ЗАТВЕРДЖЕНО
Розпорядження начальника
Щастинської міської військової
адміністрації Щастинського
району Луганської області
01 січня 2026 р. № 01/01

ІНСТРУКЦІЯ
з кібергігієни для працівників Щастинської міської військової адміністрації Щастинського району Луганської області

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 Державної 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 Щастинської міської військової адміністрації 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 Щастинської міської військової адміністрації, незалежно від їх посади та стажу роботи.

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 6 місяців;
- обов'язково застосовувати багатофакторну автентифікацію.

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 особу, відповідальну за кібербезпеку.

3. Мобільні пристрої та носії інформації:

- використовувати PIN-код, пароль або біометрію;
- встановлювати лише офіційні додатки;
- регулярно оновлювати операційну систему мобільного пристрою та додатки.

4. Робочі комп'ютери:
- заборонено встановлювати стороннє програмне забезпечення без погодження з особою, відповідальною за кібербезпеку;
- підключати з'ємні носії інформації лише після перевірки їх за допомогою антивірусного програмного забезпечення;
- заборонено передавати службову інформацію через особисті месенджери.

3. Соціальна інженерія

1. Працівники повинні знати основні методи атак: фішинг (підроблені електронні листи або сайти з посиланнями), вішинг (телефонне шахрайство з метою отримання конфіденційних даних), смішинг (різновид фішингу через SMS-повідомлення), імітація колеги (видавання себе за співробітника чи керівника, щоб отримати документи, паролі або іншу службову інформацію).
2. Заборонено передавати паролі чи службову інформацію телефоном, електронною поштою або через месенджери. Працівники повинні перевіряти особу співрозмовника через офіційні канали.
3. У разі підозри 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 роботи системи 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 «потрібно оновлення», які виглядають неофіційно;
- попередження антивірусу про виявлення 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;
- підключення невідомих пристроїв до корпоративної Wi-Fi;
- часті розриви з'єднання або нестабільної роботи VPN.

2. Алгоритм дій при кіберінциденті:
- зафіксувати ознаки інциденту;
- повідомити особу, відповідальну за кібербезпеку;

- не використовувати заражений пристрій до отримання інструкцій.

5. Організація інструктажів та тренінгів

Ознайомлення працівників з цією Інструкцією здійснюється під підпис у Листі ознайомлення, що додається до Інструкції та є її невід'ємною частиною.

Проведення інструктажів та тренінгів щодо кібергігієни для працівників Щастинської міської військової адміністрації здійснюється 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 посаді;
- 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.

Т.в.о. начальника
військової адміністрації **Вікторія ГАРУСТ**