Інструктаж з кібергігієни

(оновлено згідно з вимогами Управління СБУ від 27.01.2026 лист №57/22/593)

Цей інструктаж розроблено відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» та з урахуванням вимог Управління СБУ в Житомирській області від 27.01.2026 р. лист №57/22/593.

1. Робота з електронною поштою та фішингом

- **Критична заборона:** Не відкривайте вкладення до електронної пошти від невідомих осіб, особливо з розширеннями **.lzh, .scr, .tar, .js, .exe**.
- **Верифікація:** Навіть якщо вкладення має «безпечне» розширення (.docx, .pdf), перевірте через VirusTotal або в телефонному режимі, чи дійсно відправник надсилав вам цей файл.
- **Фішинг:** Не переходьте за невідомими посиланнями та не заповнюйте дані «логінів» та «паролів» на зовнішніх ресурсах, що надійшли поштою.
- **Службова пошта:** Заборонено використання сторонніх (особистих) поштових сервісів для виконання службових обов'язків.

2. Програмне забезпечення та безпека ПЕОМ

- **Сувора заборона WinRar:** Використання програмного забезпечення **«WinRar» заборонено** у зв’язку з використанням спецслужбами рф вразливості **CVE-2025-8088** для виконання шкідливого коду.
- **Інсталяція ПЗ:** Заборонено самостійно встановлювати будь-яке стороннє ПЗ, не пов’язане з роботою.
- **Права доступу:** Користувачам заборонено працювати під правами адміністратора або змінювати налаштування безпеки ПЕОМ.
- **Цільове використання:** ПЕОМ використовується виключно для цілей, пов'язаних із виконанням службових обов'язків.

3. Технічні правила та паролі

- **Оновлення:** Використовуйте лише ліцензійне ПЗ та антивіруси, систематично оновлюйте їх бази.
- **Паролі:** Використовуйте стійкі паролі (8+ символів: літери, цифри, спецсимволи). Не зберігайте їх на робочому столі.
- **Змінні носії:** Не підключайте невідомі флешки/диски. Відключайте автоматичний запуск носіїв (autorun).
- **Резервне копіювання:** Регулярно створюйте копії важливих даних на зовнішніх носіях.

4. Юридична відповідальність

Нехтування правилами захисту інформації може призвести до:

- **Адміністративної відповідальності:** за ст. 188-39 (порушення захисту персональних даних) та ст. 212-6 КУпАП.
- **Кримінальної відповідальності:** за ст. 361 (втручання в роботу систем), ст. 362 (несанкціоновані дії з інформацією) та ст. 363 КК України.

5. Порядок інформування про інциденти

У разі виявлення підозрілої активності (незвичайна робота ПК, підозрілі листи) **НЕГАЙНО** повідомте:

1. **Відділ цифровізації ради:** 068-679-36-83 або digitalchernyahiv@gmail.com.
2. **Управління СБУ в Житомирській обл.:** Володимир МОЛОДЕЦЬКИЙ, тел. **+380674110234**.

3. **Управління Держспецзв'язку в Житомирській обл.:** Ростислав ТЕТЕРЯ, тел. 093-115-82-83, email: cyber_zt@cip.gov.ua.

1. Використовуйте ліцензійні/легалізовані операційні системи, інші програмні продукти, своєчасно й систематично їх **оновлюйте.**
2. Користуйтеся **антивірусним** програмним забезпеченням з технологією евристичного аналізу.
3. Використовуйте програмний **міжмережевий екран** (брандмауер) та штатні засоби захисту від шкідливого програмного забезпечення.
4. Здійснюйте регулярне **резервне копіювання** даних, зберігайте резервні копії на зовнішніх носіях інформації (SSD, HDD тощо) та налаштуйте функцію «відновлення системи».
5. Не підключайте флешки та зовнішні диски, не вставляйте CD та DVD тощо у ваш комп'ютер, якщо ви не довіряєте повністю їх джерелу. Існують техніки зламування комп'ютера ще до того, як ви відкриєте файл на флешці і задовго до того, як ваш антивірус його просканує. Якщо ви знайшли пристрій всередині офісу або на вулиці, чи отримали його поштою або з доставкою, чи незнайомець дав вам його з проханням роздрукувати документ, або просто відкрити та перевірити його вміст – є велика ймовірність, що пристрій є небезпечним.
6. Довіряйте лише власним пристроям та будьте обережні з пристроями, які отримуєте від інших людей по роботі або в інших цілях.
7. При підключенні пристроїв забезпечте їх автоматичну перевірку на наявність шкідливого програмного забезпечення.
8. Відключайте автоматичний запуск змінних носіїв інформації (захист від autorun.inf).
9. Не зберігайте автентифікаційні дані в легкодоступних місцях(наприклад, на робочому столі).Використовуйте для зберігання паролів спеціальні програмні засоби (наприклад, KeePass). Використовуйте **стійкі паролі**, зокрема такі що:

