Посібник для школи

Актуально на 01.11.2026

Як працювати з SafeGate і як виконати заходи Наказу МОН №103, яких програма не робить сама: налаштування роутера, звернення до постачальника інтернету, антивірус і паролі. Розділи — для керівника й відповідальної особи, педагогів, батьків і учнів.

Зміст

1. Для керівника й відповідальної особи
   - Робота в панелі SafeGate
   - Регулярний перегляд налаштувань
   - Нові користувачі Ubuntu і Debian
   - Налаштування роутера закладу
   - Звернення до постачальника інтернету
   - Окрема мережа для комп’ютерного класу й гостей
   - Антивірус і оновлення
   - Паролі й двоетапна перевірка
2. Для педагогів
3. Для батьків
4. Для учнів: пам’ятка для комп’ютерного класу

Для керівника й відповідальної особи

Що робить адміністратор школи в панелі SafeGate і які заходи Наказу №103 заклад виконує поза програмою.

Робота в панелі SafeGate

Панель вашої школи відкривається кнопкою «Увійти» на сайті SafeGate. Обліковий запис адміністратора школи створює SUITT і надсилає запрошення на вашу пошту.

1. **Увійдіть і захистіть обліковий запис**

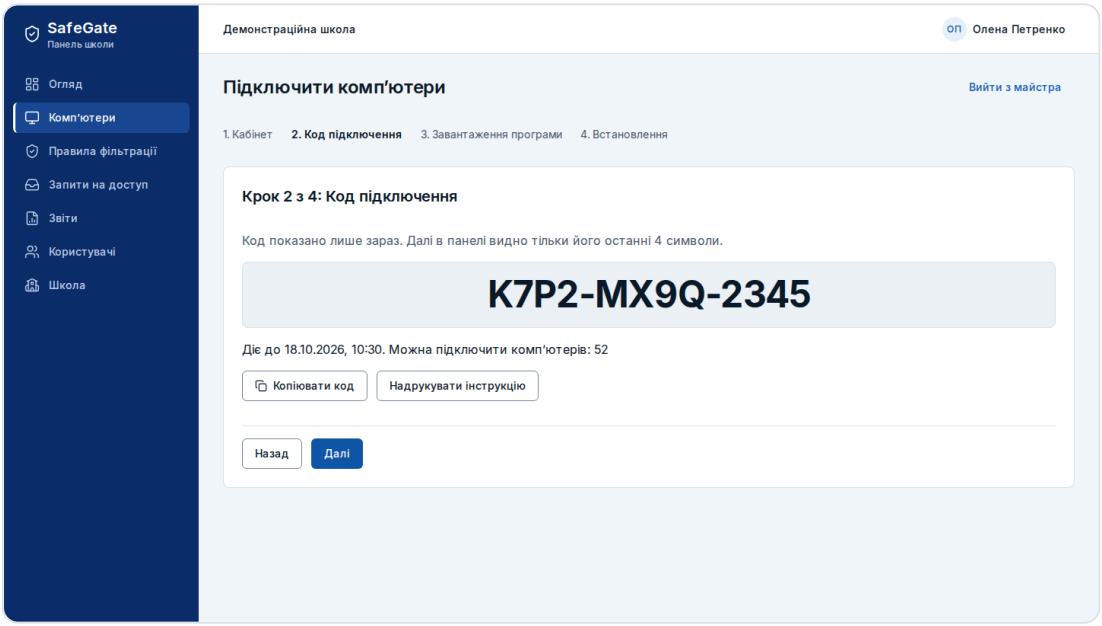
   Відкрийте лист-запрошення, задайте пароль і налаштуйте двоетапну перевірку в застосунку-автентифікаторі на телефоні. Для адміністратора школи двоетапна перевірка обов'язкова.

2. **Заповніть відомості про школу**

   На сторінці «Школа» вкажіть особу, відповідальну за фільтрацію, і керівника закладу. Ці відомості потрапляють у звіт для перевірки.

