



Державна служба
спеціального зв'язку та захисту
інформації України



МІСЯЦЬ
КІБЕРБЕЗПЕКИ

Кібергігієна: гайд

Зміст

Ст.

- | | | |
|-----|--|-------|
| 1. | Що таке кібергігієна і чому вона важлива. | 3–4 |
| 2. | Як захистити свої дані: загальні правила. | 5–7 |
| 3. | Паролі. | 8–10 |
| 4. | Двофакторна автентифікація. | 11–13 |
| 5. | Фішинг: як не стати жертвою. | 14–17 |
| 6. | Безпечне використання WI-FI. | 18–20 |
| 7. | Онлайн-сервіси зі штучним інтелектом: безпечне використання. | 21–25 |
| 8. | Програми та застосунки. | 26–27 |
| 9. | Онлайн-безпека дітей та підлітків. | 28–30 |
| 10. | Корисні контакти та посилання. | 31–32 |



Що таке кібергігієна і чому вона важлива

Кібергігієна – це базові правила безпечної поведінки в цифровому просторі, які допомагають кожній людині захистити особисті та робочі пристрої, а також особисті дані.

Кібергігієна починається з особистої відповідальності кожного, хто користується цифровими пристроями та сервісами, і має стати щоденною звичкою.

Недотримання правил кібергігієни може призвести до втрати персональних даних та конфіденційної інформації, фінансових втрат, шифрування або знищення важливих файлів і навіть до порушення роботи установи, де працює людина, або критично важливих сервісів.

А в умовах повномасштабної війни росії проти України, яка триває і в кіберпросторі, від цього може залежати навіть життя.



Як захистити свої дані: загальні правила

Базові правила кібергігієни

- 1.** Використовуйте складні та унікальні паролі для кожного акаунту, а також увімкніть двофакторну автентифікацію всюди, де це можливо (застосунки, акаунти в месенджерах, електронна пошта тощо).
- 2.** Регулярно оновлюйте операційну систему та програми. Користуйтеся лише ліцензійними програмами. Не використовуйте російського софту!
- 3.** Завантажуйте застосунки лише з офіційних магазинів та перевіряйте дозволи, які вони запитують. Обмежуйте доступ додатків до камери, мікрофона та геолокації. Видаляйте застосунки, якими не користуєтеся.
- 4.** Не публікуйте в соцмережах важливу особисту інформацію: адресу, номер телефону, документи тощо. Не надсилайте копії чи фото документів через незахищені канали зв'язку.
- 5.** Не переходьте за підозрілими посиланнями з листів або повідомлень, навіть якщо вони виглядають «офіційно» або надійшли від друзів чи знайомих.



6. Не вводьте будь-яких конфіденційних даних на незнайомих сайтах та не повідомляйте їх стороннім. Будьте уважні до дзвінків і повідомлень із «терміновими» проханнями щось підтвердити або завантажити.

7. Регулярно перевіряйте налаштування приватності у соціальних мережах і месенджерах, а також – активні сесії та пристрої, підключені до ваших акаунтів.

8. Не підключайся до відкритих Wi-Fi-мереж без потреби. Не використовуйте публічні мережі Wi-Fi для банківських операцій або входу в важливі акаунти. Не під'єднуйтеся до невідомих пристроїв, які роздають інтернет.

9. Навчайте цифрової безпеки дітей та літніх родичів, адже їх часто обирають мішенню зловмисники.

10. Дбайте про фізичну безпеку пристроїв (не губіть, слідкуйте, щоб не викрали тощо).



Надійні паролі

Пароль – ваш ключ від усіх важливих сервісів: пошти, акаунтів у соцмережах, банківських застосунків та інших, а також – перша лінія цифрового захисту. Важливо, щоб він був надійним.