- містять не менше 8 символів;
- містять літери, цифри та спеціальні символи;
- не містять персоніфікованої інформації (дати народження, номерів телефонів, номерів та серій документів, автотранспорту, банківської картки, адреси реєстрації тощо);
- не використовуються в будь-яких інших аккаунтах.

10. Уникайте використання Інтернет-банкінгу, електронних платіжних систем, введення автентифікаційних даних під час доступу до Інтернету через загальнодоступні (незахищені) безпроводові мережі (в кафе, барах, аеропортах та інших публічних місцях).
11. Будьте особливо обережними з відкриттям вкладень до електронної пошти від невідомих осіб. Сьогодні **найактуальнішим** засобом розсилання шкідливого програмного забезпечення є **електронна пошта**. Під час роботи з поштою потрібно перевіряти розширення вкладених файлів та не

відкривати файли навіть з безпечними розширеннями. Не переходьте за невідомими посиланнями та не завантажуйте файли, що мають **потенційно небезпечне розширення** (наприклад: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js тощо) **та навіть безпечне** (наприклад: .docx, .zip, .pdf), адже можуть використовуватися вразливості, макроси та інші небезпеки. Звертайте увагу на ім'я електронної пошти: навіть якщо воно здається легітимним, усе одно потрібно перевірити (у телефонному режимі або в будь-який інший спосіб), чи дійсно ця особа відправляла вам повідомлення з вкладенням.

12. Іноді, особливо під тиском часу, буває важко відрізнити шкідливі файли від легітимних. Користуйтеся сервісом VirusTotal для перевірки підозрілих файлів шляхом їх одночасного сканування більш ніж 50 антивірусами. Це набагато ефективніше, ніж сканування файлів антивірусом в автономному режимі, але враховуйте той факт, що завантажуючи файли на VirusTotal, ви надаєте доступ до нього третій стороні. Звертаємо вашу увагу на те, що, навіть якщо перевірка на VirusTotal не дала результату, це не виключає того, що файл може бути шкідливим.
13. Під час користування Інтернет-ресурсами (Інтернет-банкінгом, соціальними мережами, системами обміну повідомленнями, новинами,онлайн-іграми) не відкривайте підозрілі посилання (URL), особливо ті, що вказують на веб-сайти, які ви зазвичай не відвідуєте.
14. Будьте уважним до проявів Інтернет-шахрайства. Найпоширенішим засобом уведення в оману в мережі Інтернет є **фішинг.** Особливу увагу варто звертати на **доменне ім'я** Інтернет-ресурсу, що запитує автентифікаційні дані, перш ніж натиснути на посилання: зловмисники можуть замаскувати доменне ім'я, щоб воно виглядало знайомим (**facelook.com, goooogle.com** тощо) . В іншому разі є велика ймовірність перейти на фішингову сторінку, **ззовні ідентичну справжній**, та самостійно «віддати» власні автентифікаційні дані.
15. У разі необхідності введення автентифікаційних даних упевніться в тому, що використовується захищене з'єднання HTTPS, перевіряйте SSL-сертифікат веб-сайту, щоб переконатися, що він не клонований або не підроблений.
16. 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 на кшталт **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.
17. 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** похапцем.
18. Під час використання віддаленного доступу необхідно обмежити доступ за допомогою "білого списку" (IP whitelisting) .
19. Установіть обмеження кількості введення помилкових логінів/паролей. Регулярно переглядайте журнали логування, планувальник завдань та автозавантаження на предмет несанкціонованих дій.
20. Слідкуйте за новинами про нові кіберзагрози та швидко реагуйте на нові виклики.