РОЗПОРЯДЖЕННЯ

КРОПИВНИЦЬКОГО МІСЬКОГО ГОЛОВИ

від "____"_____ 20 ___ року №_____

Про затвердження Плану реагування на кіберінциденти та/або кібератаки

Керуючись статтею 140 Конституції України, статтею 42 Закону України "Про місцеве самоврядування в Україні", вимогами постанов Кабінету Міністрів України від 13 листопада 2025 року № 1471 "Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності", від 26 листопада 2025 року № 1533 "Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози", наказу Адміністрації Держспецзв'язку від 18 лютого 2026 № 143 "Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози":

1. Затвердити План реагування на кіберінциденти та/або кібератаки (далі – План), що додається.

2. Керівникам виконавчих органів Кропивницької міської ради зі статусом юридичної особи, районних в місті Кропивницькому рад, Новенського старостинського округу:

1) забезпечити дотримання Плану реагування на кіберінциденти та/або кібератаки;

2) призначити у виконавчих органах відповідальну особу за реагування на кіберінциденти та/або кібератаки та інформування суб'єктів забезпечення кібербезпеки;

3) забезпечити у підпорядкованих комунальних підприємствах, установах і закладах призначення відповідальних осіб за реагування на кіберінциденти та/або кібератаки та інформування суб'єктів забезпечення кібербезпеки, розробку і затвердження відповідних планів реагування;

4) надати управлінню інформаційних технологій Кропивницької міської ради список осіб (прізвище, ім'я, по батькові, посада, контактний телефон) відповідальних за реагування на кіберінциденти та/або кібератаки та

інформування суб’єктів забезпечення кібербезпеки у виконавчому органі. У випадку зміни відповідальної особи здійснювати інформування управління інформаційних технологій;

5) забезпечити вжиття заходів до кіберзахисту, спрямованих на швидке виявлення та захист від кіберінцидентів та/або 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 та інших об’єктів кіберзахисту відповідно до порядку, затвердженого цим розпорядженням.

3. Особам, відповідальним за реагування на кіберінциденти та/або кібератаки, інформування суб’єктів забезпечення кібербезпеки у комунальних підприємствах, установах і закладах Кропивницької міської ради, невідкладно інформувати управління інформаційних технологій Кропивницької міської ради про кіберінциденти та/або кібератаки та інші випадки несанкціонованого втручання в роботу комунікаційного обладнання, інформаційно-комунікаційних і автоматизованих систем.

4. План є обов’язковим для виконання виконавчими органами Кропивницької міської ради, районними в місті Кропивницькому радами і Новенським старостинським округом під час вжиття заходів із кіберзахисту відповідно до етапів реагування на різні види подій у кіберпросторі в інформаційно-комунікаційних системах міської ради.

5. Контроль за виконанням цього розпорядження залишаю за собою.

Заступник міського голови з питань діяльності виконавчих органів ради **Олександр МОСІН**

Терещенко Сергій 35 83 70

ЗАТВЕРДЖЕНО

Розпорядження міського голови
“ ” _____2026 року № ___

П Л А Н
реагування на кіберінциденти та кібератаки

1. План реагування на кіберінциденти та/або кібератаки є внутрішнім документом Кропивницької міської ради і регламентує організацію та порядок вжиття заходів у разі виникнення різних видів подій у кіберпросторі (далі – кіберінциденти та/або кібератаки, КІ/КА) і спрямований на виявлення та захист від кіберінцидентів та/або кібератак, запобігання та мінімізацію їх наслідків, швидке відновлення роботи інформаційно-комунікаційних і автоматизованих систем виконавчих органів Кропивницької міської ради, районних у місті Кропивницькому рад і Новенського старостинського округа.

