ХЕРСОНСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ

РОЗПОРЯДЖЕННЯ
НАЧАЛЬНИКА ОБЛАСНОЇ ВІЙСЬКОВОЇ АДМІНІСТРАЦІЇ

04.05.2026 Херсон 158

Про затвердження Інструкції щодо кібергігієни для працівників апарату Херсонської обласної державної адміністрації та структурних підрозділів Херсонської обласної державної адміністрації без статусу юридичних осіб публічного права

Відповідно до постанови Кабінету Міністрів України від 08 жовтня 2025 року № 1281 «Про затвердження Порядку проведення інструктажів та систематичних тренінгів щодо кібергігієни», наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 21 жовтня 2025 року № 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», керуючись статтею 6, пунктом 1 частини першої статті 39, частиною першою статті 41 Закону України «Про місцеві державні адміністрації», частиною сьомою статті 15 Закону України «Про правовий режим воєнного стану», Указом Президента України від 24 лютого 2022 року № 68/2022 «Про утворення військових адміністрацій»:

1. Затвердити Інструкцію щодо кібергігієни для працівників апарату Херсонської обласної державної адміністрації та структурних підрозділів Херсонської обласної державної адміністрації без статусу юридичних осіб публічного права (далі – Інструкція), що додається.

2. Працівникам апарату Херсонської обласної державної адміністрації та структурних підрозділів Херсонської обласної державної адміністрації без статусу юридичних осіб публічного права (далі – працівники) забезпечити неухильне дотримання Інструкції.

3. Управлінню роботи з персоналом апарату Херсонської обласної державної адміністрації надавати до управління інформаційних технологій Херсонської обласної державної адміністрації інформацію про призначення нових працівників з метою проведення з ними інструктажів щодо кібергігієни.

4. Контроль за виконанням цього розпорядження покласти на заступника голови Херсонської обласної державної адміністрації з питань цифрового розвитку, цифрових трансформацій і цифровізації (CDTO) Толоконнікова О.С.

Начальник обласної
військової адміністрації Олександр ПРОКУДІН

ХЕРСОНСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ * УКРАЇНА * Управління з питань діловодства та доступу до публічної інформації апарату Херсонської обласної державної адміністрації Згідно з ЄДРПОУ 00022645

ЗАТВЕРДЖЕНО
Розпорядження начальника
обласної військової адміністрації
04.05.2026 № 158

ІНСТРУКЦІЯ
щодо кібергігієни для працівників
апарату Херсонської обласної державної адміністрації
та структурних підрозділів Херсонської обласної державної адміністрації
без статусу юридичних осіб публічного права

І. Загальні положення

1. Інструкція щодо кібергігієни для працівників апарату Херсонської обласної державної адміністрації та структурних підрозділів Херсонської обласної державної адміністрації без статусу юридичних осіб публічного права (далі – Інструкція) розроблена відповідно до постанови Кабінету Міністрів України від 08 жовтня 2025 року № 1281 «Про затвердження Порядку проведення інструктажів та систематичних тренінгів щодо кібергігієни», а також наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 21 жовтня 2025 року № 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. Інструкція є обов'язковою для всіх працівників апарату Херсонської обласної державної адміністрації та структурних підрозділів Херсонської обласної державної адміністрації без статусу юридичних осіб публічного права (далі – працівники) незалежно від їхньої посади та стажу роботи.

ІІ. Організація інструктажів та тренінгів

1. Метою інструктажів щодо кібергігієни є підвищення рівня обізнаності працівників та формування практичних навичок безпечного користування засобами інформатизації та Інтернетом для запобігання, своєчасного виявлення й 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.

2. Методи проведення інструктажів щодо кібергігієни:

очні тренінги, що включають інтерактивні сесії та відповіді на запитання працівників;

онлайн-курси (самостійне проходження курсів через спеціальні освітні платформи) та додаткові ресурси (спеціалізовані курси Тренінгового

кіберцентру Державної служби спеціального зв'язку та захисту інформації України, статті та рекомендації Департаменту кіберполіції Національної поліції України тощо);

інформаційні кампанії – розсилки, пам'ятки та оголошення, що нагадують про правила кібергігієни;

імітація атак – проведення контрольованих фішингових атак з метою перевірки пильності працівників та надання зворотного зв'язку.