Головні правила створення надійного пароля

- ✓ Пароль має містити щонайменше 12 символів (а краще – 16): великі та малі літери, цифри, спеціальні символи.
- ✓ Можна використовувати абстрактні фрази або комбінації слів, які незрозумілі для інших, але зрозумілі для вас (так звані паролі-фрази, passphrase).
- ✓ Пароль має знати тільки власник: не розкривайте його навіть рідним, друзям, коханим, колегам, і тим більше – випадковим знайомим.
- ✓ Щоб не тримати всі паролі у голові, використовуйте спеціальні менеджери паролів для зберігання (обирайте ті, що мають надійну репутацію).
- ✓ Паролі потрібно регулярно оновлювати. Змінювати паролі рекомендовано щонайменше раз на три місяці. Чим критичніший пароль і чим частіше використовується – тим частіше потрібно його змінювати. У разі підозри щодо компрометації пароля, його потрібно змінити негайно.

Приклад надійної комбінації, створеної за допомогою генератора паролів: 5Tx0p3j>:_Zh



- ✗ Не можна використовувати очевидні комбінації та послідовності на кшталт 123456, qwerty, password, iloveyou тощо.**
- ✗ Не можна використовувати як пароль власне ім'я, прізвище, дату народження чи інші персональні дані. Також не підходять імена, прізвища та будь-яка особиста інформації батьків, дітей, чоловіка або дружини чи інших родичів. Навіть кличка кота або собаки – поганий варіант для пароля.**
- ✗ Не використовуйте однакові паролі для різних сервісів та облікових записів. Запам'ятайте: для кожного акаунта – свій пароль.**
- ✗ Не рекомендується зберігати паролі в текстовому форматі або на паперових носіях (особливо поруч із пристроєм). Не бажано зберігати паролі в браузері.**
- ✗ Не надсилайте паролі через незахищені канали, такі як електронна пошта чи звичайний текстовий чат.**



Двофакторна автентифікація (2FA)

Одного пароля задля забезпечення надійного захисту пристроїв та акаунтів – недостатньо. Разом із ним обов'язково використовуйте двофакторну автентифікацію всюди, де можливо.

Двофакторна автентифікація пропонує додатковий рівень захисту, оскільки вимагає два різні способи підтвердження особи.

Якщо хтось намагатиметься увійти до вашого акаунту з незнайомого пристрою – наштовхнеться на ще одну перепону. Зловмисник зазнає невдачі, а ви отримаєте сповіщення про таку спробу несанкціонованого входу.

Надійні методи 2FA

- Використання одноразового коду, який генерується у спеціальному додатку і змінюється щохвилини (наприклад, Google Authenticator, Microsoft Authenticator).
- Використання апаратного ключа, токена (на кшталт YubiKey) тощо.
- ✅ Один із сучасних стандартів захисту – фішинг-резистентна багатофакторна автентифікація (Phishing-resistant MFA, PR-MFA), яка використовує асиметричну криптографію та прив'язку до домену, роблячи перехоплення чи підробку облікових даних технічно неможливими.



Важливо!

SMS-коди є поширеним методом двофакторної автентифікації, проте він має суттєві ризики і може бути небезпечним через можливість втратити контроль над номером телефону і перехоплення повідомлень.

При налаштуваннях двофакторної автентифікації за допомогою додатка варто зазначати альтернативний номер телефону чи адресу електронної пошти. Це дасть змогу відновити доступ до акаунту у випадку втрати пристрою.

Інструкції щодо встановлення 2FA зазвичай можна знайти в розділах «Налаштування» / «Безпека» застосунків та програм.



Фішинг: як не стати жертвою

Фішинг – це спроба зловмисників дістати доступ до конфіденційних даних користувачів шляхом маскуванню під надійні джерела. Фішинг може мати різні «обличчя», а найдієвіший засіб захисту від нього – пильність.

