



РОЗПОРЯДЖЕННЯ

від 11 березня 2026 року

№ 30-в

Про затвердження Плану реагування на кіберінциденти та кібератаки в інформаційно-комунікаційних системах виконавчого комітету Миргородської міської ради

Відповідно до п. 20 ч. 4 ст. 42 Закону України «Про місцеве самоврядування в Україні», Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №2163-VIII, Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» від 27.03.2025 №4336-IX, Плану реалізації Стратегії кібербезпеки України, схваленого рішенням Ради національної безпеки і оборони України від 30.12.2021, Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26.11.2025 №1533, з метою підвищення кіберзахисту інформації, що створюється, зберігається та обробляється в інформаційно-комунікаційних системах виконавчого комітету Миргородської міської ради:

1. Затвердити План реагування на кіберінциденти та кібератаки в інформаційно-комунікаційних системах виконавчого комітету Миргородської міської ради (додається).
2. Відділу інформаційних технологій та комп'ютерного забезпечення міської ради (Нестефоренко Р.Ю.), відповідальному за організацію та забезпечення захисту інформації, забезпечити вжиття заходів із кіберзахисту, спрямованих на швидке виявлення та захист від кіберінцидентів/кібератак, належне інформування про них, запобігання негативним наслідкам, їх мінімізацію та усунення, виправлення вразливостей, а також відновлення сталості і надійності функціонування інформаційно-комунікаційних систем, технологічних систем та інших об'єктів кіберзахисту відповідно до Плану, затвердженого цим розпорядженням.
3. Керівникам виконавчих органів міської ради, посадовим особам виконавчого комітету Миргородської міської ради забезпечити дотримання Плану реагування на кіберінциденти та кібератаки.
4. Організацію виконання цього розпорядження покласти на відділ інформаційних технологій та комп'ютерного забезпечення (Нестефоренко Р.Ю.) та відповідального за організацію та забезпечення захисту інформації, а контроль за виконанням – на керуючу справами виконавчого комітету Нікітченко А.Б.

Міський голова

Сергій СОЛОМАХА

ПЛАН

реагування на кіберінциденти та кібератаки в інформаційно-комунікаційних системах виконавчого комітету Миргородської міської ради

1. Цей План визначає процедури реагування відповідальними за кіберзахист працівниками виконавчого комітету Миргородської міської ради (далі - відповідальні за кіберзахист) на різні види подій у кіберпросторі виконавчого комітету Миргородської міської ради (далі - кіберінциденти/кібератаки) та категорії (рівні) їх критичності.

Реагування на кіберінциденти/кібератаки здійснюється з урахуванням вимог Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 р. № 1533.

2. У цьому порядку терміни вживаються у значеннях, наведених у 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” (зі змінами, внесеними постановою Кабінету Міністрів України від 20 грудня 2024 р. № 1468) та Національним планом реагування, затвердженим постановою Кабінету Міністрів України від 26 листопада 2025 р. № 1533.

3. Реагування на кіберінциденти та/або кібератаки забезпечується відповідальними за кіберзахист шляхом здійснення заходів з кіберзахисту, спрямованих на своєчасне виявлення та протидію кіберінцидентам і кібератакам, належне інформування про такі події, запобігання їх негативним наслідкам, мінімізацію та усунення таких наслідків, усунення виявлених вразливостей, а також відновлення сталого, безперервного та надійного функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем та інших об'єктів кіберзахисту.

Відповідальні за кіберзахист здійснюють зазначені заходи відповідно до методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених Адміністрацією Державної служби спеціального зв'язку та захисту інформації України.

Виконавчий комітет Миргородська міська рада як суб'єкт забезпечення кібербезпеки є учасником національної системи реагування на кіберінциденти, кібератаки та кіберзагрози та забезпечує взаємодію з іншими суб'єктами такої системи відповідно до Національного плану реагування.

