



РОЗПОРЯДЖЕННЯ
НОВООДЕСЬКОГО МІСЬКОГО ГОЛОВИ

31 березня 2026 року

м. Нова Одеса

№ 58

Про затвердження Плану реагування
на кіберінциденти в апараті виконавчого
комітету Новоодеської міської ради

Керуючись ст. 42 Закону України «Про місцеве самоврядування в Україні», відповідно до 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, Постанови Кабінету Міністрів України від 26.11.2025 № 1533 «Про затвердження Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози», наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03.07.2023 № 570, враховуючи розпорядження Новоодеського міського голови від 24.03.2026 № 50 «Про призначення відповідального за захист інформації та кібербезпеку у виконавчому комітеті Новоодеської міської ради», з метою забезпечення своєчасного та скоординованого реагування на кіберінциденти, кібератаки та кіберзагрози,
ЗОБОВ'ЯЗУЮ:

1. Затвердити План реагування на кіберінциденти в апараті виконавчого комітету Новоодеської міської ради (додається).
2. Відповідальному за захист інформації та кібербезпеку довести План до відома працівників апарату виконавчого комітету та забезпечити його виконання.
3. Контроль за виконанням цього розпорядження покласти на керуючого справами виконавчого комітету міської ради Чубука Г.П.

Міський голова

Олександр ПОЛЯКОВ

ЗАТВЕРДЖЕНО

розпорядження Новоодеського
міського голови
від 31.03.2026р. № 58

ПЛАН

реагування на кіберінциденти в апараті виконавчого комітету Новоодеської міської ради

1. Загальні положення.

1.1. Цей План визначає порядок дій в апараті виконавчого комітету Новоодеської міської ради (далі – апарат виконкому) у разі виявлення кіберінцидентів, кібератак та кіберзагроз в інформаційно-комунікаційних системах.

1.2. План розроблений з урахуванням Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26.11.2025 № 1533, та методичних рекомендацій, затверджених наказом Адміністрації Держспецзв'язку від 03.07.2023 № 570.

1.3. Терміни в цьому Плані вживаються у значеннях, визначених Законом України «Про основні засади забезпечення кібербезпеки України».

1.4. Відповідальний за захист інформації та кібербезпеку в апараті виконавчого комітету Новоодеської міської ради (далі – Відповідальна особа) призначений розпорядженням Новоодеського міського голови від 24.03.2026 № 50 «Про призначення відповідального за захист інформації та кібербезпеку у виконавчому комітеті Новоодеської міської ради».

2. Класифікація подій кібербезпеки.

2.1. Рівень 1 (інформаційний) – подія не становить загрози функціонуванню систем, фіксується для аналізу.

2.2. Рівень 2 (низький) – подія локалізована, вплив на функціонування систем відсутній або незначний.

2.3. Рівень 3 (середній) – подія впливає на роботу окремої інформаційної системи чи сервісу, потребує вжиття заходів реагування.

2.4. Рівень 4 (високий) – подія загрожує безперервності надання послуг структурними підрозділами апарату виконкому або цілісності/конфіденційності інформації з обмеженим доступом.

2.5. Рівень 5 (критичний) – подія загрожує функціонуванню апарату виконкому в цілому або пов'язана з витоком інформації, що може завдати значної шкоди територіальній громаді.

3. Порядок повідомлення про подію.

3.1. Будь-який працівник структурного підрозділу апарату виконкому, який виявив ознаки кіберінциденту, кібератаки чи кіберзагрози, зобов'язаний невідкладно повідомити про це Відповідальну особу.

3.2. Повідомлення здійснюється невідкладно за телефоном +380976505451, а також фіксується у Журналі реєстрації подій інформаційної безпеки (Додаток

2 до Політики інформаційної безпеки апарату виконавчого комітету Новоодеської міської ради).

4. Етапи реагування.

4.1. Підготовка – заходи, що здійснюються на постійній основі: моніторинг систем, підтримання актуальності контактів з CERT-UA/MISP-UA, навчання персоналу.

4.2. Виявлення та аналіз – Відповідальна особа встановлює факт, характер і масштаб події, класифікує її за рівнем згідно з розділом 2 цього Плану.

4.3. Стимування – вжиття заходів для унеможливлення поширення інциденту, зокрема відключення або локалізація ураженої інформаційної системи.

4.4. Усунення наслідків та відновлення – відновлення систем і даних, у тому числі з резервних копій, усунення вразливостей, які спричинили інцидент.

4.5. Аналіз ефективності – оцінка вжитих заходів реагування, підготовка рекомендацій щодо запобігання подібним інцидентам у майбутньому.

5. Повідомлення зовнішніх суб'єктів.

5.1. Про кіберінциденти, кібератаки та кіберзагрози Відповідальна особа інформує команду реагування на комп'ютерні надзвичайні події України (CERT-UA) через платформу обміну інформацією MISP-UA.

5.2. Про кіберінциденти рівня 4-5 Відповідальна особа інформує Національний координаційний центр кібербезпеки (на електронну адресу report@ncscc.gov.ua) та Департамент контррозвідального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України у строки, визначені пунктом 20 Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26.11.2025 № 1533: попереднє повідомлення – протягом 24 годин після виявлення; поточний звіт – протягом 72 годин; остаточний звіт – протягом одного місяця після усунення наслідків інциденту.

6. Перегляд Плану.

6.1 План переглядається не рідше одного разу на рік, а також позапланово – у разі суттєвих змін у законодавстві чи інформаційно-комунікаційних системах апарату виконавчого комітету.

Фахівець сфери захисту інформації

Денис ГРЕБЕНЮК