2. В цьому Плані терміни вживаються в такому значенні:

артефакти події кібербезпеки – це будь-які інформаційні елементи систем суб'єкта забезпечення кібербезпеки, що свідчать про роботу, фіксують дії або є наслідками кіберінциденту;

індикатори кіберзагроз (Indicators of Threat/Compromise, IoC) – це технічні дані та ознаки (IP-адреси, хеші файлів, записи в логах), що свідчать про те, що інформаційна система або мережа зазнала кібератаки, або на неї здійснюється спроба зламу;

кіберінцидент – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти

кіберзахисту;

кіберзагроза – це наявні або потенційні явища, дії чи чинники в кіберпросторі, які можуть порушити конфіденційність, цілісність чи доступність даних, завдати шкоди комп'ютерним системам, мережам або користувачам;

кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на захист від кіберзагроз, забезпечення кібербезпеки, стійкості, цілісності, доступності та конфіденційності інформаційних ресурсів у кіберпросторі, а також здатності інфраструктури до їх обробки;

подія кібербезпеки – ідентифікована (навмисна або ненавмисна) дія в системі, електронній комунікаційній мережі або стан системи, електронної комунікаційної мережі, яка становить або може становити загрозу сталому, надійному та штатному режиму функціонування системи, електронної комунікаційної мережі та/або порушення конфіденційності, цілісності, доступності інформації в системі, електронній комунікаційній мережі та бути ознакою або передумовою кіберінциденту, кібератаки;

суб'єкти національної системи реагування – Національний координаційний центр кібербезпеки (НКЦК) при РНБО України, Державна служба спеціального зв'язку та захисту інформації України (ключовий орган, до складу якого входить CERT-UA – команда реагування на комп'ютерні надзвичайні події), Служба безпеки України (Ситуаційний центр забезпечення кібербезпеки СБУ, регіональний центр забезпечення кібербезпеки СБУ);

суб'єкти забезпечення кібербезпеки в Україні – державні органи (Держспецзв'язку, СБУ, Нацполіція, Міноборони, НБУ), органи місцевого самоврядування, військові формування, а також підприємства та організації, що захищають критичну інфраструктуру. Вони формують національну систему кібербезпеки, здійснюючи кіберзахист, протидію кіберзагрозам та реагування на кіберінциденти.

Інші терміни вживаються у значеннях, наведених в Законах України "Про основні засади забезпечення кібербезпеки України", "Про критичну інфраструктуру", "Про захист інформації в інформаційно-комунікаційних системах", "Про Державну службу спеціального зв'язку та захисту інформації України".

3. Цілями цього Плану є:

забезпечення цілісності і доступності обладнання, систем, інформаційних ресурсів і пов'язаних з ними даних міської ради, збереження та захист службової і конфіденційної інформації та інформації, що обробляється в інформаційно-комунікаційних системах та державних інформаційних ресурсах

Кропивницької міської ради;

забезпечення послідовної стратегії реагування на кіберінциденти та/або кібератаки;

мінімізація репутаційних ризиків міської ради;

відновлення роботи після кіберінцидентів та/або кібератак.

З метою виконання Плану у кожному виконавчому органі Кропивницької міської ради, районних у місті Кропивницькому радах і Новенському старостинському окрузі призначаються особи, відповідальні за реагування на кіберінциденти та/або кібератаки та інформування суб'єктів забезпечення кібербезпеки (далі – відповідальна особа). У Виконавчому комітеті Кропивницької міської ради виконання функцій відповідального за реагування на кібератаки та кіберінциденти, інформування суб'єктів забезпечення кібербезпеки, виконання функцій керівника з кіберзахисту, координації роботи відповідальних осіб, взаємодії з іншими суб'єктами кібербезпеки та контроль за дотриманням вимог законодавства у сфері кібербезпеки покладаються на начальника відділу захисту інформації управління інформаційних технологій Кропивницької міської ради.

У разі потреби, під час реагування на події кібербезпеки, відповідно до законодавства можуть залучатися додаткові ресурси (кадрові та/або технічні) інших суб'єктів національної системи реагування, міжнародних партнерів, суб'єктів господарювання усіх форм власності або окремих експертів, що провадять діяльність у сфері кібербезпеки.

4. Реагування на кіберінциденти та/або кібератаки, кіберзагрози здійснюється за такими етапами:

підготовка до реагування на кіберінциденти та/або кібератаки та кіберзагрози,

виявлення, аналіз та інформування про кіберінциденти та/або кібератаки та кіберзагрози,

стримування, усунення наслідків та відновлення після кіберінцидентів та/або кібератак та кіберзагроз, а також аналіз ефективності заходів реагування на кіберінциденти та/або кібератаки та кіберзагрози.