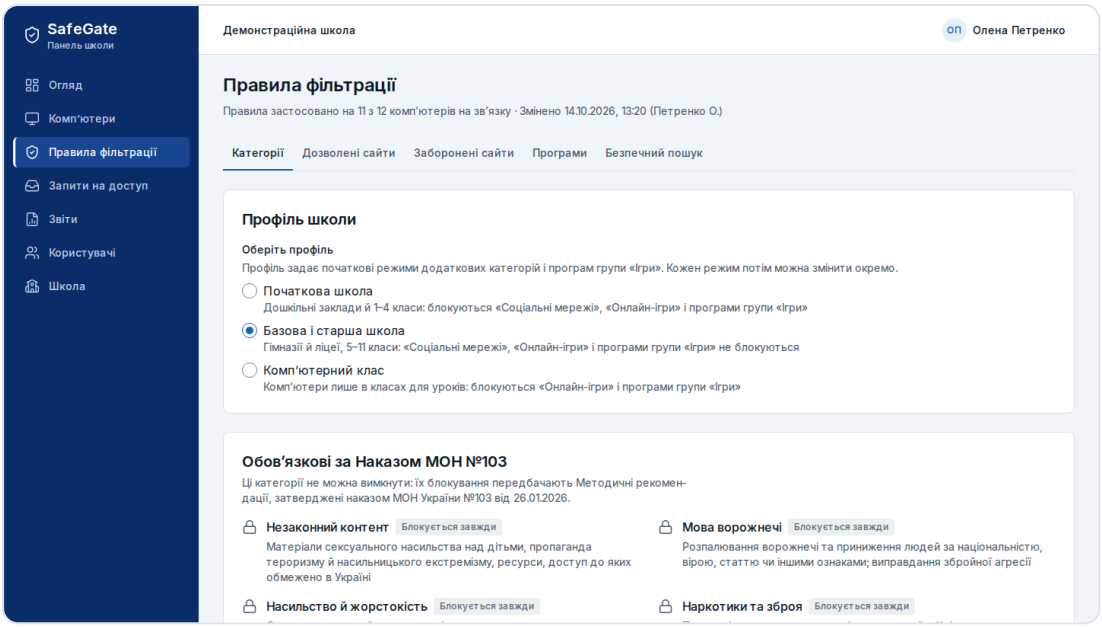
3. **Підключіть комп'ютери**

   На сторінці «Комп'ютери» відкрийте майстер «Підключити комп'ютери». Він має 4 кроки: кабінет, код підключення, завантаження програми SafeGate і встановлення на кожному комп'ютері кабінету. Код показано лише один раз, тож збережіть або надрукуйте його.



