РОЗПОРЯДЖЕННЯ
ГОЛОВИ ГОЛОВАНІВСЬКОЇ РАЙОННОЇ ДЕРЖАВНОЇ АДМІНІСТРАЦІЇ КІРОВОГРАДСЬКОЇ ОБЛАСТІ

від **28 січня** 20**26** року **№ 9-р**

селище Голованівськ

Про взаємодію під час реагування на різні види подій у кіберпросторі Голованівської районної державної адміністрації

Відповідно до статей 6, 39, 41 Закону України "Про місцеві державні адміністрації", Закону України "Про основні засади забезпечення кібербезпеки України", постанов Кабінету Міністрів України від 04 квітня 2023 року № 299 "Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі", від 29 грудня 2021 року № 1426 "Про затвердження Положення про організаційно-технічну модель кіберзахисту", з метою забезпечення ефективності та оперативності реагування на кіберзагрози, захисту інформаційних ресурсів районної державної адміністрації:

1. Затвердити порядок реагування на події у кіберпросторі Голованівської районної державної адміністрації (додається).

2. Визначити БОНДАРЯ Олександра Миколайовича, головного спеціаліста відділу організації діяльності центрів надання адміністративних послуг, цифрового розвитку, цифрових трансформацій і цифровізації Голованівської районної державної адміністрації відповідальним за інформаційну безпеку у Голованівській районній державній адміністрації.

3. Забезпечити вжиття заходів до кіберзахисту, спрямованих на швидке виявлення та захист від кіберінцидентів/кібератак, належне інформування про них, запобігання негативним наслідкам та забезпечення надійності функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем та інших об'єктів кіберзахисту відповідно до порядку, затвердженого цим розпорядженням.

3. Контроль за виконанням цього розпорядження покласти на першого заступника голови районної державної адміністрації Голованя Юрія.

Голова районної державної адміністрації **Ігор КОВЕРДЯГА**

ЗАТВЕРДЖЕНО

Розпорядження голови
Голованівської районної
державної адміністрації
28 січня 2026 року № 9-р

ПОРЯДОК
реагування на події у кіберпросторі Голованівської районної державної адміністрації

1. Цей порядок визначає процедури реагування відповідальними за інформаційну безпеку працівниками районної державної адміністрації (далі – відповідальні за інформаційну безпеку) на різні види подій у кіберпросторі районної державної 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 року № 1426 "Про затвердження Положення про організаційно-технічну модель кіберзахисту".

3. Реагування на кіберінциденти/кібератаки здійснюється відповідальними за інформаційну безпеку 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.

4. Реагування на кіберінциденти/кібератаки здійснюється відповідальними за інформаційну безпеку 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.

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 інформаційну безпеку 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 інформаційну безпеку 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 інформаційну безпеку здійснюється невідкладне інформування керівництва та суб'єктів забезпечення кіберзахисту, а саме:

за низького (зеленого) або середнього (жовтого) рівня критичності – здійснюється інформування відділу забезпечення інформаційних систем і технологій апарату обласної державної адміністрації, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, Ситуаційного центру забезпечення кібербезпеки Служби безпеки України, відповідальних співробітників УСБУ в Кіровоградській області;

за високого (помаранчевого), критичного (червоного) або надзвичайного (чорного) рівня критичності – здійснюється інформування відділу забезпечення інформаційних систем і технологій апарату обласної державної адміністрації, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, Ситуаційного центру забезпечення кібербезпеки Служби безпеки України, відповідальних співробітників УСБУ в Кіровоградській області, Національного координаційного центру кібербезпеки при РНБО України та Департаменту кіберполіції Національної поліції України.

11. Інформація про кіберінцидент/кібератаку надається відділу забезпечення інформаційних систем і технологій апарату обласної державної адміністрації на електронну адресу: admin@kr-admin.gov.ua або за телефоном: (0522) 30 50 51.

12. Інформація про кіберінцидент/кібератаку надається суб'єктам національної системи забезпечення кібербезпеки такими каналами зв'язку: 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, Ситуаційному центру забезпечення кібербезпеки Служби безпеки України – через систему обміну даними про кібератаки на базі програмної платформи MISP-UA (https://misp.gov.ua); 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 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 інформаційну безпеку 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. До головних заходів зі стримування належать:

ізоляція уражених систем, мереж, мережевих сегментів та пристроїв один від одного та/або від систем і мереж, 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 зловмисника;

встановлення правил блокування сервером доменних імен (DNS) відомих доменних імен зловмисника, а також тих, що можуть бути IPадресами 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.

16. Під час етапу усунення відповідальні за інформаційну безпеку вживають заходів до усунення артефактів інциденту (видалення зловмисного коду, створення повторного образу пам'яті елементів "заражених" систем) та ліквідації наслідків кіберінциденту/кібератаки для інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, інформації та даних, що ними обробляються.

17. 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;

зміну усіх паролів у скомпрометованих середовищах (системах/мережах); моніторинг будь-яких ознак реагування зловмисника на заходи зі стримування.

18. На етапі відновлення відповідальними за інформаційну безпеку вживаються заходи з 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.

19. 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.

20. За результатами вжиття заходів з кіберзахисту відповідальні за інформаційну безпеку забезпечують 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.

_____