ДЕРЖПРОД
СПОЖИВСЛУЖБА

Практичні рекомендації щодо кібергігієни

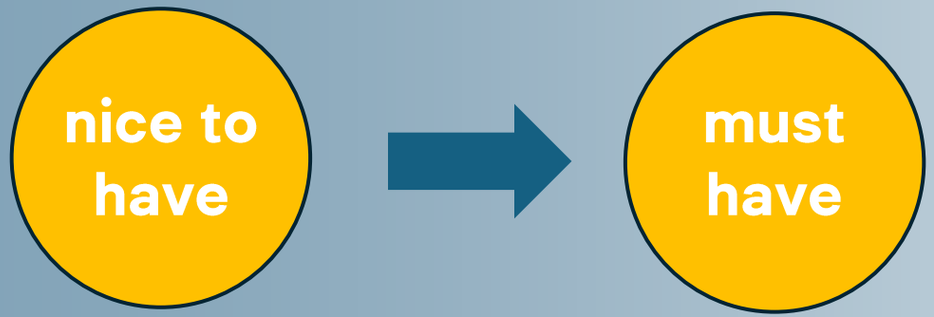
Тимощук Анастасія
Головний спеціаліст відділу адміністрування інформаційних ресурсів
Управління цифрового розвитку, цифрових трансформацій і цифровізації

UB
Держпродспоживслужба
№25-3/23839 від 17.09.2025
КЕП: Захарін С. В. 17.09.2025 12:52
3FAA9288358EC003040000006C53360034A7E200
Сертифікат дійсний з 03.04.2025 13:12 до 01.04.2027 13:12

ДЕРЖПРОД
СПОЖИВСЛУЖБА

Яка мета кібергігієни?

Кібергігієна — це базовий набір дій користувача під час взаємодії з цифровими активами організації.



Кінцева **мета** полягає у зниженні ризику спрацювання загрози, що, в свою чергу, має позитивно вплинути на загальну кібербезпеку організації.

З урахуванням постійного зростання цифровізації процесів і нестримного розвитку кіберзагроз, питання належної кібергігієни трансформувалось з опціональної чи рекомендованої практики (nice to have) в фундаментальний та критично важливий компонент (must have).

UB Держпродспоживслужба
№25-3/23839 від 17.09.2025
арк.1

ДЕРЖПРОД
СПОЖИВСЛУЖБА

Людський фактор!

Людський фактор – один з ключових векторів, використовуваних зловмисникам.

Використання скомпрометованих облікових даних залишається одним із найпоширеніших напрямів атак, причому негативні наслідки від таких інцидентів часто вищі через тривалий час їх виявлення та усунення.

Зверніть увагу!

68% усіх витоків даних пов'язані з людським фактором без злого умислу, коли людина стає жертвою соціальної інженерії або допускає певну помилку

- Звіт Verizon Data Breach Investigations Report (DBIR) за 2025 рік

UB Держпродспоживслужба
№25-3/23839 від 17.09.2025
арк.1

ДЕРЖПРОД
СПОЖИВСЛУЖБА

Правова база

План реалізації Стратегії кібербезпеки України схвалений рішенням Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України», уведений у дію Указом Президента України від 1 лютого 2022 року № 37/2022 містять такі завдання:

- ціль К1 «Національна кіберготовність та надійний кіберзахист» завдання 50
- ціль К.2. «Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки» завдання 59

Стратегія кібербезпеки України затверджена Указом Президента України від 26 серпня 2021 року № 447/2021

Указ

Президента України

Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"

Відповідно до статті 107 Конституції України **п о с т а н о в л я ю :**

1. Увести в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" (додається).

2. Затвердити Стратегію кібербезпеки України (додається).

3. Визнати такою, що втратила чинність, статтю 2 Указу Президента України від 15 березня 2016 року № 96 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України".

4. Контроль за виконанням рішення Ради національної безпеки і оборони України, введеного в дію цим Указом, покласти на Секретаря Ради національної безпеки і оборони України.

5. Цей Указ набирає чинності з дня його опублікування.