4. Реагування на кіберінциденти/кібератаки здійснюється відповідальними за кіберзахист у взаємодії з суб'єктами національної системи реагування послідовно такими етапами:

- 1) підготовка;
- 2) виявлення та аналіз;
- 3) стримування;
- 4) усунення;
- 5) відновлення;
- 6) 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 завчасного 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;
- планування заходів реагування з урахуванням результатів оцінки ризиків кібербезпеки;
- забезпечення організаційної та технічної готовності до обміну інформацією з суб'єктами національної системи реагування, у тому числі CERT-UA;
- підготовки до можливого залучення зовнішніх команд реагування (CSIRT) у разі кіберінцидентів високого та критичного рівнів.

7. Виконавчий комітет Миргородської міської ради може створювати власну команду реагування на кіберінциденти та загрози (CSIRT) або залучати зовнішні команди реагування, які відповідають встановленим вимогам.

Інформація про створення або залучення такої команди доводиться до відома суб'єктів національної системи реагування не пізніше ніж протягом 15 календарних днів.

8. 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.

9. Заходи з виявлення та аналізу передбачають:

- визначення факту кіберінциденту/кібератаки;
- визначення категорії (рівня) критичності кіберінциденту/кібератаки;
- інформування про кіберінцидент/кібератаку;
- пріоритизацію 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.

10. 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 природного 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 природного 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.

11. З урахуванням визначеного рівня критичності кіберінциденту та/або кібератаки відповідальні за кіберзахист забезпечують інформування керівництва виконавчого комітету Миргородської міської ради та відповідних суб'єктів забезпечення кібербезпеки, а саме:

У разі низького (зеленого) або середнього (жовтого) рівня критичності - здійснюється інформування керівництва виконавчого комітету Миргородської міської ради, відповідального за організацію та забезпечення захисту інформації у виконавчому комітеті Миргородської міської ради, Полтавської обласної військової адміністрації (у межах повноважень), урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, Ситуаційного центру забезпечення кібербезпеки Служби безпеки України, а також відповідальних співробітників Управління Служби безпеки України в Полтавській області.

У разі високого (помаранчевого), критичного (червоного) або надзвичайного (чорного) рівня критичності - здійснюється інформування керівництва Миргородської міської ради, відповідального за організацію та забезпечення захисту інформації у виконавчому комітеті Миргородської міської ради, Полтавської обласної військової адміністрації (у межах повноважень), урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, Ситуаційного центру забезпечення кібербезпеки Служби безпеки України, відповідальних співробітників Управління Служби безпеки України в Полтавській області, Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України та Департаменту кіберполіції Національної поліції України.

12. Інформація про кіберінцидент та/або кібератаку надається відповідним суб'єктам національної системи забезпечення кібербезпеки України такими способами:

- Урядовій команді реагування на комп'ютерні надзвичайні події України CERT-UA - через офіційний вебсайт <https://cert.gov.ua>, за контактними телефонами, визначеними CERT-UA, за допомогою електронної форми зворотного зв'язку на офіційному вебсайті, а також через офіційні канали комунікації команди;

- 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 Управління Служби безпеки України в Полтавській області - через визначені канали оперативного зв'язку та чергові служби Управління;

- Національному координаційному центру кібербезпеки - через систему електронної взаємодії органів виконавчої влади Ради національної безпеки і оборони України;

- Департаменту кіберполіції Національної поліції України - шляхом направлення повідомлення на офіційну електронну адресу, визначену Департаментом для повідомлень про кіберінциденти та кібератаки.

13. Обмін інформацією про кіберінциденти та кібератаки може здійснюватися із використанням національних інформаційних систем обміну даними у сфері кібербезпеки відповідно до вимог Національного плану реагування.

14. 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.

15. 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.

16. 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.

17. 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 (дампов 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 відомих доменних імен (DNS) 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.

18. 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.

19. Під час етапу усунення відповідальні за кіберзахист вживають заходів до усунення артефактів інциденту та ліквідації наслідків кіберінциденту/кібератаки для інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, інформації та даних, що ними обробляються.

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

21. 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.

22. 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.

23. 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.

24. 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.

25. У разі кіберінцидентів або кібератак високого, критичного чи надзвичайного рівня може здійснюватися публічне інформування про факт реагування та усунення наслідків відповідно до порядку, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 р. № 1533, з урахуванням вимог щодо захисту інформації з обмеженим доступом.

26. 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.

**Керуюча справами
виконавчого комітету**

Антоніна НІКІТЧЕНКО