ЗАТВЕРДЖЕНО

розпорядження міського голови

від 18 липня 2025 року № 139

**ПЛАН**

**реагування на кіберінциденти та кібератаки**

**у виконавчому комітеті Ніжинської міської ради**

**та виконавчих органах Ніжинської міської ради**

**І. Загальні положення**

План реагування на кіберінциденти та кібератаки у виконавчому комітеті Ніжинської міської ради та виконавчих органах Ніжинської міської ради (далі – План) є внутрішнім документом, що регламентує організацію й порядок вжиття заходів у разі виникнення різних видів подій у кіберпросторі і спрямований на виявлення та захист від кіберінцидентів/кібератак, запобігання та мінімізацію їх наслідків, швидке відновлення роботи виконавчого комітету.

Даний план розроблений у відповідності з вимогами Закону України “Про основні засади забезпечення кібербезпеки України”, постанови Кабінету Міністрів України від 04.04.2023 № 299 “Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі та Методичних рекомендаціях щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених наказом Адміністрації державної служби спеціального зв’язку та захисту інформації в Україні від 03.07.2023 № 570.

Цілями цього Плану є:

* забезпечення цілісності і доступності систем, мереж і пов’язаних з ними даних виконавчого комітету Ніжинської міської ради, збереження та захист конфіденційності інформації;
* забезпечення реагування на системні та мережеві загрози, які ставлять під загрозу дані та інформаційні системи виконавчого комітету Ніжинської міської ради;
* мінімізація репутаційних ризиків;
* відновлення роботи після кіберінцидентів/кібератак, пов’язаних з комп’ютерною або мережевою безпекою чи іншого типу витоку даних.

**ІІ. Реагування на кіберінциденти/кібератаки**

Здійснення заходів з координації, підтримки, виконання реагування на кіберінциденти/кібератаки здійснюється відповідальною особою за реагування на кіберінциденти, кібератаки (далі- Відповідальна особа).

Відповідальна особа визначає орієнтовні терміни реагування на кіберінциденти/кібератаки, а також, за потреби, осіб, які мають бути залучені до реагування.

Відповідальна особа вживає заходів відповідно до Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні

види подій у кіберпросторі, затверджених наказом Адміністрації державної служби спеціального зв’язку та захисту інформації в Україні від 03.07.2023 № 570.

Відповідальна особа для проведення аналізу, усунення наслідків та відновлення процесів після кіберінциденту/кібератаки (у разі необхідності) має право звернутися до Урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA, Державного центру кіберзахисту Держспецзв’язку, Управління цифрової трансформації, інформаційних технологій, розвитку електронних та адміністративних послуг Чернігівської ОДА з метою залучення їх представників/експертів (далі – експерти).

**ІІІ. Етапи реагування на кіберінциденти/кібератаки**

Реагування на кіберінциденти/кібератаки здійснюється послідовно такими етапами:

1. **Етап підготовки**, який включає вжиття заходів з вивчення та дослідження сучасних видів кіберінцидентів/кібератак, виявлення активів та ризиків, які можуть стати цілями для зловмисників, розроблення механізмів запобігання та протидії можливим кіберінцидентам/кібератакам, вдосконалення можливостей реагування та запобігання кіберінцидентам/кібератакам шляхом забезпечення достатнього рівня безпеки систем, мереж, додатків та процесів обробки даних.

Заходи захисту від кіберзагроз на етапі підготовки:

1. розроблення та затвердження політик та процедур реагування на кіберінциденти/кібератаки, проведення навчань щодо їх засвоєння та використання посадовими особами виконавчого комітету та виконавчих органів міської ради;
2. навчання посадових осіб виконавчого комітету та виконавчих органів міської ради щодо реагування та протидії кіберзагрозам та процедур сповіщення про них;
3. визначення порядку інформування про кіберзагрози для активного виявлення підозрілої поведінки та потенційної діяльності зловмисника;
4. регулярний аудит інформаційних систем та мереж на предмет вразливостей, оновлення програмного забезпечення.
5. **Етап виявлення та аналізу**, який передбачає виявлення та оцінювання можливих кіберінцидентів/кібератак, визначення того, чи стався кіберінцидент/кібератака, визначення типу та масштабу компрометації систем/мереж, що були уражені.