Президент України **В.ЗЕЛЕНСЬКИЙ**

м. Київ
26 серпня 2021 року
№ 447/2021

UB Держпродспоживслужба
№25-3/23839 від 17.09.2025
арк.1

ДЕРЖПРОД
СПОЖИВСЛУЖБА

Базові принципи кібергігієни

«Дотримання базових правил кібергігієни дозволяє запобігти кібер-інцидентів.» **90%**

- RSA Conference 2015, Bugcrowd

«Дотримання базових заходів кібергігієни може захистити від кібератак.» **98%**

- Microsoft Digital Defense Report 2022, Microsoft

Недостатня увага до базових принципів кібергігієни на індивідуальному та організаційному рівнях створює сприятливі умови для реалізації різноманітних атак. Серед них — фішинг, який є основною точкою входу для багатьох атак, руйнівні віруси-шифрувальники, що паралізують діяльність, а також складні цільові атаки (т.зв. Advanced Persistent Threat, APT).

UB Держпродспоживслужба
№25-3/23839 від 17.09.2025
арк.1

ДЕРЖПРОД
СПОЖИВСЛУЖБА

Базові принципи кібергігієни

1. Використовуйте лише складні паролі та обов’язково двофакторну автентифікацію
2. Регулярно оновлюйте програмне забезпечення, щоб уникнути вразливостей
3. На службових пристроях використовуйте лише службову електронну пошту

Приклади поганих паролів:
123456, qwerty, password, user, дата народження (01.01.1990)
Приклади надійних паролів:
V7k#92Lm!zQp, F1sh!ng_Is-B@d_77

UB Держпродспоживслужба
№25-3/23839 від 17.09.2025
арк.1

ДЕРЖПРОД
СПОЖИВСЛУЖБА

Робота з електронною поштою

1. Завжди перевіряйте відправника листа
2. Не відкривайте вкладення від невідомих осіб
3. Не переходьте за сумнівними посиланнями
4. Використовуйте шифрування для передавання конфіденційних документів.

Перелік підозрілих розширень файлів, які зазвичай використовують зловмисники для поширення вірусів та троянів.

- Виконувані файли (.exe, .bat, .cmd, .msi)
- Сценарії та макроси (.js, .vbs, .hta, wsf)
- Файли з подвійним розширенням (invoice.pdf.exe)
- Інші (.iso, .sys, .apk)

UB Держпродспоживслужба
№25-3/23839 від 17.09.2025
арк.1

ДЕРЖПРОД
СПОЖИВСЛУЖБА

Робота з документами та файлами

1. Використовуйте тільки перевірені носії інформації
2. Не завантажуйте файли з невідомих сайтів
3. Перевіряйте усі документи за допомогою антивірусного ПЗ
4. Зберігайте службові документи у хмарних сервісах з контролем доступу
5. Уникайте дублювання та хаотичного зберігання файлів

Безкоштовні антивіруси:

- Microsoft Defender
- Malwarebytes Free
- Avira Free Security
- AVG AntiVirus Free
- Avast One Essential

UB Держпродспоживслужба
№25-3/23839 від 17.09.2025
арк.1

ДЕРЖПРОД
СПОЖИВСЛУЖБА

Використання мобільних пристроїв

Якщо ви використовуєте робочі облікові записи на мобільних пристроях:

1. Встановіть пароль або біометричний захист на телефоні.

2. Для доступу до службових ресурсів використовуйте VPN

3. Не встановлюйте сторонні додатки з неперевірених сайтів. Лише з офіційних App Store, Google Play, Galaxy Store.

4. У разі втрати пристрою з робочим обліковим записом, попередьте адміністратора для блокування даного запису

! Не дозволяйте автоматичне збереження паролів у браузері чи сторонніх додатках

! Уникайте роботи з конфіденційними даними через публічні Wi-Fi мережі

UB Держпродспоживслужба
№25-3/23839 від 17.09.2025
арк.1

ДЕРЖПРОД
СПОЖИВСЛУЖБА

У разі виявлення підозрілої активності на пристрої, а саме:

- зміна паролів без вашої участі.
- неможливість отримати доступ до власних акаунтів або ресурсів.
- незрозумілі підключення до ресурсів з підозрілих ip-адрес
- розсилання з вашого акаунту повідомлень, без вашого відома,

звертайтеся в CERT-UA: cert@cert.gov.ua

Якщо під час компрометації облікового запису було викрадено кошти з банківської карти, звертайтеся до Кіберполіції: https://ticket.cyberpolice.gov.ua/

UB Держпродспоживслужба
№25-3/23839 від 17.09.2025
арк.1