Види фішингу

- **phishing** – класичні шахрайські листи електронною поштою;
- **quishing** – шкідливі посилання, заховані у QR-кодах;
- **spearphishing** – персоналізовані атаки на конкретну людину чи організацію;
- **smishing** – шахрайство через SMS;
- **vishing** – обман за допомогою голосових дзвінків;
- **whaling** – атаки, спрямовані на керівників компаній;
- **BEC (business email compromise)** – компрометація ділового листування для фінансового шахрайства, під час якої зловмисники видають себе за довірених осіб (керівників, постійних партнерів або вендорів), щоб змусити працівника переказати кошти чи передати дані;
- **deerfakes** – підроблені аудіо- та відеоматеріали на основі ШІ.



Електронна пошта, месенджери – серед основних каналів, які використовуються для фішингових атак.

Зловмисники можуть надсилати листи, які імітують офіційні повідомлення органів державної влади, відомих організацій, служб тощо. В них часто просять користувача перейти за посиланням, завантажити файл або ввести облікові дані на підробленому сайті.

Остерігайтеся фішингових вебсайтів. Такі інтернет-сторінки можуть імітувати вигляд легітимних ресурсів: сайтів органів влади, банків, популярних сервісів тощо. Різниця може бути навіть в одній літері чи символі.

✓ Запам'ятайте: офіційні онлайн-ресурси державних органів України мають домен gov.ua.

Зверніть увагу: у соціальних мережах зловмисники можуть використовувати фальшиві профілі або ж зламані акаунти, щоб імітувати знайомих людей або колег.

! З розвитком ШІ і технологій deer-fake навіть відео- та аудіоповідомлення більше не є надійними. Ви можете спілкуватися зі знайомою особою по відеозв'язку в реальному часі, а насправді це може бути deer-fake зображення, накладене на іншу людину. Будьте обачні!



Як убезпечитися від фішингу

- Перевіряйте адресу відправника та URL перед переходом. **Https** – безпечний протокол, тоді як **http** – незахищений. Значок замка в адресному рядку браузера свідчить про шифрування з'єднання між вами і сайтом.
- Ніколи не вводьте паролі на сторінках, на які ви перейшли за посиланням із листа. Якщо повідомлення вимагає від вас авторизації, відкрийте нову вкладку і самостійно введіть адресу потрібного сайту вручну (або скористайтеся офіційним застосунком).
- Не відкривайте архівів та файлів з листів, навіть якщо вони нібито від знайомих чи партнерів.
- У разі сумнівів – звертайтеся до організації офіційними каналами.
- Увімкніть двофакторну автентифікацію, а краще – PR-MFA.
- Не скануйте QR-коди з невідомих джерел.
- Одна з найпоширеніших тактик шахраїв – створення нібито критичної ситуації, яка викликає у людини паніку, страх (наприклад: ваш рахунок буде заблоковано). Не реагуйте миттєво на заклик до термінових дій у повідомленнях. Аналізуйте та перевіряйте перед тим, як діяти.
- Критично оцінюйте дзвінки та відео з проханнями про термінові дії чи перекази коштів.



Безпечне використання WI-FI

Публічні мережі Wi-Fi – невід’ємна частина повсякденного життя. Ми використовуємо їх у магазинах, закладах харчування, на автозаправках тощо. Це зручно, допомагає заощадити мобільний трафік, але водночас такі мережі можуть загрожувати безпеці ваших персональних даних.

Зловмисники активно використовують відкриті мережі для перехоплення трафіку, крадіжки паролів, банківських даних і особистої інформації.

Як мінімізувати ризики під час користування публічним Wi-Fi

1. За можливості взагалі уникайте відкритих Wi-Fi-мереж без пароля. Якщо мережа не потребує автентифікації – це сигнал до підвищеної обережності. За змоги надавайте перевагу мобільному інтернету або власній точці доступу.

2. Перевіряйте назву мережі у персоналу закладу. Зловмисники часто створюють фейкові точки доступу зі схожими назвами (наприклад, «Free_Cafe_WiFi» замість «Cafe_Free_WiFi»), щоб користувачі підключилися саме до них.



