

Методичні рекомендації
щодо способів фільтрації доступу до мережі Інтернет та протидії
шкідливому контенту в закладах освіти

1. Методичні рекомендації розроблені на виконання пункту 92 плану заходів на 2025-2026 роки з реалізації Національної стратегії із створення безбар'єрного простору в Україні на період до 2030 року, затвердженого розпорядженням Кабінету Міністрів України від 25 березня 2025 року № 374-р, завдань та заходів, передбачених Концепцією цифрової гігієни дітей дошкільного віку, схваленою розпорядженням Кабінету Міністрів України від 02 травня 2025 року № 432-р, з метою забезпечення безпечного використання інтернету в закладах загальної середньої, дошкільної та позашкільної освіти.

2. Створення безпечного освітнього середовища є пріоритетним завданням для закладів освіти. Відповідно до пункту 2¹ частини першої статті 1 Закону України «Про освіту» безпечне освітнє середовище - сукупність умов у закладі освіти, що унеможливають заподіяння учасникам освітнього процесу фізичної, майнової та/або моральної шкоди, зокрема внаслідок недотримання вимог санітарних, протипожежних та/або будівельних норм і правил, законодавства щодо кібербезпеки, захисту персональних даних, безпечності та якості харчових продуктів та/або надання неякісних послуг з харчування, шляхом фізичного та/або психологічного насильства, експлуатації, дискримінації за будь-якою ознакою, приниження честі, гідності, ділової репутації (зокрема шляхом булінгу (цькування), поширення неправдивих відомостей тощо), пропаганди та/або агітації, у тому числі з використанням кіберпростору, а також унеможливають вживання на території та в приміщеннях закладу освіти алкогольних напоїв, тютюнових виробів, наркотичних засобів, психотропних речовин. В умовах цифрової трансформації освіти це поняття включає не лише фізичну безпеку, а й захист учасників освітнього процесу в кіберпросторі.

Мережа Інтернет забезпечує широкі можливості для комунікації, доступу до інформаційних ресурсів та використання розважального контенту. Водночас у відкритому доступі наявні, інформаційні ресурси, що містять матеріали сексуального або еротичного характеру, сцени жорстокості та насильства, а також інший контент, який може негативно впливати на психологічний стан користувачів і становити загрозу їхній безпеці, зокрема безпеці дітей.

Згідно пункту 4 частини першої статті 5 Закону України «Про медіа», одним із завдань державної політики у сфері медіа є захист користувачів, особливо дітей, від шкідливого впливу інформації.

Серед способів убезпечення від небажаного контенту одним з основних є блокування. Цей механізм дозволяє заблокувати доступ до певних вебсайтів або категорій вмісту. Наприклад, можна встановити блокування для певних категорій вмісту, які вважаються небажаними, або для конкретних вебсайтів, які містять шкідливий матеріал.

3. Для забезпечення інформаційної безпеки дітей дошкільного віку та учнів рекомендується блокування доступу до небажаного контенту, до якого відносять такі категорії вебресурсів:

3.1. Нелегальний та небезпечний контент:

матеріали, що містять сцени насильства над дітьми (Child Abuse Content); пропаганда тероризму та екстремізму (Terrorism and Violent Extremism); сайти, що пропагують розпалювання ворожнечі (Hate Speech); інформація про нелегальні наркотики та зброю (Illegal Drugs, Weapons);

3.2. Контент для дорослих:

інформація сексуального чи еротичного характеру (Pornography, Adult); азартні ігри та лотереї (Gambling, Lotteries); пропаганда вживання алкоголю та тютюну (Alcohol, Tobacco).

3.2. Загрози цифровій безпеці;

шкідливе програмне забезпечення, фішинг, хакерські ресурси (Hacking, Malicious Software, Phishing);

інструменти для обходу фільтрації (Filter Avoidance, DNS-Tunneling).

3.4 Ресурси, що базуються на використанні технологій штучного інтелекту: сервіси для створення дипфейків (Deepfakes);

інструменти генерації неетичного контенту, що може бути використаний для кібербулінгу або дезінформації.

