Комунальне ПІДПРИЄМСТВО
«ОБЛАСНИЙ ЦЕНТР ЕКСТРЕНОЇ МЕДИЧНОЇ ДОПОМОГИ ТА МЕДИЦИНИ КАТАСТРОФ»
Рівненської обласної ради
(КП ОЦЕМД та МК РОР)

ІНСТРУКЦІЯ
З ДОТРИМАННЯ ПРАВИЛ КІБЕРГІГІЄНИ
ДЛЯ ПРАЦІВНИКІВ
КОМУНАЛЬНОГО ПІДПРИЄМСТВА « ОБЛАСНИЙ ЦЕНТР ЕКСТРЕНОЇ МЕДИЧНОЇ ДОПОМОГИ ТА МЕДИЦИНИ КАТАСТРОФ» РІВНЕНСЬКОЇ ОБЛАСНОЇ РАДИ

м. Рівне — 2026

ЗАТВЕРДЖУЮ:
В.о. директора комунального підприємства
«Обласний центр екстреної медичної допомоги та медицини катастроф»
Рівненської обласної ради

_____Олег ГИКАВЧУК

19 лютого 2026 року

ІНСТРУКЦІЯ З ДОТРИМАННЯ ПРАВИЛ КІБЕРГІГІЄНИ ДЛЯ ПРАЦІВНИКІВ КОМУНАЛЬНОГО ПІДПРИЄМСТВА « ОБЛАСНИЙ ЦЕНТР ЕКСТРЕНОЇ МЕДИЧНОЇ ДОПОМОГИ ТА МЕДИЦИНИ КАТАСТРОФ» РІВНЕНСЬКОЇ ОБЛАСНОЇ РАДИ

1. Загальні положення

1. Інструкція розроблена відповідно до постанови Кабінету Міністрів України № 1281 від 08.10.2025 «Про затвердження Порядку проведення інструктажів та систематичних тренінгів щодо кібергігієни» та наказу Адміністрації служби спеціального зв'язку та захисту інформації від 21.10.2025 № 661 «Про затвердження Методичних рекомендацій щодо проведення інструктажів і тренінгів щодо кібергігієни на період призначення на посади державних службовців, працівників органів державної влади та інших державних органів, військовослужбовців, керівників та працівників державних підприємств, установ та організацій».

2. Метою інструктажу з кібергігієни для працівників КП ОЦЕМД та МК РОР є підвищення рівня їх обізнаності та формування в них практичних навичок безпечного користування засобами інформатизації та Інтернетом для запобігання, своєчасного виявлення та реагування на кіберінциденти, кібератаки, забезпечення захисту персональних даних, а також дотримання вимог законодавства у сфері кібербезпеки та відповідних стандартів, політик безпеки та особливостей у відповідній сфері або галузі.

3. Інструкція є обов'язковою для всіх працівників КП ОЦЕМД та МК РОР.

2. Основні вимоги кібергігієни

1. Паролі та автентифікація:

- використовувати складні паролі (мінімум 12 символів, комбінація літер, цифр, символів);
- не застосовувати однакові паролі для різних систем;
- змінювати паролі не рідше ніж раз на 12 місяців;

- використовувати двофакторну (2FA) або багатофакторну (MFA) автентифікацію скрізь, де це можливо;
- не зберігати паролі у відкритому вигляді на папері чи в незашифрованих текстових файлах на комп’ютері; використовувати для цього менеджери паролів, наприклад KeePass.