3. Використовуйте VPN. Правильно налаштована віртуальна приватна мережа шифрує весь трафік між вашим пристроєм та інтернетом, що робить перехоплення даних практично марним для зловмисника.

4. Не виконуйте чутливих операцій через публічний Wi-Fi. Уникайте входу в інтернет-банкінг, поштові сервіси, державні портали (зокрема «Дія») та інші ресурси з конфіденційними даними, якщо це не є критично необхідним.

5. Вимкніть автоматичне підключення до Wi-Fi мереж. Ця функція в налаштуваннях смартфона чи ноутбука може автоматично з'єднати пристрій із небезпечною мережею без вашого відома.

6. Зберігайте паролі лише в парольних менеджерах, періодично перевіряйте і видаляйте збережені дані автозаповнення.

7. Завершуйте сеанси після закінчення роботи з важливими сервісами, а не просто закривайте вкладку браузера.



Сервіси зі штучним інтелектом: безпечне використання

Штучний інтелект (ШІ) – потужний інструмент, що відкриває нові можливості для роботи, навчання, творчості, спрощує виконання щоденних завдань. Він набуває дедалі більшої популярності.

Проте, як і будь-яка інша технологія, він вимагає відповідального та обережного підходу.



Правила безпеки при роботі з ШІ

1. Ніколи не вводьте конфіденційних даних та не надавайте чат-ботам жодної чутливої інформації. До такої належать:

- персональні дані: ПІБ, дата народження, ідентифікаційний код (РНОКПП), паспортні дані, адреса проживання;
- фінансова інформація: номери банківських карток, паролі до інтернет-банкінгу, дані про рахунки;
- медичні дані: діагнози, результати аналізів, історія хвороби;
- облікові дані: логіни, паролі, секретні запитання від будь-яких сервісів.

Пам'ятайте: вся введена інформація зберігається на серверах компанії-розробника та може бути використана для тренування моделі, а також асоціюватиметься конкретно з вами (вашим акаунтом).



2. Не використовуйте ШІ для роботи з документами, що містять інформацію з обмеженим доступом – конфіденційну, таємну, службову. Наприклад, дані про клієнтів, фінансові звіти компанії, тим більше – документи, що становлять державну таємницю. Це створює пряму загрозу національній та корпоративній безпеці.

3. Перевіряйте налаштування приватності. Сучасні ШІ-сервіси дозволяють керувати приватністю. Зайдіть у налаштування та перевірте такі опції:

- історія чатів (Chat History). Ви можете вимкнути збереження історії діалогів. У такому разі ваші розмови не будуть зберігатися та використовуватися для навчання моделі;
- використання даних для тренування. Деякі сервіси надають можливість заборонити використання ваших даних для вдосконалення ШІ.

4. Усвідомлюйте ризики функції «Поділитися» (Share). Функція створення посилання на діалог робить вашу розмову публічною. Не використовуйте цю функцію для обміну чутливою інформацією. Розглядайте таке посилання як публікацію в інтернеті – її може побачити будь-хто. Якщо ви ділитесь посиланням, переконайтеся, що в діалозі немає жодних даних, які могли б скомпрометувати вас чи інших людей.



5. Використовуйте анонімізацію даних. Якщо вам потрібно обговорити з ШІ певну ситуацію, що стосується реальних даних, замініть їх на вигадані або узагальнені.

6. Будьте обережні з розширеннями для браузерів. Існує багато сторонніх плагінів, які нібито розширюють можливості ШІ-сервісів. Встановлюйте розширення лише з офіційних магазинів та від перевірених розробників. Ненадійні плагіни можуть перехоплювати всі дані, які ви вводите.



Програми та застосунки

✓ Використовуйте лише ліцензійні та підтримувані операційні системи і програмні продукти.

✓ Своєчасно встановлюйте оновлення операційної системи, браузерів, офісних програм, месенджерів, засобів захисту та мікропрограмного забезпечення пристроїв. Вразливості в застарілому програмному забезпеченні активно використовуються злоумисниками.