Заходи з виявлення та аналізу:

1. збір інформації щодо підозрілої поведінки в мережі;
2. визначення та підтвердження, що ймовірний або виявлений кіберінцидент/кібератака стався або триває;
3. визначення категорії (рівня) критичності кіберінциденту/кібератаки відповідно до Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених Адміністрацією Держспецзв’язку;
4. відповідальна особа інформує керівництво виконавчого комітету чи виконавчого органу міської ради та Урядову команду реагування на комп’ютерні надзвичайні події в Україні CERT-UA (далі – СERT-UA) щодо кіберінциденту/кібератаки: 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;
5. визначення потреби в аналітичній підтримці з боку третіх сторін (СERT-UA та інші сили кіберзахисту, правоохоронні органи, експерти).
6. **Етап стримування**, який передбачає попередження подальшої ескалації та зменшення негативного впливу від кіберінциденту/кібератаки шляхом усунення/зменшення можливостей зловмисника, у відмові йому в доступі.

Заходами зі стримування є:

вжиття негайних заходів для припинення будь-якої зловмисної активності, що триває (ізоляція уражених систем та мереж, мережевих сегментів та пристроїв; створення образів пам’яті (дампів оперативної пам’яті), оновлення фільтрів брандмауерів, ведення логів (створення лог-файлів) щодо несанкціонованого доступу; блокування джерел поширення ШПЗ, встановлення правил блокування сервером доменних імен (DNS) відомих доменних імен зловмисника, закриття (блокування) мережевих портів та інтерфейсів);

1. **Етап усунення**, який передбачає відновлення штатного режиму функціонування системи шляхом усунення артефактів кіберінциденту/кібератаки (видалення зловмисного коду, створення повторного образу пам’яті елементів «заражених» систем) і пом’якшення наслідків від кіберзатаки або інших умов, якими скористався зловмисник (зловмисні групи).

Заходами з усунення є:

забезпечення повного технічного усунення загрози та пов’язаної з нею зловмисної активності (перевірка усіх заражених середовищ щодо вразливостей, часткове або повне відновлення обладнання, заміна скомпрометованих артефактів артефактами із систем резервного копіювання та відновлення, зміна усіх паролів у скомпрометованих середовищах).

1. **Етап відновлення**, який спрямований на пом’якшення наслідків від реалізації кіберзагроз та інших умов, якими скористався зловмисник. На цьому етапі основними завданнями є підтвердження того, що усунення наслідків від кіберінцидентів/кібератак було успішним, відбулися перебудова систем/мереж (зміна налаштувань пристроїв системи та/або мережевих пристроїв, їх структури у внутрішньому периметрі системи/мережі), повторне підключення систем/мереж, відтворення або виправлення інформації.
2. **Етап аналізу ефективності заходів реагування на кіберінциденти/кібератаки**, який включає проведення оцінки загальної ефективності реагування та визначення можливостей для вдосконалення заходів реагування або пом’якшення використаних вразливостей.

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

1. впевненість в усуненні та подоланні першопричин кіберінциденту/кібератаки;
2. визначення проблем з програмним та апаратним забезпеченням, які необхідно розв’язати;
3. визначення проблем з організаційною політикою та процедурами, які необхідно розв’язати;
4. визначення потреб у технічній підготовці, підготовці осіб, що забезпечують реагування на кіберінциденти/кібератаки;
5. удосконалення інструментів, необхідних для виконання заходів із захисту, виявлення, аналізу та/або реагування на кіберінциденти/кібератаки;
6. застосування отриманого досвіду для забезпечення готовності в майбутньому.
   1. **Внесення змін до Порядку**

Порядок підлягає перегляду та внесенню змін у разі:

* зміни в підходах, принципах чи завданнях щодо реагування на кіберінциденти/кібератаки з урахуванням виникнення нових типів загроз або ризиків;
* зміни в законодавчих та інших нормативно-правових актах щодо реагування на кіберінциденти/кібератаки.