4. З метою забезпечення обмеження доступу (блокування) до інформаційних ресурсів можуть використовуватись списки блокування, ключові слова та додаткові критерії фільтрації. Списки блокування містять перелік вебсайтів або категорій вмісту, які потрібно блокувати. Ключові слова використовуються для виявлення та блокування вмісту, який містить такі ключові слова. Критерії фільтрації дозволяють встановлювати параметри фільтрації, зокрема вікові обмеження, тип вмісту тощо (ДСТУ ISO/IEC 27002:2023 «Інформаційні технології. Заходи безпеки інформації»).

5. Фільтрація контенту — це процес відсіювання небажаного матеріалу за допомогою спеціальних програмних засобів. Правильно налаштована фільтрація дозволяє забезпечити безпеку користувачів та обмежити доступ до небажаного контенту.

Фільтрація контенту в інтернеті може бути здійснена за допомогою різних методів, включаючи блокування певних сайтів, ключових слів або категорій вмісту. Встановлення фільтрів допомагає забезпечити безпеку користувачів, особливо дітей, від небажаних матеріалів.

6. Фільтрація контенту може бути реалізована на різних рівнях: на рівні мережі, на рівні комп'ютера або на рівні програми.

Рекомендується застосовувати багаторівневу систему захисту, враховуючи наявний досвід адміністраторів та технічні можливості.

6. 1. На рівні постачальника електронних комунікаційних послуг, що надає послуги доступу до мережі Інтернет.

За допомогою фільтрації контенту можна заблокувати доступ до небажаного матеріалу на рівні мережі. Це означає, що навіть якщо користувач намагається зайти на сайт з небажаним вмістом, його запит буде заблоковано і він не зможе переглянути цей матеріал. На рівні мережі фільтрація здійснюється постачальником електронних комунікаційних, послуг, який блокує доступ до певних сайтів або типів контенту.

Закладам освіти рекомендується звертатися до постачальників електронних комунікаційних послуг із запитом на активацію послуг централізованої фільтрації контенту («Чистий Інтернет»), що дозволяє блокувати шкідливі ресурси ще до потрапляння трафіку в мережу закладу.

6. 2. Нарівні мережевого обладнання (роутера).

Налаштування DNS-серверів із функцією батьківського контролю та фільтрації шкідливого контенту (наприклад, використання сімейних DNS від Cisco OpenDNS, Cloudflare Family, Cisco Umbrella, CleanBrowsing, AdGuard DNS тощо). Це безкоштовне та ефективне рішення для базового захисту всієї локальної мережі.

6.2.1, DNS-фільтрація на рівні шлюзу.

Найефективніший спосіб базової фільтрації — використання спеціалізованих DNS-серверів, які блокують розпізнавання імен шкідливих доменів.

Фільтрування DNS (або блокування системи доменних імен) забезпечує додатковий онлайн-захист, блокуючи доступ до небезпечних вебсайтів. Коли користувач намагається відвідати вебсайт, його пристрій просить DNS-сервер перетворити доменне ім'я вебсайту на IP-адресу. Під час цього процесу служба фільтрування контенту на основі DNS перевіряє запит за списком доменів, щоб дізнатися, чи дозволено користувачу під'єднуватися до них, тобто, чи є певне доменне ім'я у списку небезпечних вебсайтів, і, якщо це так, відображає попередження.

З метою забезпечення безперервної та коректної роботи DNS -фільтрації рекомендується періодично, але не рідше ніж один раз на 3-6 місяців перевіряти актуальність IP-адрес DNS-серверів на офіційних ресурсах відповідних постачальників, використовувати офіційну документацію вендорів як першоджерело інформації, а також визначити відповідальну особу, яка буде здійснювати контроль та актуалізацію налаштувань DNS-фільтрації в закладі освіти

6.2.1.1. Налаштування DHCP.