Вжиті заходи повинні забезпечити:

швидке виявлення кіберінциденту та/або кібератаки;

належне інформування про їх виникнення уповноважених органів та залучених сторін;

запобігання, мінімізацію та усунення негативних наслідків;

виявлення вразливостей;

відновлення надання суб'єктами забезпечення кібербезпеки послуг;

сталість і надійність систем та інших об'єктів кіберзахисту, що належать суб'єктам забезпечення кібербезпеки;

унеможливлення повторної реалізації виявленого кіберінциденту, а щодо кібератак – збереження можливих електронних доказів.

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

Під час зазначеного етапу створюються організаційні, технічні та кадрові умови для ефективного реагування на кіберінциденти та/або кібератаки та кіберзагрози, зокрема:

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 та/або 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;

створення технічних можливостей підключення власних систем до засобів і технічних систем реагування суб'єктів національної системи реагування, зокрема до системи реагування на кіберінциденти та/або кібератаки, кіберзагрози щодо об'єктів кіберзахисту, функціонування та розвиток якої забезпечується Державним центром кіберзахисту Держспецзв'язку.

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

7. Заходи з виявлення та аналізу передбачають:

визначення факту кіберінциденту та/або кібератаки;

визначення категорії (рівня) критичності кіберінциденту та/або кібератаки;

інформування про кіберінцидент та/або кібератаку;

пріоритетизацію кіберінциденту та/або кібератаки;

визначення масштабу проведення реагування на кіберінциденти та/або кібератаки;

збір та зберігання даних;

проведення технічного аналізу, зокрема: зіставлення подій між собою та документування їх хронології; визначення підозрілої поведінки; визначення першопричини (першоджерела) кіберінциденту та/або кібератаки та умов, що

сприяють ескалації кіберінциденту та/або кібератаки; збір індикаторів кіберзагроз; і аналіз загальних тактик, технік та процедур зловмисника; перевірку перегляд масштабу проведення процесу реагування на кіберінциденти та/або кібератаки;

аналітичну підтримку з боку третіх сторін;

налаштування інструментів з виявлення кіберінцидентів та/або кібератак.

Визначення критичності кіберінциденту та/або кібератаки проводиться 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 не загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем;

рівень 1, низький (зелений) – кіберінцидент 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 3, високий (помаранчевий) – кіберінцидент безпосередньо загрожує сталому, надійному та штатному режиму функціонування систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що в них обробляються, внаслідок чого виникають потенційні загрози для національної безпеки і оборони, стану навколишнього природного середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою;

рівень 4, критичний (червоний) – кіберінцидент безпосередньо загрожує сталому, надійному та штатному режиму функціонування кількох систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що в них 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;

рівень 5, надзвичайний (чорний) – кіберінцидент безпосередньо загрожує сталому, надійному та штатному режиму функціонування значної кількості систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що в них обробляються, внаслідок чого виникають невідворотні загрози для повноцінного функціонування держави або загроза життю людей.

Визначення категорії кіберінциденту здійснюється відповідно до національної таксономії кіберінцидентів затвердженої наказом Адміністрації Держспецзв'язку від 18.02.2026 № 143 "Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози".

Якщо подія кібербезпеки класифікована як кібератака, відповідальні

особи невідкладно інформують про неї в порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози:

відділ захисту інформації управління інформаційних технологій Кропивницької міської ради (тел. 35 83 70);

Національну команду реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України - CERT-UA (e-mail: incidents@cert.gov.ua) або за телефоном +38 (044) 281-88-25;

Національний координаційний центр кібербезпеки (e-mail: report@ncscc.gov.ua);

ситуаційний центр забезпечення кібербезпеки СБУ (e-mail: incident@dis.gov.ua);

регіональний центр забезпечення кібербезпеки Служби безпеки України в Кіровоградській області (e-mail: cybercentre_kvg@ssu.gov.ua);

сектор з кіберзахисту Управління Державної служби спеціального зв'язку та захисту інформації України в Кіровоградській області (e-mail: cyber_kr@cip.gov.ua).

