# УЖГОРОДСЬКИЙ МІСЬКИЙ ГОЛОВА

# Р О З П О Р Я Д Ж Е Н Н Я

28.08.2025 м. Ужгород № 571

**Про Політику інформаційної безпеки Ужгородської міської ради**

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 Політику інформаційної безпеки Ужгородської міської ради згідно з додатком.
2. Контроль за виконанням розпорядження покласти на заступника міського голови В. Борця

**Міський голова** **Богдан АНДРІЇВ**

ЗАТВЕРДЖЕНО
Розпорядження міського голови
28.08.2025 № 571

# ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УЖГОРОДСЬКОЇ МІСЬКОЇ РАДИ

## 1. Загальні положення

1.1. Політика інформаційної безпеки (далі – Політика) визначає основні принципи, правила та вимоги щодо забезпечення захисту інформації в інформаційних системах та у діяльності Ужгородської міської ради.

1.2. Політика розроблена відповідно до законів України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про електронні довірчі послуги», «Про доступ до публічної інформації» та інших нормативно-правових актів.

1.3. Дія Політики поширюється на всіх працівників ради, посадових осіб, тимчасових працівників, підрядників та осіб, які мають доступ до інформаційних ресурсів.

## 2. Мета Політики

- Забезпечення конфіденційності, цілісності та доступності інформації.
- Захист персональних даних громадян, службової інформації та іншої інформації з обмеженим доступом.
- Запобігання несанкціонованому доступу до інформаційних систем.
- Створення умов для безперервного функціонування інформаційних систем ради.

## 3. Основні принципи інформаційної безпеки

- Законність – дотримання вимог чинного законодавства.
- Пропорційність – застосування заходів безпеки відповідно до рівня ризику.
- Комплексність – поєднання організаційних, технічних та правових заходів.
- Відповідальність – особиста відповідальність кожного працівника за збереження інформації.
- Безперервність – постійний моніторинг та вдосконалення системи безпеки.

## 4. Організація захисту інформації

4.1. Відповідальність за організацію інформаційної безпеки покладається на начальника управління програмного та комп’ютерного забезпечення.

4.2. Кожен структурний підрозділ призначає відповідальну особу за дотримання вимог інформаційної безпеки.

## 5. Класифікація та обробка інформації

5.1. Інформація поділяється на:

- відкриту (публічну);
- службову;
- інформацію з обмеженим доступом (у тому числі персональні дані).

5.2. Доступ до інформації надається виключно в межах службових обов’язків.

5.3. Забороняється передача службової інформації стороннім особам без відповідного дозволу.

## 6. Технічний захист інформації

- Використання антивірусного захисту та систем виявлення вторгнень.
- Регулярне оновлення програмного забезпечення та операційних систем.
- Резервне копіювання критично важливих даних та зберігання їх у захищених місцях.
- Використання засобів криптографічного захисту інформації та електронних довірчих послуг.

## 7. Доступ до інформаційних систем

- Доступ надається лише після авторизації користувача.
- Використання індивідуальних логінів та паролів, регулярна їх зміна.
- Заборона використання сторонніх носіїв інформації без перевірки.
- Ведення журналу реагування на кібератаки та кіберінциденти.

## 8. Реагування на інциденти

- Кожен працівник зобов’язаний негайно повідомляти про інциденти у сфері інформаційної безпеки.
- Відділ інформатизації та технічного захисту інформації управління програмного та комп’ютерного забезпечення здійснює аналіз та фіксацію інциденту, вживає заходів для його усунення.
- У разі витоку або компрометації інформації інформуються керівництво ради та відповідні державні органи.

## 9. Навчання та підвищення обізнаності

- Регулярне проведення тренінгів і інструктажів з питань інформаційної безпеки.
- Ознайомлення нових працівників з Політикою під час прийняття на роботу.

## 10. Контроль і відповідальність

- Контроль за виконанням Політики здійснює заступник міського голови.
- Працівники, які порушили вимоги Політики, несуть відповідальність згідно з законодавством України.

## 11. Прикінцеві положення

11.1. Політика переглядається у випадку змін законодавства.

11.2. Політика набирає чинності з дня її затвердження розпорядженням міського голови.

---