміністрації (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 відповідальними за кіберзахист 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.

Відповідальні за кіберзахист 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 відповідальними за кіберзахист послідовно такими етапами:

підготовка;
виявлення та аналіз;
стримування;
усунення;
відновлення;
аналіз ефективності заходів з реагування на кіберінциденти/кібератаки.

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

Підготовка до реагування на кіберінциденти/кібератаки починається

заздалегідь до того, як вони відбудуться, заради пом’якшення будь-якого впливу на суб’єкт забезпечення кібербезпеки.

6. Заходи з підготовки складаються з:

визначення переліку усіх інформаційних активів, послуг, систем та мереж, встановлення показників штатного функціонування систем та мереж суб’єктів забезпечення кібербезпеки;

розроблення та затвердження політик та процедур реагування на кіберінциденти/кібератаки, доведення їх персоналу суб’єкта забезпечення кібербезпеки;

підготовки інструментальних засобів, середовищ для виявлення підозрілої та зловмисної активності;

навчання користувачів щодо реагування та протидії кіберзагрозам та процедур сповіщення про них;

визначення порядку інформування, використання інформації про кіберзагрози для проактивного виявлення підозрілої поведінки та потенційної діяльності зловмисника;

підготовки інфраструктури для оброблення кіберінцидентів/кібератак, зокрема з урахуванням специфіки функціонування систем суб’єкта забезпечення кібербезпеки;

розроблення і тестування алгоритмів/порядку дій для стримування (локалізації) та ліквідації наслідків кіберінцидентів/кібератак.

7. На етапі виявлення та аналізу відповідальні за кіберзахист здійснюють виявлення кіберінциденту/кібератаки та визначають їх критичність для забезпечення пропорційності та/або співрозмірності подальших заходів з кіберзахисту реальним та потенційним ризикам.

8. Заходи з виявлення та аналізу передбачають: визначення факту кіберінциденту/кібератаки;

визначення категорії (рівня) критичності кіберінциденту/кібератаки;

інформування про кіберінцидент/кібератаку; пріоритетизацію кіберінциденту/кібератаки;

визначення масштабу проведення реагування на кіберінциденти/кібератаки;

збір та зберігання даних;

проведення технічного аналізу, зокрема: зіставлення подій між собою та документування їх хронології;

визначення підозрілої поведінки;

визначення першопричини (першоджерела) кіберінциденту/кібератаки та умов, що сприяють ескалації кіберінциденту/кібератаки;

збір індикаторів кіберзагроз;

аналіз загальних тактик, технік та процедур (далі – ТТП) зловмисника;

перевірку і перегляд масштабу проведення процесу реагування на кіберінциденти/кібератаки;

аналітичну підтримку з боку третіх сторін;

налаштування інструментів з виявлення кіберінцидентів/кібератак.

9. Відповідальні за кіберзахист 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.

10. На підставі визначеного рівня критичності кіберінциденту/кібератаки відповідальними за кіберзахист здійснює інформування керівництва та суб'єктів забезпечення кіберзахисту, а саме:

за низького (зеленого) або середнього (жовтого) рівня критичності – здійснюється інформування управління цифрової трансформації та сектору інформаційно-комп'ютерного забезпечення управління документального забезпечення апарату обласної військової адміністрації, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, Ситуаційного центру забезпечення кібербезпеки Служби безпеки України, відповідальних співробітників УСБУ в Тернопільській області.

за високого (помаранчевого), критичного (червоного) або надзвичайного (чорного) рівня критичності – здійснюється інформування управління цифрової трансформації та сектору інформаційно-комп'ютерного забезпечення управління документального забезпечення апарату обласної військової адміністрації, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, Ситуаційного центру забезпечення кібербезпеки Служби безпеки України, відповідальних співробітників УСБУ в Тернопільській області, Національного координаційного центру кібербезпеки при РНБО України та Департаменту кіберполіції Національної поліції України.

