СТАРОБІЛЬСЬКА МІСЬКА ВІЙСЬКОВА АДМІНІСТРАЦІЯ
СТАРОБІЛЬСЬКОГО РАЙОНУ ЛУГАНСЬКОЇ ОБЛАСТІ

РОЗПОРЯДЖЕННЯ
начальника військової адміністрації

12 червня 2026 року м. Львів № 65

Про затвердження Інструкції щодо забезпечення інформаційної безпеки та кіберзахисту працівниками Старобільської міської військової адміністрації та структурних підрозділів Старобільської міської ради Луганської області під час виконання службових обов'язків

Відповідно до законів України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про правовий режим воєнного стану», керуючись Указом Президента України від 23.09.2022 № 665/2022 «Про утворення військових адміністрацій населених пунктів у Луганській області», постановою Верховної Ради України від 03.11.2022 № 2705-IX «Про здійснення начальниками військових адміністрацій населених пунктів у Сватівському, Старобільському, Щастинському районах Луганської області повноважень, передбачених частиною другою статті 10 Закону України "Про правовий режим воєнного стану", постановою Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» це попередня редакція, поточна «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем» (із змінами), враховуючи рекомендації Державної служби спеціального зв'язку та захисту інформації України щодо забезпечення кібербезпеки в умовах воєнного стану, з метою забезпечення належного рівня інформаційної безпеки, захисту службової інформації, інформаційних ресурсів та інформаційно-комунікаційних систем, недопущення витоку інформації, несанкціонованого доступу до інформаційних ресурсів, кіберінцидентів та кібератак,

зобов'язую:

1. Затвердити Інструкцію щодо забезпечення інформаційної безпеки та кіберзахисту працівниками Старобільської міської військової адміністрації та структурних підрозділів Старобільської міської ради Луганської області (далі – Інструкція, працівники) під час здійснення службових обов'язків, що додається.

2. Заступникам начальника Старобільської міської військової адміністрації та керівникам структурних підрозділів Старобільської міської ради:

2.1. Забезпечити ознайомлення працівників з Інструкцією під особистий підпис шляхом подання власноруч написаного повідомлення про ознайомлення.

2.2. Організувати неухильне дотримання працівниками вимог цієї Інструкції під час виконання службових обов'язків.

2.3. Забезпечити контроль за виконанням вимог цієї Інструкції та вживати заходів реагування у разі виявлення порушень.

3. Контроль за виконанням цього розпорядження залишаю за собою.

Начальник **Яна ЛІТВІНОВА**

ЗАТВЕРДЖЕНО
Розпорядження начальника
Старобільської міської військової
адміністрації Старобільського району
Луганської області
від 12.06.2026 №65

ІНСТРУКЦІЯ
щодо забезпечення інформаційної безпеки та кіберзахисту працівниками Старобільської міської військової адміністрації та структурних підрозділів Старобільської міської ради Луганської області під час виконання службових обов'язків

1. Загальні положення

1.1. Ця Інструкція визначає основні вимоги щодо забезпечення інформаційної безпеки працівниками Старобільської міської військової адміністрації та структурних підрозділів Старобільської міської ради Луганської області (далі – працівники) під час використання інформаційно-комунікаційних систем, комп'ютерної техніки, мобільних пристроїв, електронної пошти, мережі Інтернет, соціальних мереж та месенджерів.

1.2. Метою цієї Інструкції є забезпечення належного рівня захисту інформації під час виконання службових обов'язків (далі-службова інформація), запобігання її втраті, розголошенню або несанкціонованому доступу до неї, мінімізація ризиків виникнення кіберінцидентів та кібератак.

1.3. Вимоги Інструкції є обов'язковими для виконання всіма працівниками незалежно від займаної посади.

1.4. Працівники зобов'язані дотримуватися вимог законодавства України у сфері захисту інформації, кібербезпеки, захисту персональних даних, зокрема:

Закону України «Про інформацію»;

Закону України «Про захист інформації в інформаційно-комунікаційних системах»;

Закону України «Про захист персональних даних»;

Закону України «Про основні засади забезпечення кібербезпеки України»;

Закону України «Про правовий режим воєнного стану»;

інших нормативно-правових актів у сфері захисту інформації та кібербезпеки.