3. Проведення інструктажів та тренінгів щодо кібергігієни для працівників здійснюється з такою періодичністю:

після призначення їх на посади – протягом одного календарного місяця після дати призначення на посаду (первинний);

не рідше одного разу на рік протягом всього строку перебування на посадах (повторний);

після настання значного кіберінциденту, кібератаки – протягом одного календарного місяця після дня настання (позаплановий);

за потреби згідно з результатами аналізу ризиків (цільовий).

4. Проведення інструктажів із працівниками фіксується працівниками управління інформаційних технологій Херсонської обласної державної адміністрації (далі – УІТ) в журналі обліку інструктажів щодо кібергігієни за формою, визначеною в додатку до цієї Інструкції.

III. Тематика інструктажів

Інструктажі щодо кібергігієни для працівників охоплюють такі ключові теми:

безпека на робочому місці;

правила безпечного використання електронної пошти;

створення та зберігання надійних паролів;

безпечна робота з даними;

безпека пристроїв;

безпека бездротової мережі;

реагування на інциденти.

IV. Безпека на робочому місці

Мета цього інструктажу – підвищення обізнаності працівників про загрози на робочому місці та набуття навичок ефективного захисту від них.

Основні види кібератак:

Фішинг: спроба зловмисників отримати конфіденційну інформацію (логіни, паролі, дані банківських карток) шляхом маскування під надійне джерело (наприклад, колегу, керівника або банк).

Приклади:

лист із проханням терміново надати пароль;

повідомлення про нібито виграш, для отримання якого потрібно ввести особисті дані.

Шкідливе програмне забезпечення: програми, розроблені для деградації продуктивності, некоректної роботи програмного забезпечення, несанкціонованих змін у системі та потенційної компрометації інформації. Вони можуть потрапити на комп'ютер через вкладення електронної пошти, завантаження з ненадійних джерел або відвідування заражених вебсайтів.

Різновиди:

віруси: поширюються, прикріплюючись до файлів;

троянські програми: маскуються під корисні програми, але всередині містять шкідливий код;

віруси-вимагачі: шифрують файли на комп'ютері й вимагають викуп за їх розблокування.

Соціальна інженерія: набір психологічних маніпуляцій, спрямованих на те, щоб змусити працівника розкрити конфіденційну інформацію або виконати певні дії. Це може бути телефонний дзвінок нібито від «системного адміністратора» з проханням назвати пароль або запит у месенджері від «керівника».

Атаки на незахищені бездротові мережі: Підключення до публічних і незахищених мереж (наприклад, у кафе чи аеропортах) може призвести до перехоплення трафіку зловмисниками.

Методи кіберзахисту

Управління паролями:

створення складних та унікальних паролів для кожного робочого облікового запису;

використання корпоративних менеджерів паролів для безпечного зберігання та управління паролями;

багатофакторна автентифікація всюди, де це можливо.

Безпечна робота з електронною поштою:

перевірка адреси відправника;

недовіра підозрілим або невідомим адресам;

ігнорування посилань та вкладень з підозрілих листів.

Захист робочих пристроїв:

установлення оновлень операційної системи та програмного забезпечення (далі – ПЗ), що використовуються УІТ.

Робота з конфіденційними даними:

зберігання конфіденційної інформації лише у призначених для цього місцях (наприклад, на корпоративному сервері, а не на робочому столі);

недопущення залишення конфіденційних документів без нагляду;

блокування комп'ютера під час відходу від нього.

Дії у разі кіберінциденту:

якщо є підозра, що комп'ютер скомпрометований (заражений), негайно відключити його від мережі (витягнути кабель);

якщо стали жертвою фішингу, негайно змінити пароль і повідомити про це безпосереднього керівника та УІТ;

повідомляти про всі підозрілі події, листи та повідомлення безпосереднього керівника та УІТ.