11. Інформація про кіберінцидент/кібератаку надається департаменту цифрової трансформації та сектору інформаційно-комп'ютерного забезпечення управління документального забезпечення апарату обласної державної адміністрації на електронні адреси digital@te.gov.ua та ikz@te.gov.ua, або за телефонами 0352517011 та 0352529131 відповідно.

12. Інформація про кіберінцидент/кібератаку надається суб'єктам національної системи забезпечення кібербезпеки такими шляхами:

урядовій команді реагування на комп'ютерні надзвичайні події України CERT-UA – https://cert.gov.ua, тел. +38 (044) 281-88-25, +38 (044) 281-88-05 або за допомогою форми на сайті https://cert.gov.ua/contact-us, через офіційну сторінку команди на Facebook: https://facebook.com/UACERT;

Ситуаційному центру забезпечення кібербезпеки Служби безпеки України – через систему обміну даними про кібератаки на базі програмної платформи MISP-UA (https://misp.gov.ua);

відповідальним співробітникам УСБУ в Тернопільській області Цапуну

Сергію Миколайовичу (+380982438996), Дубині Віталію Васильовичу (+380975283051) або співробітникам чергової служби Управління (+380673250800, (0352)524542);

Національному координаційному центру кібербезпеки – через СЕВ ОВВ РНБО України;

Департаменту кіберполіції Національної поліції України – на електронну адресу incident@cyberpolice.gov.ua.

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

тип кіберінциденту/кібератаки (відповідно до таксономії кіберінцидентів);

рівень критичності кіберінциденту/кібератаки;

короткий опис;

попередню оцінку: кібератака чи кіберінцидент;

підрозділ, ПІБ та контактні дані посадової особи, яка виявила кіберінцидент/кібератаку;

перелік суб'єктів, повідомлених про кіберінцидент/кібератаку;

інформацію чи потрібна допомога в реагуванні або реагування здійснюється власними силами.

14. Під час етапу стримування відповідальними за кіберзахист 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.

15. Оцінюючи напрям дій зі стримування, необхідно враховувати:

будь-які додаткові несприятливі впливи у певній сфері, вплив на доступність (можливість надання послуг клієнтам тощо);

тривалість процесу стримування, необхідні ресурси та ефективність стримування (наприклад, повне чи часткове стримування;

повне стримування чи рівень стримування невідомий);

будь-який вплив на спроможність збору, збереження, захисту і документування доказів.

16. До головних заходів зі стримування належать:

ізоляція уражених пристроїв один від одного та/або від пристроїв, які не були уражені. Необхідно врахувати операційні та/або бізнес-процеси та необхідність їх продовження (продовження надання послуг, наскільки це можливо);

створення образів пам'яті (дампів оперативної пам'яті) для збереження електронних доказів, їх використання в рамках розслідування інциденту;

оновлення фільтрів брандмауерів;

блокування несанкціонованого доступу, журналювання, ведення логів

(створення лог-файлів) щодо несанкціонованого доступу; блокування джерел поширення шкідливого програмного забезпечення;

встановлення правил блокування сервером доменних імен (DNS) відомих доменних імен зловмисника, а також тих, що можуть бути IP-адресами зловмисника (на основі аналізу);

закриття (блокування) мережевих портів та інтерфейсів на уражених системах/мережевих пристроях, через які може здійснюватися взаємодія зловмисника зі службами та сервісами уражених систем (наприклад, SSH, HTTP (HTTPS), SMTP, IMAP, FTP тощо), а також на неуражених системах/мережевих пристроях (лише за необхідності та при загрозі використання цих портів (інтерфейсів) зловмисником для досягнення власних цілей);

скасування привілейованого доступу користувачів, зміна паролів системного адміністратора, облікових записів служб/застосунків, якщо є підозра на проникнення в систему/мережу за допомогою привілейованого доступу.