У налаштуваннях DHCP-сервера (на роутері Mikrotik, Ubiquiti, Cisco

тощо) вказати як Primary та Secondary DNS адреси провайдерів із сімейним фільтром.

6.2.1.2. Запобігання обходу (DNS Hijacking/Redirection).

Користувачі можуть вручну змінити DNS на своїх пристроях (наприклад, на 8.8.8.8) для обходу фільтра. Для цього необхідно створити правило NAT/Firewall, яке перехоплює весь трафік на порт 53 (UDP/TCP) від клієнтів і примусово перенаправляє його на обраній вами фільтруючий DNS-сервер.

6.2.2. Сегментація мережі (VLAN та Wi-Fi).

В рамках сегментації мережі необхідно впровадити модель «Нульової довіри» (Zero Trust), відмовитися від концепції безпечної внутрішньої мережі та забезпечити мікросегментацію (ізоляцію пристроїв) не лише для Wi-Fi, а й для дротових підключень у комп'ютерних класах для запобігання горизонтальному переміщенню (Lateral Movement) загроз.

6.2.3. Примусовий безпечний пошук (Force SafeSearch).

Більшість пошукових систем (google, bing, youtube) підтримують режим «SafeSearch», який приховує відвертий контент.

Налаштуйте локальний DNS -сервер (наприклад, якщо використовується Windows Server DNS або BIND/Unbound на роутері) так, щоб запити до www.google.com отримували дозвіл як forcesafesearch.google.com. Це автоматично активує безпечний пошук для всіх пристроїв у мережі, і користувач не зможе його вимкнути.

Для youtube необхідно налаштувати перенаправлення www.youtube.com -> restrict.youtube.com (суворий режим) або restrictmoderate.youtube.com.

6.2.4. Протидія методам обходу фільтрації.

Учні часто використовують VPN-сервіси, проксі-сервери або TOR для доступу до забороненого контенту.

6.2.4.1. Блокування VPN-протоколів.

Для блокування VPN-протоколів передбачити використання технологій DPI (Deep Packet Inspection) на мережевому обладнанні, яке підтримує цю функцію, для виявлення VPN/тунелювання за характерними ознаками трафіку, а не лише за портами та L4-правилами,

6.2.4.2. Блокування DoH (DNS over HTTPS).

Сучасні браузерери використовують шифрований DNS, який обходить фільтри. Необхідно заблокувати доступ до IP-адрес відомих DoH-резолверів або використовувати групові політики (GPO) для відключення DoH у браузерах Chrome / Edge на шкільних комп'ютерах.

Крім блокування DoH передбачити блокування протоколу QUIC (UDP 443), оскільки деякі сучасні браузерери використовують його для обходу традиційних методів інспекції трафіку, та ECH (Encrypted Client Hellos), що заважає фільтрації на рівні доменних імен.

6.2.4.3. Блокування розширень браузера.

Використовуйте GPO (Group Policy Object) для заборони встановлення VPN-розширень у браузерах на шкільних ПК.

6.3. На рівні кінцевого пристрою (комп'ютера / планшета).

На рівні комп'ютера фільтрація може бути налаштована користувачем або адміністратором системи, що дозволяє обмежити доступ до небажаного контенту на окремих пристроях. Наприклад налаштування безпечного пошуку у браузерях.

Обмеження доступу через браузери Google Chrome, Edge, Safari тощо.

6.3.1. Налаштування фільтрації сайтів у браузері Google Chrome.

Відкрийте <chrome://settings/security> у браузері.

У розділі «Безпека» виберіть «Покращений захист».

Увімкніть Google SafeSearch, щоб блокувати небажаний контент у пошуку.

Встановіть розширення «BlockSite» або «StayFocusd», щоб заблокувати конкретні сайти.