✓ Встановлюйте програми та застосунки лише з офіційних та перевірених джерел. Не завантажуйте програмне забезпечення з випадкових сайтів, файлових архівів або за посиланнями з листів та повідомлень. Перед інсталяцією перевіряйте, які дозволи запитує програма і чи дійсно вони необхідні для її роботи.

✓ Якщо не користуєтеся застосунком – видаліть його з пристрою. Його завжди можна встановити знову у разі потреби.

✓ Регулярно створюйте резервні копії даних. Резервному копіюванню підлягають документи, бази даних, конфігурації, ключові службові файли та інша критична інформація. Резервні копії слід зберігати на окремих носіях або в ізольованому середовищі. Необхідно періодично перевіряти можливість відновлення даних із резервних копій.



Онлайн-безпека дітей та підлітків

Забезпечення безпеки, добробуту кожної дитини – найвищий пріоритет для дорослих. Важливо дбати і про те, щоб діти були захищені також в онлайн-просторі.

Рекомендації

- **Навчіть дитину базовим правилам кібергігієни. Розкажіть, як створювати надійні паролі, налаштовувати двофакторну аутентифікацію, чому не можна переходити за підозрілими посиланнями та завантажувати ігри чи програми з невідомих сайтів.**
- **Навчіть дитину тримати в секреті особисту інформацію. Не можна розголошувати в інтернеті номер телефону, дані про місце проживання тощо. Також не слід надсилати стороннім власні фото та відео.**
- **Розповідайте дітям, що довіряти незнайомцям – небезпечно. Спілкуватися краще лише з тими, кого дитина знає у реальному житті.**
- **Пояснюйте, чому потрібно ігнорувати підозрілі пропозиції в соцмережах і месенджерах. Наприклад, щодо особистих зустрічей, вчинення протиправних дій, запрошень брати участь у небезпечних квестах. Дитина має знати, що про подібні випадки потрібно обов'язково повідомити батьків.**



- Розкажіть дитині про те, що не вся інформація в інтернеті є правдою. Навчіть розпізнавати фейки та маніпуляції.
- Поясніть дитині, що робити у разі кібербулінгу: повідомити дорослого, зберегти докази, заблокувати кривдника тощо.
- Також навчайте етичної поведінки в онлайн-просторі: не можна ображати інших користувачів, цькувати однолітків, розповсюджувати без дозволу чужі фото.
- За потреби, щоб обмежити небажаний контент, налаштуйте «батьківський контроль» на смартфоні, планшеті та комп'ютері дитини.
- Розкажіть дитині про корисні можливості інтернету, про надійні сайти та застосунки.
- Будьте дитині другом, до якого вона може звернутися за порадою щодо будь-якої ситуації в онлайн-просторі.



Корисні контакти та посилання

■ На сайті Державної служби спеціального зв'язку та захисту інформації України ви знайдете більше рекомендацій щодо кібергігієни, безпеки в онлайн-просторі, а також поради для державних органів та організацій <https://cip.gov.ua/ua/faqs>

■ Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського, заклад освіти Держспецзв'язку, реалізує власну соціальну ініціативу «Кібергігієна в школах України», в межах якої учнів навчають протидіяти кібербулінгу, безпечно користуватися гаджетами, соцмережами, дбати про приватність в інтернет-просторі та захищати персональні дані тощо.

Контакти для тих, хто бажає долучитися:

 vstup@iscip.kpi.ua

 +380 63 937 27 00

■ Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA надає допомогу у разі кіберінцидентів державним органам, організаціям незалежно від форми власності.

Офіційний сайт команди: <https://cert.gov.ua/>
Повідомити про кіберінцидент: incidents@cert.gov.ua





МІСЯЦЬ
КІБЕРБЕЗПЕКИ

сір.gov.ua
2026



Державна служба
спеціального зв'язку та захисту
інформації України