Додаткові правила поведінки

Віддалена робота:

використовувати VPN (віртуальну приватну мережу) для підключення до корпоративної мережі з дому;

уникати використання публічних бездротових мереж для роботи з корпоративною інформацією.

Знищення даних:

використовувати затверджені процедури для видалення конфіденційних даних з метою недопущення потрапляння їх до сторонніх.

Фізична безпека:

захищати робочі пристрої від крадіжки. У разі віддаленої роботи тримати пристрої при собі.

V. Правила безпечного використання електронної пошти

Мета цього інструктажу – ознайомлення працівників з основними загрозами, пов'язаними з використанням електронної пошти, та оволодіння ними правилами безпеки для захисту персональних даних, особистої інформації та корпоративної мережі.

Управління паролями та обліковим записом:

надійність паролів: пароль має бути унікальним і складним, містити комбінацію великих і малих літер, цифр і спеціальних символів. Уникати використання очевидної інформації, наприклад, дат народження або імен близьких;

різні паролі: не використовувати один і той самий пароль для різних облікових записів. Якщо один із них буде «зламано», інші залишаться захищеними;

багатофакторна автентифікація: додатковий рівень захисту вимагає підтвердження входу, наприклад, через sms-повідомлення, електронну пошту або спеціальний застосунок. Це значно ускладнює доступ зловмисникам;

регулярне оновлення паролів: час від часу (кожні три місяці) змінювати паролі, особливо якщо є підозра, що вони могли бути скомпрометовані.

Розпізнавання фішингових листів

Фішинг – це поширений вид шахрайства, коли зловмисники маскуються під надійне джерело (наприклад, банк, державну установу або колегу), щоб виманити конфіденційні дані.

Ознаки фішингових листів:

підозрілий відправник: адреса електронної пошти відправника може бути схожою на офіційну, але містити незначні помилки або зайві символи;

непереконливий текст: часто містить граматичні помилки, незвичні формулювання або дивний тон, нехарактерний для офіційного листування;

сумнівні посилання: навести курсор на посилання, щоб побачити повну адресу (але не натискати!). Якщо адреса виглядає дивно, це може бути фішинг. Завжди вводити адреси сайтів вручну;

термінові заклики: листи можуть вимагати негайних дій, погрожуючи блокуванням облікового запису або іншими негативними наслідками;

вимога конфіденційних даних: прохання надати паролі, номери карток або іншу особисту інформацію через пошту – це завжди шахрайство.

Обережність із вкладеннями та посиланнями:

не відкривати вкладення від невідомих відправників. У вкладених файлах можуть міститися віруси або шкідливе ПЗ. Якщо файл неочікуваний, краще не відкривати його;

перевіряти вкладення від знайомих. Навіть якщо лист надіслано від колеги чи знайомого, але зміст здається нетиповим, уточнити у відправника іншим каналом зв'язку (наприклад, телефоном) чи насправді відправник надсилав цей файл. Пошта відправника могла бути скомпрометована;

не натискати на підозрілі посилання. У разі надходження листа з незрозумілим посиланням, краще його проігнорувати. Якщо це може бути важлива інформація, перейти на сайт вручну через браузер.

Загальні правила безпеки:

не використовувати публічні бездротові мережі для доступу до пошти. Відкриті мережі можуть бути перехоплені зловмисниками. Завжди використовувати захищені мережі або VPN;

використовувати окрему поштову скриньку для робочого та особистого листування. Це допомагає уникнути витоку корпоративної інформації та захистити особисті дані;

не поширювати електронну адресу без потреби. Це допоможе зменшити кількість спаму;

оновлювати ПЗ. Завжди вчасно оновлювати операційну систему, браузери та антивірусні програми для захисту від нових загроз;

негайно повідомляти про інциденти. Якщо обліковий запис скомпрометовано («зламано») або отримано фішинговий лист, негайно повідомити про це безпосереднього керівника та УІТ.