Детальна інформація доступна за посиланнями:

для Google Chrome

<https://support.google.com/chrome/answer/114662?hl=uk&co=GENIE.Platform%3DDesktop>

для Edge

<https://support.microsoft.com/uk-ua/microsoft-edge/%D0%B7%D0%BC%D1%96%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F-%D0%B4%D0%BE%D0%B7%D0%B2%D0%BE%D0%BB%D1%96%D0%B2-%D0%BD%D0%B0%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF-%D0%B4%D0%BE%D0%B2%D0%B5%D0%B1-%D1%81%D0%B0%D0%B9%D1%82%D1%96%D0%B2-%D0%B4%D0%BB%D1%8F-%D1%80%D0%BE%D0%B7%D1%88%D0%B8%D1%80%D0%B5%D0%BD%D1%8C-%D1%83-microsoft-edge-7d1c889d-e267-4be0-15d4-3ed5d0c82ef5>

для Safari

<https://support.apple.com/uk-ua/guide/personal-safety/ips375e6d608/web>

6.3.2 Використання батьківського контролю на пристроях.

Ефективним способом забезпечити безпеку в інтернеті є використання батьківського контролю на пристроях. Цей інструмент дозволяє батькам блокувати або обмежувати доступ до небажаного контенту для своїх дітей. Його також можна використовувати для убезпечення роботи в закладах освіти.

Одним з аспектів його використання є можливість індивідуального налаштування: можна встановлювати обмеження залежно від віку або інтересів дітей. Наприклад, дітям до певного віку може бути заборонено переглядати фільми або грати в ігри з високим рівнем насильства.

Застосування батьківського контролю на пристроях є ефективнішим способом забезпечення безпеки дітей в інтернеті. Він дозволяє батькам мати контроль над доступом до небажаного матеріалу і забезпечує спокій та безпеку для всієї родини.

6.3.2.1. Батьківський контроль у Windows.

ОС Windows має вбудовані засоби батьківського контролю, які дозволяють встановлювати обмеження на час використання комп'ютера, блокувати сайти та переглядати активність дитини.

Створіть обліковий запис дитини.

Відкрийте «Параметри» —> «Облікові записи» —> «Сім'я та інші користувачі».

Натисніть «Додати члена сім'ї» та виберіть «Дитина».

Введіть email дитини (якщо його немає, створіть новий обліковий запис Microsoft).

Налаштуйте контроль через Microsoft Family Safety. Перейдіть на сайт family.microsoft.com та увійдіть під своїм обліковим записом.

Виберіть профіль дитини та встановіть обмеження: ліміти використання (задайте максимальний час використання комп'ютера); фільтрація контенту (блокуйте сайти з небажаним контентом); контроль покупок (забороніть витрати без дозволу).

Увімкніть «Безпечний пошук» у браузері «Microsoft Edge», щоб дитина не натрапила на небажаний контент.

Детальна інформація доступна за посиланням

<https://support.microsoft.com/uk-ua/account-billing/%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-microsoft-family-safety-b6280c9d-38d7-82ff-0e4f-a6cb7e659344>

6.3.2.2. Батьківський контроль у macOS.

MacBook та iMac мають функцію «Екранний час», яка дозволяє обмежувати доступ до програм, контролювати використання комп'ютера та блокувати небезпечні сайти.

Відкрийте «Системні параметри» —> «Екранний час».

Натисніть «Увімкнути екранний час для сім'ї».

Виберіть профіль дитини та встановіть обмеження: обмеження за часом (вказіть, скільки годин на день можна користуватися комп'ютером); контроль додатків (забороніть використання певних програм (наприклад, youtube або ігор); фільтрація контенту (блокуйте доступ до сайтів для дорослих тощо).

Встановіть пароль для змін налаштувань, щоб дитина не могла їх самостійно змінити.

Детальна інформація доступна за посиланням

<https://support.apple.com/uk-ua/guide/mac-help/mchlcdcc9382/mac>

6.3.2.3. Батьківський контроль у ChromeOS.

Відкрийте додаток Family Link.

Виберіть профіль дитини.

Натисніть «Контроль» —> «Google Chrome і Інтернет» —> «Розширені налаштування».

Увімкніть або вимкніть опцію «Дозволи для сайтів, розширень і даних сайтів на пристрої».

