НОВОКАХОВСЬКА МІСЬКА ВІЙСЬКОВА АДМІНІСТРАЦІЯ
КАХОВСЬКОГО РАЙОНУ ХЕРСОНСЬКОЇ ОБЛАСТІ

РОЗПОРЯДЖЕННЯ
НАЧАЛЬНИКА МІСЬКОЇ ВІЙСЬКОВОЇ АДМІНІСТРАЦІЇ

27.06.2025 **м. Нова Каховка** № 357-од

Про затвердження алгоритму дій працівників центру надання адміністративних послуг виконавчого комітету Новокаховської міської ради у разі виявлення спроби чи факту несанкціонованого доступу до інформаційних систем та витоку персональних даних

З метою своєчасного реагування на кіберінциденти в інформаційних системах центру надання адміністративних послуг, відповідно до Законів України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII, «Про захист персональних даних» від 01.06.2010 № 2297-VI, керуючись Законом України «Про правовий режим воєнного стану», постановою Верховної Ради України від 06 лютого 2023 року № 2898-IX «Про здійснення начальниками військових адміністрацій населених пунктів у Каховському та Херсонському районах Херсонської області повноважень, передбачених частиною другою статті 10 Закону України «Про правовий режим воєнного стану»:

1. Затвердити алгоритм дій працівників центру надання адміністративних послуг виконавчого комітету Новокаховської міської ради у разі виявлення спроби чи факту несанкціонованого доступу до інформаційних систем та витоку персональних даних згідно з додатком.
2. Контроль за виконанням цього розпорядження залишаю за собою.

Начальник міської
військової адміністрації Валерій БРУСЕНСЬКИЙ

Додаток
до розпорядження начальника
міської військової адміністрації
від 27.06.2025 № 357-од

Алгоритм дій
працівників центру надання адміністративних послуг
виконавчого комітету Новокаховської міської ради
у разі виявлення спроби чи факту несанкціонованого доступу до інформаційних систем та витоку персональних даних

1. **Реагування на інцидент**

У разі виявлення спроби несанкціонованого доступу або факту витоку персональних даних, працівник центру надання адміністративних послуг зобов'язаний:

- припинити роботу із відповідною інформаційною системою;
- зафіксувати час, обставини та характер інциденту (знімок екрану, повідомлення системи тощо);
- повідомити керівника центру надання адміністративних послуг та відповідальну особу за забезпечення кіберзахисту комунікаційних і технологічних систем Новокаховської міської військової адміністрації (далі – відповідальна особа);
- утриматись від самостійних спроб виправлення ситуації до прибуття технічного фахівця.

2. **Фіксація та попередній аналіз**

Відповідальна особа:

- здійснює попередню перевірку лог-файлів, прав доступу, дій користувачів;
- кваліфікує рівень інциденту (локальна помилка, спроба вторгнення, витік даних тощо);
- складає акт про інцидент із зазначенням дати, часу, прізвища, ім'я, по батькові учасників, обставин та попередніх висновків.

3. **Інформування відповідних органів**

У разі підтвердження інциденту відповідальною особою:

- надсилається службова записка до Управління інформаційних технологій Херсонської обласної державної адміністрації;
- інформуються органи кібербезпеки — Національний координаційний центр кібербезпеки, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України (за потреби);

- забезпечується збереження доказів (лог-файли, копії листування, скріншоти тощо).

4. **Блокування доступу та локалізація інциденту**

Відповідальною особою:

- тимчасово блокується доступ ураженого облікового запису/системи;
- оновлюються паролі, перевіряються права доступу користувачів;
- відключається певна система до завершення розслідування (за потреби).

5. **Оцінка ризиків і попередження наслідків**

Проводиться аналіз потенційного масштабу витоку:

- які персональні дані могли бути скомпрометовані;
- хто мав/міг мати до них доступ;

У разі необхідності — інформуються власники персональних даних.

6. **Реєстрація інциденту та звітність**

Інформація про інцидент:

- реєструється в журналі обліку інформаційних інцидентів центру надання адміністративних послуг;
- вноситься до звіту, який подається до Управління інформаційних технологій Херсонської обласної державної адміністрації.

7. **Профілактичні заходи**

За результатами інциденту:

- проводиться позачерговий інструктаж серед працівників, що мають доступ до інформаційних систем;
- переглядається політика доступу, оновлюються технічні інструкції;
- ініціюється оновлення програмного забезпечення або аудиту безпеки (за необхідності).