VI. Створення та зберігання надійних паролів

Мета цього інструктажу – навчити працівників створювати та зберігати безпечні паролі.

Створення безпечного пароля є важливим завданням для забезпечення захисту особистої інформації.

Основні правила створення безпечного пароля:

використання різних паролів для різних сервісів. При використанні одного й того ж пароля для різних сервісів виникає ризик. Якщо хакер «зламає» один з акаунтів, то він отримає доступ до всіх інших, для яких використовується цей же пароль;

використання довгих паролів. Довгі паролі складніше «зламати». Рекомендується використовувати паролі довжиною не менше 8 – 14 символів;

використання комбінацій символів. Комбінації символів (цифр, літер верхнього і нижнього регістрів та спеціальних символів) роблять паролі

складнішими для «зламу». Наприклад, пароль «P@ssw0rd» є складнішим для «зламу», ніж простий пароль «password»;

уникати використання як пароля особистих даних, таких як ім'я, дата народження, адреса електронної пошти, номер телефону тощо. Ці дані легкодоступні для хакерів, які можуть використовувати їх для «зламу» акаунтів;

не зберігати паролі відкрито: на комп'ютері, мобільному пристрої чи в онлайн-сервісах. Якщо хакер отримає доступ до пристрою, він може легко знайти паролі та використовувати їх у злочинних цілях. Рекомендовано використовувати менеджери паролів для зберігання паролів у зашифрованому вигляді;

періодично змінювати паролі. Рекомендовано змінювати паролі періодично (раз на три місяці), щоб запобігти їх «зламу». Це особливо важливо для сервісів, що містять чутливу інформацію, таку як банківські акаунти або особисті електронні пошти;

використовувати багатофакторну автентифікацію. Наприклад, двоетапна автентифікація (2FA) є додатковим етапом захисту для акаунту. Під час входу до акаунту, крім пароля, потрібно ввести додатковий код, який можна отримати на мобільний пристрій або інший підключений пристрій. Це робить акаунт більш захищеним від хакерських атак.

VII. Безпечна робота з даними

Мета цього інструктажу – довести до працівників основні правила роботи з конфіденційними даними для запобігання їх витоку, пошкодженню або несанкціонованому доступу до них.

Класифікація даних

Кожен працівник повинен розуміти та розрізняти дані за ступенем конфіденційності:

публічні: інформація, яка не є конфіденційною і може вільно поширюватися;

внутрішні: дані, призначені для корпоративного використання, але які не становлять критичної загрози у разі витоку;

конфіденційні: інформація, яка може завдати шкоди у разі розголошення. Це дані з обмеженим доступом, що стосуються фізичних осіб (персональні дані), або інформація, обмежена юридичними особами, якою володіють працівники;

секретні: відомості у сфері оборони, економіки, безпеки та зовнішніх зносин, розголошення яких завдає шкоди національній безпеці.

Правила зберігання конфіденційних даних

Місце зберігання.

Конфіденційні дані слід зберігати тільки на захищених корпоративних ресурсах:

корпоративні сервери;

зашифровані мережеві диски;

спеціальні хмарні сховища, які використовуються Херсонською обласною державною адміністрацією.

Фізичний доступ.

Необхідно забезпечити фізичний захист носіїв інформації:

не залишати документи з конфіденційною інформацією на робочому столі без нагляду;

використовувати сейфи для зберігання паперових носіїв та захищених переносних пристроїв (USB-накопичувачі, зовнішні жорсткі диски тощо) у безпечному місці.

Електронний доступ.

Використовувати надійні методи захисту електронних даних:

встановити надійні паролі для всіх файлів і документів, що містять конфіденційні дані;

використовувати шифрування, за потреби перенести дані на зовнішній носій;

не зберігати конфіденційну інформацію на особистих пристроях або в особистих хмарних сховищах.

Резервне копіювання.

Регулярно створювати резервні копії важливих даних. Це допоможе відновити інформацію у разі її втрати, пошкодження або атаки вірусу-здирника.

