Додаток
до рішення виконавчого комітету

ЗАТВЕРДЖЕНО
Рішення виконавчого комітету
селищної ради
_____ 2026 року
№_____

ІНСТРУКЦІЯ
з дотримання правил кібербезпеки та цифрової гігієни для працівників селищної ради та її виконавчих органів Теофіпольської селищної ради Хмельницького району Хмельницької області

Інструкція з кібербезпеки та цифрової гігієни для працівників селищної ради та її виконавчих органів Теофіпольської селищної ради Хмельницького району Хмельницької області (далі - Інструкція), розроблена відповідно до Закону України від 05 жовтня 2017 року №2163-VIII «Про основні засади забезпечення кібербезпеки України» (із змінами та доповненнями), а також постанов Кабінету Міністрів України від 08 жовтня 2025 року №1281 «Про затвердження Порядку проведення інструктажів та систематичних тренінгів щодо кібергігієни» та від 29 березня 2006 року №373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем».

1. Терміни та скорочення

ІКС - інформаційно-комунікаційна система.

КСЗІ - комплексна система захисту інформації (за наявності/впровадженні).

КЕП - кваліфікований електронний підпис.

ПК - персональний комп'ютер.

Токен - захищений носій особистих ключів (засіб КЕП/печатки), призначений для зберігання особистого ключа та захисту даних.

URL - адреса ресурсу в Інтернеті.

Кіберінцидент - подія, що може свідчити про порушення кібербезпеки.

Кібератака - умисний вплив на ІКС з метою порушення конфіденційності/цілісності/доступності.

2. Загальні положення

2.1. Інструкція визначає мінімальні обов’язкові вимоги кібергігієни та безпечної роботи для всіх працівників селищної ради та її виконавчих органів (далі - Користувачі) Теофіпольської селищної ради Хмельницького району Хмельницької області (далі - Рада).

2.2. Інструкція застосовується до всіх випадків використання:

стаціонарних ПК/ноутбуків/планшетів та інших пристроїв, що належать Раді або підключені до її ресурсів;

робочої електронної пошти;

мережевих ресурсів, файлових сховищ, баз даних, інформаційних систем;

мережі Інтернет у службових цілях;

засобів КЕП/електронної печатки.

2.3. Мета Інструкції - запобігання:

витоку/втраті персональних даних та службової інформації;

несанкціонованому доступу до ІКС;

шкідливому програмному впливу (віруси, трояни, шифрувальники тощо);

порушенню організаційних та технічних заходів захисту інформації.

3. Уповноважена особа з питань кібербезпеки:

3.1. Уповноважена особа з питань кібербезпеки організовує інформування користувачів про порядок повідомлення щодо кіберінцидентів та приймає первинні повідомлення.

3.2. Користувач зобов'язаний негайно повідомляти про ознаки кіберінциденту уповноважену особу з питань кібербезпеки. Якщо уповноважена особа тимчасово недоступна - повідомляється безпосередній керівник.

4. Облікові записи, автентифікація та паролі

4.1. Користувач зобов'язаний:

працювати лише під власним робочим обліковим записом (Windows/пошта/сервіси);

не передавати логіни/паролі/коди підтвердження іншим особам;

використовувати багатофакторну автентифікацію (MFA) там, де вона впроваджена/доступна;

негайно повідомити Відповідальну особу у разі підозри компрометації облікового запису.

5. Безпечна робота з робочим місцем і пристроями

5.1. Користувач зобов'язаний:

блокувати екран при відході від робочого місця (Win + L);

виконувати перезавантаження та встановлення оновлень, коли цього вимагає система/адміністратор;

дотримуватися принципу «чистого столу»: не залишати документи/носії/токени без нагляду.

5.2. Забороняється:

самостійно встановлювати/видаляти програмне забезпечення або змінювати системні налаштування без дозволу;

вимикати/змінювати налаштування антивірусного захисту, брандмауера, засобів контролю доступу;

використовувати неліцензійне програмне забезпечення, невідомі розширення браузера.

6. КЕП, токени та криптографічні засоби

6.1. Користувач зобов’язаний:

використовувати виключно особистий КЕП і особистий токен (за наявності);

забезпечити нерозголошення пароля до токена;

від’єднувати токен після підпису/автентифікації та зберігати його у безпечному місці.

6.2. У разі втрати/пошкодження/підозри компрометації токена або КЕП Користувач негайно повідомляє безпосереднього керівника та уповноважену особу.

6.3. Забороняється:

передавати токен/КЕП/ключі/паролі третім особам;

копіювати особисті ключі на інші носії або зберігати їх у хмарі/пошті/месенджерах.

7. Робота з електронною поштою та фішинг

7.1. Робоча електронна пошта використовується у службових цілях.

7.2. Забороняється:

використовувати службову електронну пошту для реєстрації на сторонніх сервісах, соцмережах, розсилках (без службової необхідності);

відкривати листи/вкладення/посилання з підозрілих адрес або з нетиповими/помилковими доменами;

відкривати вкладення з потенційно небезпечними типами файлів, зокрема: **.exe, .bat, .cmd, .js, .vbs, .scr, .ps1, .dll**, а також архіви **.zip/.rar/.7z** з невідомого джерела.