17. Якщо будуть виявлені нові ознаки підозрілої поведінки та діяльності зловмисника, необхідно повернутися до етапу виявлення та аналізу, щоб повторно визначити заходи, необхідні для реагування на кіберінциденту/кібератаки.

Після успішного стримування (тобто, якщо немає нових ознак підозрілої поведінки, діяльності зловмисника, мінімізовано наслідки впливу зловмисника та визначено усі джерела поширення шкідливого програмного забезпечення) необхідно зберегти електронні докази для використання у подальшій роботі уповноваженими органами та розслідування правоохоронними органами, а також повторно налаштувати інструменти з виявлення кіберзагроз відповідно до отриманого досвіду і висновків та перейти до ліквідації наслідків і відновлення систем.

18. Заходи з усунення наслідків передбачають:

перевірку усіх заражених середовищ (систем, мереж, мережевих пристроїв, хостів, сховищ даних тощо) на предмет вразливостей;

повторне створення образів пам’яті елементів уражених середовищ, відновлення систем від заводських налаштувань;

часткове або повне відновлення технологічного, технічного, мережевого, іншого обладнання, що постраждало від наслідків кіберінциденту/кібератаки (за необхідності – заміна такого обладнання на нове);

заміну скомпрометованих артефактів артефактами із систем резервного копіювання та відновлення (відповідно до передбачених процедур перевірки артефактів на предмет компрометації, порушення властивостей інформації та будь-яких дій з ними);

встановлення патчів та оновлень;

вжиття заходів з заміни усіх паролів у скомпрометованих середовищах (системах/мережах);

моніторинг будь-яких ознак реагування зловмисника на заходи зі стримування.

19. Після ліквідації наслідків кіберінциденту/кібератаки необхідно продовжувати дії з виявлення та аналізу, щоб спостерігати за будь-якими ознаками повторного проникнення зловмисника або використання нових методів доступу. Якщо після завершення заходів із ліквідації наслідків буде виявлено підозрілу поведінку або активність зловмисника, необхідно повернутися до етапу технічного аналізу або стримування та виконати повторно всі заходи реагування, доки не буде ідентифіковано справжній масштаб компрометації та початкові вектори зараження. Якщо нової активності зловмисника не виявлено, можна переходити до етапу відновлення.

20. Заходи з відновлення передбачають:

повторне підключення відновлених/нових систем до мереж;

посилення безпеки периметра (наприклад, нові переліки правил брандмауера, списки управління доступом до граничного маршрутизатора і правила доступу з нульовим рівнем довіри (Zero Trust));

ретельне тестування систем, у тому числі заходів безпеки;

моніторинг операцій щодо підозрілої поведінки.

21. За результатами вжиття заходів з кіберзахисту відповідальні за кіберзахист проводять аналіз ефективності реагування на кіберінциденти/кібератаки.

Під час цього етапу забезпечується вивчення задокументованих даних щодо кіберінциденту/кібератаки, інформування керівництва, узагальнення та

проведення аналізу досвіду реагування для подальшого підвищення ефективності вжиття заходів з кіберзахисту у разі можливих кіберінцидентів/кібератак у подальшому.

22. Основні цілі етапу аналізу ефективності заходів реагування на кіберінциденти/кібератаки передбачають:

впевненість в усуненні та подоланні першопричин інциденту;

визначення проблем з програмним та апаратним забезпеченням, які необхідно розв’язати;

визначення проблем з організаційною політикою та процедурами, які необхідно розв’язати;

запровадження постійного перегляду й оновлення ролей персоналу суб’єкта забезпечення кібербезпеки, зон відповідальності та повноважень кожного фахівця (спеціаліста) суб’єкта забезпечення кібербезпеки;

визначення потреб у технічній підготовці, підготовці персоналу суб’єкта забезпечення кібербезпеки, відповідальних за кіберзахист;

удосконалення інструментів, необхідних для виконання заходів із захисту, виявлення, аналізу та/або реагування на кіберінциденти/кібератаки.