Крім того:

у випадку отримання повідомлень з погрозами терористичного змісту (погрози, повідомлення про мінування тощо) відповідальні особи невідкладно інформують про них територіальний підрозділ Департаменту кіберполіції Національної поліції України (e-mail: kg@cyberpolice.gov.ua, andrii.bielov@cyberpolice.gov.ua);

у випадку отримання повідомлень про зовнішні кіберзагрози, спрямовані проти національної безпеки, та/або повідомлень в яких виявлено ознаки дій або потенційних можливостей іноземних держав, організацій та осіб, відповідальні особи невідкладно інформують про них управління Служби безпеки України в Кіровоградській області.

8. Повідомлення про кіберінцидент/кібератаку має містити таку інформацію:

джерело виявлення кіберінциденту, кібератаки, кіберзагрози;

категорію і тип кіберінциденту, кібератаки (відповідно до таксономії кіберінцидентів);

короткий опис;

заархівований з паролем EML-файл повідомлення, пароль до архіву (у випадку повідомлення про отримання підозрілих листів на електронну скриньку);

назву виконавчого органу міської ради, який здійснює інформування про кіберінцидент/кібератаку;

інформацію чи потрібна допомога в реагуванні (за необхідності);

повідомлення про отримання погроз терористичного змісту, яке надсилається територіальному підрозділу Департамента кіберполіції Національної поліції України повинно містити скріншот повідомлення з

відображенням інформації про відправника, отримувача, дати і часу отримання.

9. Інформування про кіберінциденти, кібератаки та кіберзагрози здійснюється безперервно в режимі, наближеному до реального часу. Власники або розпорядники систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, відповідно до порядку обміну інформацією невідкладно (протягом години) повідомляють галузевій або регіональній команді реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) про всі кіберінциденти.

10. Суб'єкти національної системи реагування після отримання та опрацювання повідомлень про кіберінциденти, кібератаки, кіберзагрози надають суб'єктам забезпечення кібербезпеки рекомендації щодо можливих заходів реагування та технічної підтримки (у разі потреби).

11. Якщо під час технічного дослідження національною командою реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) або відповідною галузевою/регіональною командою реагування на кіберінциденти, кібератаки, кіберзагрози виявлено ознаки кримінального правопорушення, така інформація невідкладно (протягом години) передається до СБУ.

Суб'єкти забезпечення кібербезпеки надають національній команді реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), регіональному центру забезпечення кібербезпеки Служби безпеки України в Кіровоградській області безпосередній доступ до систем, безпосередньо пов'язаних із заходами реагування.

Адміністрація Держспецзв'язку та Служба безпеки України з метою вжиття заходів оперативного реагування на кіберінциденти, кібератаки, кіберзагрози в межах повноважень надають вимоги про реагування, які є обов'язковими до виконання суб'єктами забезпечення кібербезпеки

12. Під час етапу стримування, усунення наслідків та відновлення відповідальні особи самостійно або разом із суб'єктами національної системи реагування вживають заходів до зниження негативного впливу кіберінциденту, кібератаки, запобігання порушенню безпеки, несанкціонованому втручанню в їх роботу, забезпечення сталого, надійного та штатного режиму функціонування систем, захищеності (конфіденційності, цілісності і доступності) інформації та даних, що у них обробляються.

Оцінюючи напрям дій зі стримування, необхідно враховувати:

будь-які додаткові несприятливі впливи у певній сфері, вплив на доступність (можливість надання послуг 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.

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;

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.

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 кіберінцидент та/або кібератаку.

Під час етапу усунення відповідальні за кіберзахист вживають заходи стрямовані на усунення артефактів події кібербезпеки та ліквідації її наслідків для інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, інформації та даних, що ними обробляються.

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 та/або кібератаки (за необхідності – заміна такого обладнання на нове);

заміну скомпрометованих елементів елементами із систем резервного копіювання та відновлення (відповідно до передбачених процедур їх перевірки 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 можливих ознак реагування зловмисника на заходи зі стримування.

13. Після ліквідації наслідків кіберінциденту та/або 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.

14. На етапі відновлення відповідальними за кіберзахист 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.

15. 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 чи нештатної роботи систем і обладнання.

