ХОРОЛЬСЬКА МІСЬКА РАДА
ЛУБЕНСЬКОГО РАЙОНУ ПОЛТАВСЬКОЇ ОБЛАСТІ

РОЗПОРЯДЖЕННЯ

12 лютого 2026 року м. Хорол №40-р

Про заходи щодо забезпечення
інформаційної та кібербезпеки

З метою забезпечення захисту інформаційних ресурсів, персональних даних, стабільної роботи інформаційно-комунікаційних систем, а також з урахуванням дії правового режиму воєнного стану в Україні, відповідно до статті 5 Закону України «Про основні засади забезпечення кібербезпеки України», керуючись статтею 42 Закону України «Про місцеве самоврядування в Україні»,

1. Затвердити Пам'ятку з інформаційної та кібербезпеки (далі – Пам'ятка) для усіх працівників Хорольської міської ради (додаток 1).

2. Усім працівникам неухильно дотримуватися вимог інформаційної та кібербезпеки зазначених у Пам'ятці.

3. Відповідальній особі, яка виконує функції та завдання керівника з кіберзахисту у Хорольській міській раді (Тягній Ю.І.) організувати ознайомлення працівників з Пам'яткою під підпис.

4. Контроль за виконанням розпорядження покласти на заступника міського голови з питань діяльності виконавчих органів Місніченка В.О.

В. п. міського голови Юлія БОЙКО

Додаток 1
до розпорядження міського голови
від 12.02.2026 №40-р

ПАМ'ЯТКА
з інформаційної та кібербезпеки

Ця пам'ятка обов'язкова для виконання всіма працівниками Хорольської міської ради з метою захисту службової інформації, персональних даних та інформаційних систем.

1. Робота з паролями.

1.1. Використовуйте складні унікальні паролі, зокрема такі що: містять не менше 8 символів, містять щонайменше одну літеру та один спецсимвол ("_" або "- " або "!" тощо), не містять персоніфікованої інформації (дати народження, номерів телефонів, номерів та серій документів, автотранспорту, банківської картки, адреси реєстрації тощо).

1.2. Заборонено використовувати один пароль для кількох сервісів чи аккаунтів.

1.3. Не передавайте паролі колегам, керівництву чи стороннім особам.

1.4. Не зберігайте паролі на папері, у файлах Word/Excel або в браузері без захисту.

1.5. За можливості використовуйте двофакторну автентифікацію (2FA).

2. Робота з електронною поштою.

2.1. Не відкривайте листи від невідомих або підозрілих відправників, наприклад santorin@abrgv.com тощо. Не відкривайте листи в яких у темі присутні фрази типу "Ви виграли 500 тисяч…", "Відкрийте, та отримайте свій приз…" тощо.

2.2. Перевіряйте адресу відправника перед відкриттям посилань.

2.3. Не переходьте за посиланнями та не відкривайте вкладення, якщо маєте сумніви.

2.4. Якщо в листі присутні вкладені файли з потенційно небезпечним розширенням (послідовність символів, що додаються до назви файлу і призначені для ідентифікації типу (формату) файлу), наприклад "Додаток 2.exe" або "Протокол 245 від 25 числа.bat" тощо НЕ відкривайте їх. Особливо небезпечні файли з розширеннями: .exe, .bin, .ini, .bat, .dll, .sys, .js, .vbs, .zip, .rar.

2.5. Ніколи не вводьте логіни та паролі за посиланнями з електронних листів у безпеці, яких ви не впевнені.

2.6. Повідомляйте відповідальну особу або IT-фахівця про підозрілі листи.

3. Захист комп'ютера та ноутбука.

3.1. Встановіть пароль на вхід та не залишайте робочий комп'ютер без блокування (Win+L).

3.2. Не встановлюйте програми без погодження з відповідальною особою.

3.3. Заборонено використовувати робочі комп'ютери для особистих потреб (ігри, сторонні програми).

3.4. Антивірус має бути увімкнений та оновлений.

4. Використання USB-флешок та зовнішніх носіїв.

4.1. Заборонено використовувати невідомі або особисті флешки.