Правила передачі конфіденційних даних

Належні канали зв'язку.

Передавати конфіденційні дані тільки через корпоративну електронну пошту.

Уникати незахищених каналів.

Категорично заборонено використовувати для передачі конфіденційних даних:

особисту електронну пошту;

публічні хмарні сервіси;

незахищені месенджери.

Перевірка одержувача.

Завжди переконуватися, що одержувач має право доступу до цієї інформації. У разі сумнівів уточнити через інший канал зв'язку.

Правила утилізації даних:

електронні носії: не видаляти конфіденційні дані простим переміщенням до «кошика». Використовувати спеціальне ПЗ для повного стирання інформації;

паперові носії: знищувати документи за допомогою шредера.

Відповідальність:

особиста відповідальність: кожен працівник несе персональну відповідальність за збереження та нерозголошення конфіденційної інформації;

звітування про інциденти: у разі втрати або компрометації конфіденційної інформації необхідно негайно повідомити про це безпосереднього керівника та УІТ.

VIII. Безпека пристроїв

Мета цього інструктажу – довести до працівників основні правила запобігання витоку даних і захисту пристроїв.

Безпека пристроїв – це комплекс заходів, спрямованих на захист комп'ютерів, смартфонів, планшетів та інших гаджетів від несанкціонованого доступу, шкідливого ПЗ та втрати даних. Це невід'ємна частина загальної кібербезпеки, адже незахищений пристрій може стати вразливим місцем для зловмисників.

Ключові принципи та заходи захисту:

використання надійних паролів та багатофакторної автентифікації: встановлення складних, унікальних паролів на всіх пристроях і в облікових записах, а також активація багатофакторної автентифікації значно підвищує рівень захисту;

регулярне оновлення ПЗ: важливо своєчасно встановлювати оновлення для операційних систем і додатків, оскільки це допомагає усунути відомі вразливості, якими можуть скористатися хакери;

встановлення антивірусного та антишпигунського ПЗ: антивірусне ПЗ захищає від вірусів, програм-вимагачів та інших шкідливих програм, скануючи пристрій на наявність загроз;

шифрування даних, яке перетворює конфіденційну інформацію на незрозумілі коди, що допомагає захистити її у разі втрати або викрадення пристрою;

обережна робота з публічними бездротовими мережами: слід уникати передачі конфіденційних даних через незахищені публічні мережі. Для безпечного з'єднання варто використовувати VPN;

обмеження доступу до застосунків: регулярний перегляд і обмеження дозволів для застосунків допомагає запобігти доступу до особистих даних, якщо програма виявиться шкідливою;

обережність з посиланнями та вкладеннями: важливо не переходити за підозрілими посиланнями та не відкривати вкладення з електронних листів від невідомих відправників;

резервне копіювання даних: регулярне створення резервних копій важливих файлів на зовнішньому носії або у хмарному сховищі дасть змогу відновити інформацію у разі її втрати;

налаштування блокування пристрою: використання біометричних даних (відбиток пальця, Face ID тощо) або надійного коду для блокування пристрою – це перший рубіж захисту від несанкціонованого доступу;

віддалене керування: налаштування функцій віддаленого відстеження та видалення даних дозволяє захистити інформацію у разі втрати або крадіжки пристрою.

IX. Безпека бездротової мережі

Мета цього інструктажу – довести до працівників рекомендації щодо захисту бездротової мережі вдома для зменшення ризику незаконного доступу зловмисників до особистих даних, паролів, особистих ключів для створення електронного підпису, банківських даних та рахунків тощо.