2. Електронна пошта:
   - використовувати лише службову електронну пошту;
   - перевіряти адресу відправника та домен;
   - не відкривати вкладення та посилання від невідомих відправників;
   - у разі сумнівів повідомити про це системних адміністраторів.
3. Мобільні пристрої та носії інформації:
   - використовувати PIN-код, пароль або біометрію;
   - встановлювати лише офіційні додатки;
   - заборонено підключати особисті флеш-накопичувачі до службових комп'ютерів;
   - регулярно оновлювати операційну систему мобільного пристрою та додатки.
4. Робочі комп'ютери:
   - заборонено встановлювати стороннє програмне забезпечення без погодження з ІТ-відділом;
   - оновлюйте операційну систему, антивірус та інше прикладне ПЗ;
   - не вимикайте оновлення без дозволу системного адміністратора;
   - підключати переносні носії інформації лише при активному і оновленому антивірусі;
   - передавайте конфіденційні дані лише через корпоративні канали: корпоративна електронна пошта з шифруванням, службові захищені месенджери, захищені файлообмінні сервіси, зашифровані USB-накопичувачі. Пароль до захищених даних передавайте іншим захищеним каналом (наприклад, телефоном);
   - завжди переконуйтеся, що одержувач має право доступу до цієї інформації. У разі сумнівів, уточніть по іншому каналу.

3. Соціальна інженерія

1. Працівники повинні знати основні методи атак: фішинг (підроблені електронні листи або сайти за посиланнями), вішинг (телефонне шахрайство з метою отримати конфіденційні дані), смішинг (різновид фішингу через SMS), імітація колеги (видавання себе за співробітника чи керівника, щоб отримати документи, паролі або іншу службову інформацію).

2. Заборонено передавати паролі чи службову інформацію особистою електронною поштою, месенджери хмарні сховища тощо.

3. Працівники повинні перевіряти особу співрозмовника через офіційні канали.

4. У разі підозрі на атаку працівник зобов'язаний негайно повідомити керівника та відповідального за кібербезпеку.

4. Реагування на кіберінциденти

1. Ознаки кіберінциденту;

- підозріла активність на комп’ютері:
  - різке уповільнення без видимих причин;
  - самовільне відкриття або закриття програм;
  - зміна налаштувань без відома користувача;
  - незвичні повідомлення та сповіщення;
  - вікна з вимогою ввести пароль або дані картки;
  - повідомлення про «блокування системи» чи «потрібне оновлення», які виглядають незвично для даної операційної системи;
  - попередження антивірусу про виявлені загрози;
  - проблеми з доступом до даних;
  - втрата доступу до файлів або їх раптове шифрування;
  - поява невідомих файлів чи програм;
  - зникнення або пошкодження документів;
- аномалії в електронній пошті та месенджерах:
  - листи, які ви не надсилали, але вони з’являються у «Відправлених»;
  - масові розсилки від вашого акаунта без вашої участі;
  - підозрілі вкладення чи посилання від колег;
- ознаки несанкціонованого доступу:
  - вхід у систему з пристрою, який ви не використовували;
  - зміна паролів або налаштувань без вашої участі;
  - незвично високий трафік у мережі;
  - підключення невідомих пристроїв до корпоративної Wi-Fi;
  - часті розриви з’єднання або нестабільна робота VPN.

2. Алгоритм дій при кіберінциденті:

- зафіксувати ознаки кіберінциденту;
- повідомити ІТ-відділ, особу відповідальну за кібербезпеку;
- не використовувати заражений пристрій до отримання інструкцій.

5. Організація інструктажів та тренінгів

Проведення інструктажів та тренінгів щодо кібергігієни для працівників КП ОЦЕМД та МК РОР проводиться з такою періодичністю:

- після призначення їх на посади — протягом одного календарного місяця після дати призначення на посаду або набуття повноважень;

- не рідше одного разу на рік протягом всього строку перебування на посадах;
- після настання значного кіберінциденту, кібератаки — протягом одного календарного місяця;
- за потреби згідно з результатом аналізу ризиків.

6. Відповідальність

Працівники несуть персональну відповідальність за дотримання вимог кібергігієни.

7. Додаткові освітні матеріали з кібергігієни

Для самостійного вивчення основ кібергігієни доступні навчальні матеріали за наступним посиланням: https://rocemd.org.ua/kiberhihiyena/.

Розробив:
Відповідальний за кібербезпеку Іван ОНИЩУК