1.5. Кожен працівник несе персональну відповідальність за дотримання вимог цієї Інструкції та збереження інформації під час виконання обов'язків.

2. Визначення термінів

Відповідно до статті 1 Закону України від 19 жовтня 2025 року № 4336-IX "Про основні засади забезпечення кібербезпеки України" (зі змінами) нижченаведені терміни в цій Інструкції вживаються в такому значенні:

1) індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

2) інформація про інцидент кібербезпеки - відомості про обставини кіберінциденту, зокрема про те, які об'єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

3) інцидент кібербезпеки (далі - кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

4) кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

5) кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

6) кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

7) кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на захист від кіберзагроз, забезпечення кібербезпеки, стійкості, цілісності, доступності та конфіденційності інформаційних ресурсів у кіберпросторі, а також здатності інфраструктури до їх обробки;

8) кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

9) кіберзлочинність - сукупність кіберзлочинів;

10) кібероборона - сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових,

організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

11) кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

(залишити терміни, які реально використані в цій інструкції).

2. Захист облікових записів та паролів

2.1. Для доступу до інформаційних ресурсів працівники повинні використовувати надійні паролі довжиною не менше 12 символів, які містять великі та малі літери, цифри та спеціальні символи.

2.2. Забороняється:

повідомляти свої паролі іншим особам;

використовувати однакові паролі для різних ресурсів;

записувати паролі на паперових носіях, що перебувають у відкритому доступі;

зберігати паролі у незахищених текстових файлах або повідомленнях.

2.3. Для ресурсів, де це технічно можливо, обов'язково використовується двофакторна автентифікація.

2.4. У разі виникнення підозри щодо компрометації пароля працівник зобов'язаний негайно змінити його та повідомити профільного заступника начальника Старобільської міської військової адміністрації, керівника структурного підрозділу Старобільської міської ради Луганської області або начальника Старобільської міської військової адміністрації.

3. Робота з електронною поштою

3.1. Для листування використовуються виключно офіційні електронні адреси.

3.2. Працівники повинні перевіряти адресу відправника та зміст отриманих повідомлень перед відкриттям вкладень або переходом за посиланнями.

3.3. Забороняється:

відкривати вкладення або переходити за посиланнями з підозрілих повідомлень;

використовувати особисті електронні скриньки для службового листування;

пересилати службову інформацію стороннім особам без відповідного погодження;

надавати службову інформацію у відповідь на запити невідомих осіб.

3.4. У разі отримання підозрілого електронного листа працівник зобов'язаний негайно повідомити профільного заступника начальника Старобільської міської військової адміністрації, керівника структурного підрозділу Старобільської міської ради Луганської області або начальника Старобільської міської військової адміністрації.

4. Робота в мережі Інтернет

4.1. Доступ до мережі Інтернет здійснюється для виконання службових завдань та функцій.

4.2. Забороняється:

завантажувати програмне забезпечення з неперевірених джерел;

використовувати інформаційні ресурси держави-агресора та ресурси, щодо яких застосовано санкції;

відвідувати вебресурси сумнівного походження;

вимикати або обходити засоби захисту інформації;

використовувати програмні продукти, хмарні сервіси, електронні поштові сервіси, месенджери та інші інформаційні ресурси держави-агресора, а також програмне забезпечення, щодо якого застосовано санкції відповідно до законодавства України.

4.3. Перед введенням службових або персональних даних працівник повинен переконатися у справжності вебресурсу та наявності захищеного з'єднання.

4.4. Забороняється використовувати службові облікові записи для реєстрації на сторонніх вебресурсах, не пов'язаних із виконанням службових обов'язків.

5. Використання комп'ютерної техніки та мобільних пристроїв

5.1. Усі службові комп'ютери та мобільні пристрої повинні бути захищені паролем або іншими засобами автентифікації.

