

ЗАТВЕРДЖЕНО  
Розпорядження начальника  
Баштанської районної військової  
адміністрації

03.03.2026 № 21-р

## План реагування на кіберінциденти у Баштанській районній державній (військовій) адміністрації

### I. Негайні дії на місці інциденту

1. Ідентифікація кіберзагрози:
  - а) визначення типу загрози (вірус, спроба несанкціонованого доступу, підозрілий трафік, вразливість в системі тощо);
  - б) скріншот екрану (за можливості), збереження журналів подій, що підтверджують інцидент.
2. Ізоляція ураженого компонента:
  - а) відключення від мережі підозрілого пристрою або сервера для мінімізування поширення загрози;
  - б) блокування доступу до зовнішніх ресурсів, які можуть бути джерелом атаки.
3. Фіксація даних:
  - а) фіксація часу, IP-адреси, портів, шляхів доступу, з якими пов'язана підозра;
  - б) збереження відповідних файлів, журналів та підозрілих даних для подальшого аналізу.

### II. Інформування ключових сторін

1. Сповіднення внутрішньої команди:
  - а) інформування керівництва та спеціалістів кібербезпеки про загрозу;
  - б) забезпечення передачі зібраних доказів та опису інциденту.
2. Інформування CERT-UA за контактами, визначеними у розділі VI цього Плану:
  - а) направлення офіційного повідомлення до CERT-UA за допомогою електронної пошти або через вебсервіс, враховуючи:
    - опис інциденту;
    - характер загрози;
    - файли із зібраними даними (журнали, зразки шкідливого програмного забезпечення тощо).
3. Сповіднення MISP-UA:
  - а) передача технічних даних загрози (IoC — Indicators of Compromise) через платформу MISP-UA з наданням відповідних тегів та пояснень для точної класифікації.

### III. Дії щодо нейтралізації загрози

1. Аналіз загрози:
  - а) самостійний аналіз або з допомогою експертів кібербезпеки, CERT-UA, MISP-UA з використанням спеціалізованих інструментів (Wireshark, Splunk, інші IDS/IPS).
- 2) Знешкодження:
  - а) застосування оновлення безпеки, патчів або видалення шкідливих файлів;
  - б) перевірка резервних копій та відновлення системи з безпечного стану, (за необхідності).

### IV. Запобіжні заходи на майбутнє

1. Оновлення політик безпеки:
  - а) перегляд існуючих правил доступу, моніторинг та обробка інцидентів;
  - б) впровадження багаторівневого захисту.
2. Проведення навчань:
  - а) проведення тренінгів для співробітників з розпізнавання кіберзагроз;
  - б) симулювання кіберінцидентів для покращення реагування.
3. Моніторинг і аудити:
  - а) впровадження регулярного аналізу мережевого трафіку та вразливостей;
  - б) використання SIEM-системи для цілодобового моніторингу.

### V. Документування інциденту

1. Підготовка детального звіту, що включає:
  - опис інциденту та вжитих дій;
  - висновки щодо впливу на систему;
  - рекомендації для запобігання повторним атакам.
2. Доведення звіту до відома керівництва районної державної (військової) адміністрації, Управління Держспецзв'язку у Миколаївській області, Управління Служби безпеки України в Миколаївській області, Управління з питань цифрового розвитку, цифрових трансформацій і цифровізації Миколаївської обласної державної (військової) адміністрації та CERT-UA.
3. Оформлення відповідальним за кіберзахист картки інформування про кіберінцидент/кібератаку, згідно з наказом Адміністрації державної служби спеціального зв'язку та захисту інформації України від 03.07.2023 № 570 відповідно до додатку 6 Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій в кіберпросторі (пункт 6 розділу III).

## VI. Контакти для екстреного реагування

CERT-UA: [cert@cert.gov.ua](mailto:cert@cert.gov.ua), [incidents@cert.gov.ua](mailto:incidents@cert.gov.ua)

Пн - Чт: 8:00 - 17:00, Пт: 8:00 - 15:45:

+38 (044) 281-88-25

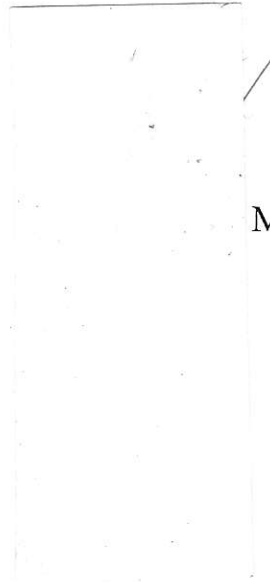
+38 (044) 281-88-05

Вихідні та святкові дні (цілодобово):

+38 (044) 281-88-01

MISP-UA: через кабінет управління або [support@dis.gov.ua](mailto:support@dis.gov.ua)

Начальник відділу цифрового розвитку,  
цифрових трансформацій і цифровізації  
та організації діяльності центрів  
надання адміністративних послуг  
районної військової адміністрації



Михайло ДАНИЛЮК