7.3. Якщо лист викликає підозру:

не відкривати вкладення та не переходити за посиланнями;

за можливості зафіксувати тему/адресу відправника (скриншот);

негайно повідомити Відповідальну особу.

7.4. Додатково допускається перевірка файлів/посилань у VirusTotal як допоміжний захід. Позитивний результат перевірки не гарантує повну безпечність.

8. Інтернет-ресурси, посилання, QR-коди

8.1. Під час роботи в Інтернеті Користувач зобов’язаний:

перевіряти URL перед введенням облікових даних;

бути обережним із повідомленнями «терміново підтвердити», «оновіть пароль», «отримайте приз» тощо;

уважно читати системні/браузерні попередження.

8.2. Забороняється:

переходити за підозрілими посиланнями, у т.ч. скороченими URL (bit.ly, tinyurl тощо) невідомого походження;

сканувати QR-коди невідомого походження для авторизації/входу/платежів;

вводити службові паролі на сторонніх ресурсах.

9. Зовнішні носії, обмін файлами та хмарні сервіси

9.1. Забороняється:

підключати до службового ПК особисті флеш-накопичувачі/диски/телефони для копіювання даних без дозволу;

копіювати службову інформацію на зовнішні носії «для зручності»;

використовувати особисті хмарні сервіси/месенджери/особисту пошту для передачі службових файлів або персональних даних.

9.2. Обмін файлами здійснюється через дозволені Радою канали та сервіси.

10. Персональні дані та службова інформація

10.1. Обробка персональних даних здійснюється лише за наявності законних підстав та у межах службових повноважень.

10.2. Перед відправкою/передачею документів Користувач зобов’язаний:

перевірити адресата (ів) і вкладення;

забезпечити мінімізацію даних (не передавати зайве);

за потреби погодити спосіб передачі з відповідальною особою з питань інформаційної безпеки та кіберзахисту.

10.3. Забороняється:

передавати персональні дані через незахищені або несанкціоновані канали;

публікувати/поширювати службову інформацію поза визначеними процедурами.

11. Реагування на кіберінциденти

11.1. Ознаки кіберінциденту (не вичерпно):

попередження антивіруса/системи;

самовільний запуск програм, підозрілі вікна;

неможливість відкрити файли, зміна їх розширень, повідомлення про «викуп»;

випадкове відкриття підозрілого вкладення/посилання;

ідозріла активність у пошті/облікових записах.

11.2. Дії Користувача при підозрі на кіберінцидент:

11.2.1. Припинити роботу з підозрілим листом/сайтом/файлом.

11.2.2. Заблокувати екран (Win+L) або за вказівкою Відповідальної особи з питань інформаційної безпеки та кіберзахисту від’єднати ПК від мережі.

11.2.3. Вилучити токен (якщо підключений).

11.2.4. Негайно повідомити Відповідальну особу.

11.2.5. Не виконувати самостійних «ремонтних» дій без вказівки Відповідальної особи (не перевстановлювати ОС, не видаляти файли «наосліп»).

12. Відповідальність

12.1. За порушення, що призвели до витоку конфіденційної інформації, її знищення або порушення вимог цієї Інструкції, працівники апарату селищної ради та її виконавчих органів несуть відповідальність згідно з чинним законодавством України.

13. Прикінцеві положення

13.1. Інструкція та шаблон повідомлення (додаток 1 до Інструкції) про кіберінцидент доводиться до відома працівників під підпис.

13.2. Інструктажі та систематичні тренінги щодо кібергігієни проводяться та фіксуються уповноваженою особою з питань кібербезпеки, зокрема:

після призначення/набуття повноважень - протягом одного календарного місяця;

не рідше одного разу на рік протягом усього строку перебування на посаді/строку повноважень;

після значного кіберінциденту/кібератаки - протягом одного календарного місяця;

за потреби - за результатами аналізу ризиків.

13.3. Контроль за проведенням інструктажів/тренінгів та зберіганням підтвердних матеріалів (журнали/списки/протоколи/сертифікати тощо) здійснюються уповноваженою особою з питань кібербезпеки.

Додаток 1
до Інструкції

Шаблон повідомлення про кіберінцидент (для Користувача)

1. Дата/час події: _____
2. Виконавчий орган/підрозділ: _____
3. ПІБ Користувача, посада: _____
4. Контактний телефон: _____
5. Опис події (що саме сталося): _____
6. Джерело (лист/сайт/файл/USB/інше): _____
7. Адреса сайту/тема листа/ім'я файлу (за наявності): _____
8. Які дії вже виконано (Win+L, від'єднання мережі тощо): _____
9. Чи був підключений токен з КЕП (так/ні): _____
10. Скриншоти/файли (за можливості): _____

Важливо: не намагайтесь самостійно налагоджувати систему (не перевстановлюйте операційну систему, не видаляйте файли навмання) - це може ускладнити реагування.