Також можна змінити це налаштування, вибравши профіль дитини на інформаційній панелі в браузері Chrome.

Детальна інформація доступна за посиланням <https://support.google.com/chromebook/answer/7680868?hl=uk>

6.4. На рівні програми фільтрація здійснюється за допомогою спеціальних програм або додатків, які відсіюють небажаний контент на певних вебсайтах або в програмах. Таке програмне забезпечення автоматично перевіряє вебсторінки на наявність небажаного вмісту. Ці програми використовують різні алгоритми та бази даних, щоб визначити, чи є вміст небажаним.

6.4.1. Використання антивірусного програмного забезпечення є важливим елементом безпеки в мережі. В закладах освіти його необхідно встановити на всіх пристроях.

Одним з основних завдань антивірусних програм є фільтрація вмісту, що надходить з інтернету: програма здатна виявляти небажаний контент і обмежувати його доступ для користувача. Блокування небажаного вмісту допомагає забезпечити безпеку користувача та запобігти можливим загрозам, які можуть призвести до компрометації даних чи інших проблем.

Антивірусне програмне забезпечення може мати різні функції фільтрації контенту, які дозволяють користувачу налаштувати рівень обмежень в залежності від його потреб і вимог безпеки. Наприклад, ви можете встановити блокування певних категорій вебсайтів або використовувати рейтингову систему, яка визначає рівень небезпеки для кожного вебресурсу.

Антивірусне програмне забезпечення також забезпечує захист від шкідливих програм та вірусів, які можуть пошкодити комп'ютер або викрасти важливу інформацію. Воно перевіряє вміст, що завантажується з інтернету, і блокує потенційно небезпечні файли або повідомлення, що містять шкідливий код.

6.4.2. Для забезпечення надійного захисту необхідно також регулярно перевіряти наявність оновлень для операційної системи та програм, що використовуються. Оновлення виробників зазвичай містять виправлення вразливостей та додаткові заходи безпеки, що дозволяють уникнути можливих загроз та атак з боку зловмисників. (ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт»).

Оновлення операційної системи та програм можна перевірити за допомогою спеціальних інструментів або вбудованих функцій. Більшість операційних систем автоматично перевіряють наявність оновлень та надають можливість встановити їх автоматично. Важливо включити цю функцію та періодично перевіряти, чи не з'явилися нові оновлення.

Також слід пам'ятати, що багато програм, особливо ті, що мають доступ до мережі, також мають функцію автоматичної перевірки оновлень.

Рекомендується налаштувати цю функцію та періодично перевіряти, чи не з'явилися нові версії програми з виправленням безпекових проблем.

Таким чином регулярно оновлення дозволить уникнути можливих загроз та забезпечить надійний захист від небажаного матеріалу та потенційних атак з боку зловмисників.

7. Безпека паролів.

Складність паролів: необхідно використовувати унікальні паролі довжиною не менше 8-12 символів (літери різних регістрів, цифри, спеціальні символи).

Регулярна ротація: зміна паролів кожні 3 місяці.

Багатофакторна аутентифікація (MFA): обов'язкова активація 2FA для корпоративної пошти, електронних журналів та соціальних мереж.

Менеджери паролів: використання спеціалізованого програмного забезпечення (наприклад, KeePassXC, Bitwarden) замість збереження паролів у браузері чи нотатках.

8. Рекомендовані ресурси.

буклет “Приватність дитини в інтернеті”

<https://dignityonline.in.ua/adult/posibnyky/buklet-pryvatnist-dytyny-v-interneti/>

вебпортал «Кібер Брама. Кібербезпека в освіті»

<https://stopfraud.gov.ua/cybersecurity-in-education>

гайд «Гаджет дитини. Загальні рекомендації використання, налаштування та контроль»

<https://dignityonline.in.ua/adult/hayd-dlia-batkiv-batkivski-kontroli/>

гайд «Кібергігієна для дітей: правила поведінки в інтернеті»

<https://osvita.diia.gov.ua/guides/cyber-hygiene-for-children>

гайд «Онлайн-безпека для дітей»

