УЖГОРОДСЬКИЙ МІСЬКИЙ ГОЛОВА

Р О З П О Р Я Д Ж Е Н Н Я

23.07.2025 м. Ужгород № 470

Про внутрішній план реагування
на кібератаки та кіберінциденти

Відповідно до статті 42 Закону України «Про місцеве самоврядування в Україні», законів України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про електронні документи та електронний документообіг», Постанови Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»:

1. Затвердити внутрішній план реагування на кібератаки та кіберінциденти, що додається.
2. Виконавчим органам міської ради неухильно дотримуватись зазначеного плану.
3. Контроль за виконанням розпорядження покласти на заступника міського голови В. Борця.

Міський голова **Богдан АНДРІЇВ**

ЗАТВЕРДЖЕНО
Розпорядження міського голови
23.07.2025 № 470

І. Внутрішній план реагування на кібератаки та кіберінциденти

1. Загальні положення

Цей документ визначає порядок дій та відповідальність структурних підрозділів Ужгородської міської ради (далі — Міська рада) у разі виявлення, фіксації та реагування на кіберінциденти та кібератаки, що можуть загрожувати конфіденційності, цілісності або доступності інформації, ІТ-ресурсів чи комунікаційних мереж.

2. Терміни та визначення

2.1. Кіберінцидент — порушення або потенційне порушення безпеки інформаційної системи.

2.2. Кібератака — навмисні дії, спрямовані на завдання шкоди ІТ-інфраструктурі або викрадення інформації.

2.3. Реагування на інцидент — комплекс заходів з ідентифікації, аналізу, локалізації, усунення та відновлення після інциденту.

3. Цілі плану

- Забезпечення оперативної реакції на кіберінциденти.
- Мінімізація впливу інцидентів на діяльність Міської ради.
- Відновлення нормального функціонування інформаційних систем.
- Виконання вимог чинного законодавства у сфері кібербезпеки.

4. Відповідальні особи

- Урста Микола Валерійович — начальник управління програмного та комп’ютерного забезпечення.
- Ковач Руслан Іванович — начальник відділу інформатизації та технічного захисту інформації (ідентифікація інцидентів, аналіз, взаємодія з держорганами, такими як CERT-UA, СБУ).
- Блискун Михайло Михайлович — системний адміністратор (локалізація та усунення наслідків інциденту).

5. Класифікація кіберінцидентів

- Несанкціонований доступ.

- Вірусні атаки/шкідливе програмне забезпечення.
- DDoS-атаки.
- Витік або компрометація даних.
- Фішинг.

6. Етапи реагування

6.1. Виявлення — фіксація часу, типу та обставин інциденту.
6.2. Ідентифікація — визначення джерела, типу і масштабу інциденту.
6.3. Повідомлення — інформування CERT-UA і керівництва.
6.4. Локалізація — ізоляція уражених систем.
6.5. Усунення — видалення шкідливого ПЗ, оновлення політик безпеки.
6.6. Відновлення — перевірка стабільності, інформування користувачів.
6.7. Аналіз — підготовка звіту, аналіз причин та запобігання повторенню.

7. Запобігання та навчання

7.1. Регулярне оновлення програмного забезпечення.
7.2. Наявність антивірусного захисту.
7.3. Щоквартальні навчання персоналу.
7.4. Щорічне тестування сценаріїв реагування.

8. Взаємодія з національними органами

- Повідомлення CERT-UA або СБУ у разі суттєвих інцидентів.
- Співпраця з національними центрами реагування на інциденти.

9. Документування інцидентів

Ведення Журналу інцидентів працівниками відділу інформатизації та технічного захисту інформації управління програмного та комп'ютерного забезпечення з обов'язковою реєстрацією кожного випадку.

10. Перегляд плану

У разі змін у законодавстві, структурі ІТ-інфраструктури або виявлення нових загроз.

11. Шаблон повідомлення для CERT-UA

Адресат: cert@cert.gov.ua
Тема листа: [ІНЦИДЕНТ] Виявлено кіберінцидент в ІС Ужгородської міської ради.
Зміст повідомлення:
Дата та час виявлення: [дата/час]
Тип інциденту: [наприклад, фішинг/вірус / DDoS]

Стислий опис: [короткий опис ситуації]

Уражені системи: [перелік]

Контактна особа: [ПІБ, посада, телефон, e-mail]

Додатки: [логи, скріншоти, технічні дані (за наявності)]

II. **Порядок дій для працівників при підозрі на кібератаку**

Мета: забезпечити швидку та скоординовану реакцію співробітників при підозрі на кібератаку для мінімізації ризиків.

Алгоритм дій:

1. Негайно припинити дії на пристрої:

- Не закривати підозрілі вікна або повідомлення (за можливості — зробити скріншот);
- Не вводити жодних логінів, паролів або інших даних;
- Не відкривати вкладення або посилання;
- Не перезавантажувати комп'ютер без консультації з ІТ-відділом.

2. Повідомити:

- Керівника свого підрозділу;
- Відповідального ІТ-фахівця: начальника відділу інформатизації та технічного захисту інформації.

3. У повідомленні вказати:

- Дата і час підозрілих дій;
- Суть підозри (приклад: лист, повідомлення, сплеск активності тощо);
- Додати скріншоти, якщо можливо.

4. Від'єднати комп'ютер від мережі:

- Вимкнути Wi-Fi або витягти мережевий кабель;
- Не вимикати пристрій повністю (для збереження цифрових слідів).

5. Дочекатися інструкцій від працівників управління програмного та комп'ютерного забезпечення:

- Не вживати самостійних дій;
- Забезпечити доступ до пристрою для аналізу.

6. Утриматися від розповсюдження інформації:

- Не обговорювати інцидент поза службовим колом;
- Не публікувати інформацію у соціальних мережах або месенджерах.