16. Під час етапу проведення аналізу ефективності реагування на кіберінциденти, кібератаки або кіберзагрози забезпечується документування інциденту шляхом формування звіту про реагування на кіберінцидент, кібератаку або кіберзагрозу, інформування відповідних галузевих/регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози відповідно до порядку обміну інформацією, удосконалення захисних механізмів систем і мереж, перегляд внутрішньої документації та політик безпеки для запобігання подібним інцидентам у майбутньому, а також застосування набутого досвіду для покращення управління майбутніми кіберінцидентами, кібератаками або кіберзагрозами.

Результати такого аналізу враховуються під час оновлення планів реагування на кіберінциденти, кібератаки або кіберзагрози, внутрішніх політик кібербезпеки та плану кіберзахисту, а також під час планування і проведення

навчань, тренувань та інших заходів підготовки персоналу до реагування на кіберінциденти, кібератаки або кіберзагрози.

17. Інформація про кіберінцидент, кібератаку щодо систем та про їх наслідки є відкритою інформацією.

18. Інформація про характер, технічні та інші деталі кіберінциденту, кібератаки щодо систем належить до інформації з обмеженим доступом, якщо вона відповідає хоча б одному з таких критеріїв:

містить неоприлюднені відомості про архітектуру, конфігурацію, технічні характеристики або вразливості системи, щодо якої здійснено кіберінцидент, кібератаку;

містить відомості про скомпрометовані облікові записи, системи, вектори реалізації кіберінцидентів, кібератак або масштаби впливу, які можуть бути використані для повторних кіберінцидентів, кібератак;

безпосередньо стосується або дає змогу встановити перебіг, зміст або результати оперативно-розшукових, контррозвідувальних заходів, слідчих дій або розвідувальної діяльності;

надана з вимогою обмеження доступу міжнародними, міжурядовими чи приватними партнерами суб'єктів національної системи реагування;

дає змогу ідентифікувати фізичних чи юридичних осіб або містить персональні дані осіб, пов'язаних з кіберінцидентом, кібератакою.

19. Інформація про характер, технічні та інші деталі кіберінциденту, кібератаки, віднесена до інформації з обмеженим доступом, може бути повністю або частково розкрита власником або розпорядником систем відповідно до вимог Законів України "Про інформацію", "Про доступ до публічної інформації" у такому разі:

у межах функціонування національної системи реагування або національної системи обміну інформацією за умови, що таке розкриття є обґрунтовано необхідним для виконання визначених законодавством повноважень суб'єктів національної системи реагування, залучених до реагування на кіберінциденти та кібератаки, обміну інформацією про кіберінциденти, кібератаки чи розслідування кіберінцидентів та кібератак;

за погодженням із суб'єктом національної системи реагування, який прийняв рішення про обмеження доступу, у разі потреби забезпечення координації реагування або розслідування кіберінциденту та кібератаки;

коли розкриття є необхідним для запобігання подальшим кіберінцидентам і кібератакам або мінімізації їх наслідків.

Таке розкриття здійснюється за умови, якщо обробка інформації буде здійснюватися з визначеною метою розкриття, а також якщо це не створює загроз національній безпеці України, не порушує вимог законодавства про захист персональних даних, комерційної, банківської, державної таємниці або інших вимог захисту інформації, визначених законом.

20. Інформація про індикатори кіберзагроз, отримана під час реагування на кіберінциденти, кібератаки, кіберзагрози, є відкритою інформацією і поширюється у порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, визначеному Адміністрацією Держспецзв'язку, а також може публічно поширюватися для виявлення загроз та запобігання ним іншими суб'єктами національної системи реагування.

Особливості реагування на кіберінциденти високого (помаранчевого), критичного (червоного) та надзвичайного (чорного) рівня критичності

21. Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузеві або регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози, інші суб'єкти національної системи реагування мають право самостійно розпочати реагування на кіберінциденти високого (помаранчевого), критичного (червоного) та надзвичайного (чорного) рівня критичності без попереднього погодження із суб'єктом забезпечення кібербезпеки, якщо зволікання може призвести до непоправних наслідків для національної безпеки, оборони, функціонування критичної інфраструктури або життя людей.

Про початок таких дій національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузева або регіональна команда реагування на кіберінциденти, кібератаки, кіберзагрози негайно інформує керівника з кіберзахисту або відповідальну особу, яка виконує функції та завдання керівника з кіберзахисту, суб'єкта забезпечення кібербезпеки.