5.2. Працівник зобов'язаний:

блокувати робочу станцію при залишенні робочого місця;

регулярно встановлювати оновлення операційної системи та програмного забезпечення;

використовувати виключно ліцензійне програмне забезпечення;

забезпечувати резервне копіювання важливих документів відповідно до встановленого порядку;

використовувати антивірусне програмне забезпечення .

5.3. Забороняється:

підключати невідомі зовнішні носії інформації;

використовувати службову техніку для встановлення неліцензійного програмного забезпечення;

передавати службові пристрої стороннім особам.

5.4. У разі втрати, викрадення або пошкодження службового пристрою працівник повинен невідкладно повідомити профільного заступника начальника Старобільської міської військової адміністрації, керівника структурного підрозділу Старобільської міської ради Луганської області або начальника Старобільської міської військової адміністрації..

6. Використання соціальних мереж та месенджерів

6.1. Працівникам забороняється розміщувати або поширювати:

службову інформацію;

внутрішні документи та листування;

відомості про діяльність військової адміністрації, які не призначені для оприлюднення;

документи, що містять персональні дані, службову інформацію або іншу інформацію з обмеженим доступом, якщо такий спосіб передачі не погоджений керівництвом та не забезпечує належного рівня захисту інформації.

6.2. Забороняється публікувати фотографії:

службових документів;
екранів комп’ютерів;
робочих приміщень із видимими документами чи технічними засобами;
об’єктів критичної інфраструктури без відповідного дозволу.

6.3. Під час використання месенджерів необхідно застосовувати лише дозволені канали комунікації та не передавати службові документи через незахищені сервіси.

Використання мереж Wi-Fi та дистанційна робота

7.1. Забороняється використовувати відкриті або незахищені мережі Wi-Fi для роботи зі службовою інформацією.

7.2. У разі роботи поза службовим приміщенням рекомендується використовувати мобільний інтернет або захищені канали зв’язку.

7.3. Функцію автоматичного підключення до бездротових мереж необхідно вимикати.

7.4. Під час дистанційної роботи працівник зобов’язаний забезпечити неможливість доступу сторонніх осіб до службової інформації та техніки.

7.5. Забороняється:
використовувати комп'ютерну техніку третіх осіб;
передавати службові пристрої членам сім'ї або іншим особам;
залишати без нагляду носії інформації та службові документи.

8. Дії у разі кіберінциденту

8.1. Ознаками можливого кіберінциденту можуть бути:
несанкціонований доступ до облікових записів;
блокування пристрою або файлів;
поява невідомих програм;
зміна налаштувань без відома користувача;
надсилання повідомлень від імені працівника без його участі;
інша підозріла активність.

8.2. У разі виявлення ознак кіберінциденту працівник повинен:
негайно припинити роботу з відповідним ресурсом;
повідомити безпосереднього керівника;
за можливості відключити пристрій від мережі Інтернет;
не видаляти файли та не здійснювати самостійних спроб усунення інциденту.

8.3. Відповідальна особа з питань інформаційної безпеки визначається розпорядженням начальника Старобільської міської військової адміністрації та забезпечує фіксацію, аналіз та реагування на кіберінцидент у встановленому порядку.

9. Навчання

9.1. Працівники зобов’язані проходити навчання, інструктажі для удосканалення знань з питань інформаційної безпеки.

10. Прикінцеві положення

10.1. Працівники проходять ознайомлення з цією Інструкцією шляхом подання повідомлення написано власноруч з особистим підписом;

10.2. Контроль за виконанням вимог цієї Інструкції покладається на керівників структурних підрозділів, профільних заступників начальника

Старобільської міської військової адміністрації за відповідним напрямком роботи;

10.3. Порушення вимог кібербезпеки та цієї Інструкції може тягнути за собою відповідальність відповідно до законодавства України.

Перший заступник начальника
Старобільської міської військової
адміністрації Старобільського району
Луганської області Юлія ЯКУЩЕНКО