Рекомендації щодо захисту бездротової мережі:

обирати роутер зі стійкими протоколами безпеки. Важливо вибирати роутери з протоколами безпеки WPA3 або WPA2, оскільки WEP та WPA вважаються застарілими та менш безпечними;

встановити надійні логіни та паролі. Змінити стандартні логіни та паролі від виробника та створити власні. Зробити це потрібно перш ніж підключати роутер до Інтернету;

налаштувати списки доступу за визначеними атрибутами (наприклад, MAC-адреса);

приховати SSID (назву бездротової мережі) зі списку доступних мереж задля уникнення виявлення мережі сторонніми користувачами;

створити окрему бездротову мережу для відвідувачів. Вони зможуть підключатися до Інтернету, але не знатимуть основного пароля;

зменшити зону покриття роутера. Обмежити зону покриття бездротової мережі так, щоб сигнал був доступний лише у приміщеннях;

вимкнути функцію WPS – це додатковий захист, що дає змогу підключати пристрої без введення пароля.

X. Реагування на кіберінциденти

Кіберінцидент – це подія навмисного або ненавмисного характеру, яка становить загрозу безпеці інформаційних систем або мереж та може призвести до порушення їх нормального функціонування.

Реагування на інциденти – це організований підхід до управління наслідками кібератаки, витоку даних, збою в роботі системи або іншої події, яка загрожує безпеці інформації. Ефективне реагування допомагає мінімізувати збитки, швидко відновити нормальну роботу та запобігти подібним інцидентам у майбутньому. Це ключова частина загальної стратегії кібербезпеки.

Етапи реагування на інциденти

Процес реагування зазвичай складається з кількох етапів, визначених міжнародними стандартами.

Ідентифікація

Цей етап передбачає виявлення інциденту та збір інформації. Важливо не переплутати звичайні події з реальним інцидентом.

Дії включають:

моніторинг: постійний контроль за системою на предмет підозрілої активності;

аналіз даних: збір журналів подій, аналіз мережевого трафіку;

оцінка інциденту: визначення масштабу, типу та потенційного впливу інциденту.

Ізоляція (стримування)

Основна мета цього етапу – не допустити подальшого поширення інциденту, і він може включати:

відключення: від'єднання уражених пристроїв або сегментів мережі від основної інфраструктури;

блокування: ізоляція шкідливого ПЗ або облікових записів;

усунення вразливостей: закриття прогалин, через які відбулася атака.

Усунення (видалення)

Після ізоляції інциденту необхідно видалити шкідливі елементи, що передбачає:

видалення шкідливого ПЗ: видалення вірусів, програм-вимагачів або інших шкідливих програм;

очищення системи: відновлення системи до стану, що передував атаці, або її перевстановлення.

Відновлення

На цьому етапі відбувається повернення системи до нормальної роботи, що включає:

відновлення системи: повернення до роботи уражених систем;

перевірку: тестування системи для впевненості у повній безпеці;

посилення захисту: застосування додаткових заходів безпеки задля уникнення повторного інциденту.

Аналіз

Після повного усунення інциденту проводиться ретельний аналіз для виявлення причин і покращення захисту, що включає:

збір інформації: документування всіх обставин інциденту, вжитих заходів та їх ефективності;

аналіз першопричин: виявлення корінної причини інциденту;

оновлення політик безпеки: внесення змін до політик і процедур безпеки для запобігання подібним атакам у майбутньому.

XI. Відповідальність

Працівники несуть персональну відповідальність за дотримання вимог Інструкції.

За умисне порушення вимог Інструкції, що призвело до витоку інформації або компрометації системи, працівник може бути притягнутий до дисциплінарної або кримінальної відповідальності відповідно до чинного законодавства.

Заступник начальника управління
інформаційних технологій
обласної державної адміністрації –
начальник відділу цифрового забезпечення Олександр КАСІЧ

Додаток
до Інструкції
(пункт 4 розділу II Інструкції)

Форма

ЖУРНАЛ
обліку інструктажів щодо кібергігієни
в Херсонській обласній державній адміністрації

№ п/п	Дата проведення інструктажу	Назва (тип) інструктажу	Прізвище, ініціали працівника, який проходив інструктаж	Посада працівника, який проходив інструктаж	Підпис працівника про проходження інструктажу	Прізвище, ініціали працівника, який проводив інструктаж
1	**2**	**3**	**4**	**5**	**6**	**7**