<https://osvita.diia.gov.ua/guides/gajd-dla-ditej-moa-onlajn-bezpeka>

гайд «Кібергігієна під час війни»

<https://osvita.diia.gov.ua/guides/kibergigiena-pid-cas-vijni>

гайд «Сексуальне насильство в інтернеті: що це і як запобігти»

<https://osvita.diia.gov.ua/guides/sexual-violence-on-the-internet-what-it-is-and-how-to-prevent-it>

довідник “Рекомендації щодо онлайн-безпеки для педагогічних працівників” <https://dignityonline.in.ua/adult/posibnyky/dovidnyk-rekomendatsii-shchodo-onlayn-bezpeky-dlia-pedahohichnykh-pratsivnykiv/>

довідник для батьків та вихователів «Створюємо онлайн-простір разом з дітьми»

<https://dignityonline.in.ua/adult/posibnyky/stvoriuiemo-onlayn-prostir-razom-z-ditmy-dovidnyk-dlia-batkiv-ta-vykhovateliv/>

інформаційна довідка для вчителів з кібергігієни, розроблена ІТ-Асоціацією України

<https://drive.google.com/file/d/11f95cwhNS11L28XU-g48UzVWYV2RuIsB/view>

інформаційна довідка для учнів з кібергігієни, розроблена ІТ-Асоціацією України

<https://drive.google.com/file/d/10N5JbD680yfS5qt22AvIGnAG3BPsmDyd/view>

освітній проєкт Common Sense Media:

<https://www.common sense.org/>

освітній серіал «ДезінФАКЕція»

<https://osvita.diia.gov.ua/courses/disinfakation>

освітній серіал «Кібергігієна: як захиститись від фішингу»

<https://osvita.diia.gov.ua/courses/kibergigiena-ak-zahistitisa-vid-fisingu>

освітній серіал «Особиста безпека підлітків»

<https://osvita.diia.gov.ua/courses/teenagers-personal-safety>

освітній серіал «Безпека дітей в інтернеті для батьків»

<https://osvita.diia.gov.ua/courses/serial-dlya-batkiv-onlayn-bezpeka-ditey>

освітній серіал «Про кібербулінг для підлітків»

<https://osvita.diia.gov.ua/courses/cyberbullying>

пам'ятка «Шкідливий контент: як батькам протидіяти його впливу на дитину?»» https://stop-sexting.in.ua/wp-content/uploads/2021/06/stop_sexting_buklet_dlya_batkiv.pdf

посібник із безпеки дітей в Інтернеті

https://services.google.com/fh/files/events/bia_curriculum_2023.pdf

посібник з онлайн-безпеки дітей для шкільних психологів

<https://dignityonline.in.ua/adult/posibnyky/posibnyk-z-onlayn-bezpeky-ditey-dlia-shkilnykh-psykholohiv/>

посібник «Кібербезпека для шкіл» Національного центру кібербезпеки Сполученого Королівства Великої Британії та Північної Ірландії (NCSC).

https://www.ncsc.gov.ie/pdfs/NCSC_Quick_Guide_Schools.pdf

сайт Агенства з кібербезпеки та безпеки інфраструктури (CISA) США

<https://www.cisa.gov/topics/cybersecurity-best-practices/K12cybersecurity/protecting-our-future-cybersecurity-k12>

симулятор «Онлайн-безпека для дітей»

<https://osvita.diia.gov.ua/simulators/e-safety-children-simulator>

симулятор «Онлайн-безпека для підлітків»

<https://osvita.diia.gov.ua/simulators/e-safety-teens-simulator>

симулятор «Онлайн-безпека для освітян»

<https://osvita.diia.gov.ua/simulators/onlajn-bezpeka-dla-osvitan>

симулятор «Кібергігієна: як захиститись від фішингу»

<https://osvita.diia.gov.ua/simulators/cyber-hygiene-how-to-protect-yourself-from-phishing>

Генеральний директор
директорату цифрової трансформації



Роксолана ШВАДЧАК