4.2. Усі зовнішні носії повинні перевірятися антивірусом.

4.3. Не підключайте до комп'ютера флешки, знайдені у громадських місцях.

5. Робота з документами та даними.

5.1. Службова інформація та персональні дані не повинні передаватися через месенджери без дозволу.

5.2. Не надсилайте службові документи на особисту пошту.

5.3. Документи з конфіденційною інформацією зберігайте у не доступному для сторонніх осіб місцях (сейфах, захищених папках).

5.4. Не залишайте документи та носії без нагляду.

5.5. Не обговорюйте службову інформацію у відкритих чатах чи соціальних мережах.

5.6. Регулярно проводьте резервне копіювання важливих службових даних (backup).

5.7. Повідомляйте керівництво про втрату або крадіжку документів, даних або пристроїв.

6. Інтернет та мережа.

6.1. Використовуйте лише службові мережі.

6.2. Заборонено підключатися до відкритих публічних мереж для службової роботи.

6.3. Не відвідуйте підозрілі сайти та ресурси розважального характеру на робочому ПК.

6.4. Звертайте особливу увагу на назву Інтернет-ресурсу, що запитує автентифікаційні дані, перш ніж натиснути на посилання: зловмисники можуть замаскувати назву, щоб воно виглядало знайомим (замаскована назва: facelook.com, правильна назва: facebook.com; замаскована назва:gooogle.com, правильна назва: google.com тощо) . В іншому разі є велика ймовірність перейти на фішингову сторінку, ззовні ідентичну справжній, та самостійно «віддати» власні автентифікаційні дані. Шкідливі URL-адреси можуть бути закодовані у вигляді QR-кодів та/або роздруковані на папері, у тому числі у формі скорочених URL, згенерованих спеціальними сервісами, такими як tinyurl.com, bit.ly, ow.ly тощо. Не вводьте ці посилання до браузера та не скануйте QR-коди вашим смартфоном якщо ви не впевнені у їх вмісті та походженні.

6.5. Будьте обережні щодо випливаючих вікон та повідомлень у вашому браузері, програмах, операційній системі та мобільному пристрої. Завжди читайте вміст цих вікон та не "схвалюйте" і не "приймайте" нічого необдумано.

6.5. Використовуйте лише офіційні сайти та сервіси.

7. Соціальна інженерія та шахрайство.

7.1. Будьте уважні до дзвінків «від банку», «СБУ», «керівництва» з вимогою термінових дій; прохань повідомити пароль, код або встановити програму; повідомлень про «термінову перевірку» або «інцидент безпеки». Пам'ятайте: жоден ІТ-спеціаліст не має права запитувати ваші паролі.

8. Дії у разі підозри на кіберінцидент.

Негайно:

1. Припиніть роботу з комп'ютером.
2. Від'єднайте його від мережі (інтернету).
3. Повідомте керівництво або відповідальну особу з кібербезпеки.
4. Не намагайтеся самостійно усунути проблему.

9. Відповідальність.

9.1. Порушення правил інформаційної та кібербезпеки може призвести до:

- витоку персональних даних;
- зупинки роботи ради;
- дисциплінарної та юридичної відповідальності.

10. Робота з інформацією та ІТ-системами під час воєнного стану

У період дії воєнного стану працівники зобов'язані дотримуватися посилених вимог інформаційної та кібербезпеки:

10.1. Заборонено розголошувати в будь-якій формі (усно, письмово, у соцмережах, месенджерах) інформацію про:

переміщення, розташування, наслідки обстрілів об'єктів критичної інфраструктури;

роботу органів влади, резервних об'єктів, систем зв'язку та електропостачання;

персональні дані військовослужбовців, працівників критичної інфраструктури та ВПО.

10.2. Заборонено фотографувати або публікувати зображення службових документів, екранів комп'ютерів, робочих місць.

10.3. Усі підозрілі інциденти (фішинг, спроби зламу, дивна робота ПК) негайно повідомляються відповідальній особі.

Керуючий справами
(секретар) виконавчого комітету Галина КОЗЛОВА