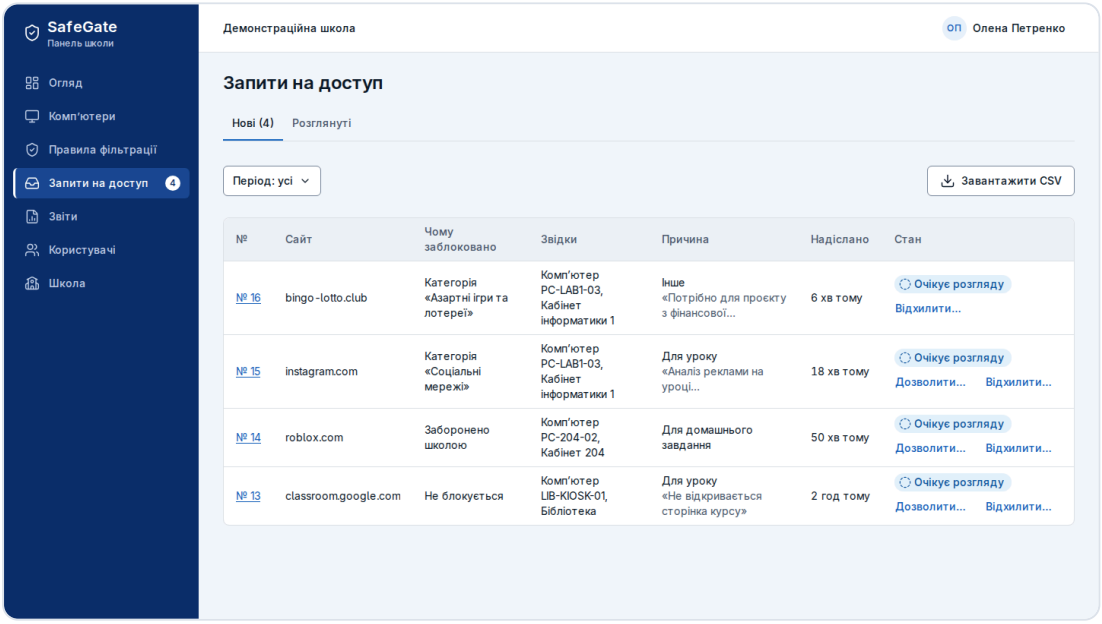
4. **Перевірте правила фільтрації**

   На сторінці «Правила фільтрації» оберіть профіль школи: «Початкова школа», «Базова і старша школа» чи «Комп'ютерний клас». Обов'язкові категорії Наказу блокуються завжди, для додаткових оберіть «Блокувати» чи «Не блокувати». Там само — дозволені й заборонені сайти школи, заборонені програми й безпечний пошук.



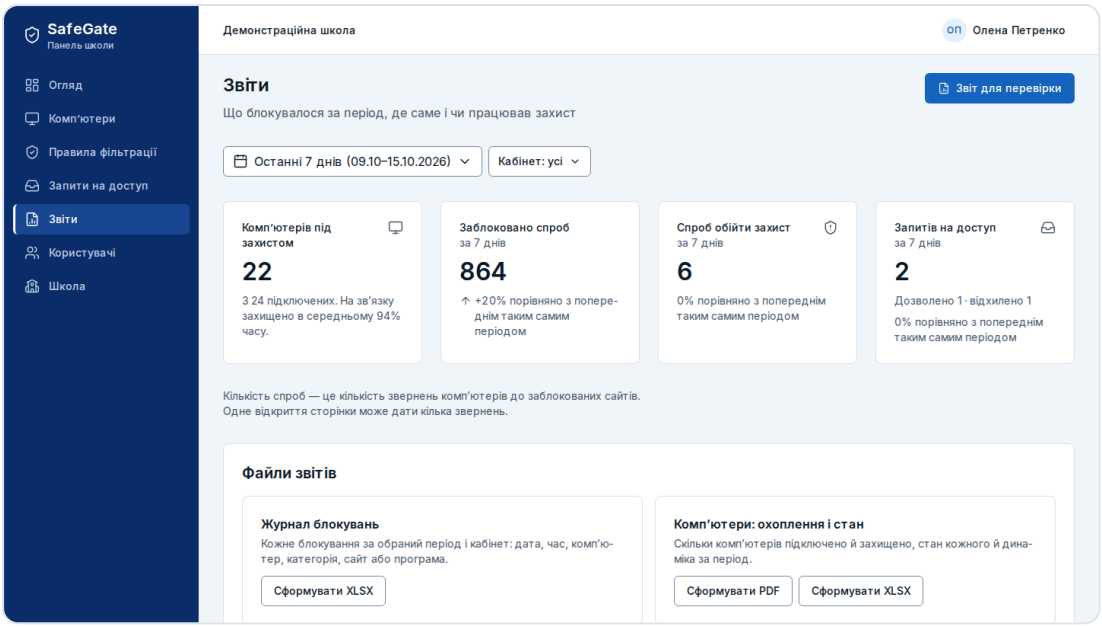
5 Розглядайте запити на доступ

Якщо на шкільному комп'ютері заблоковано сайт, потрібний для уроку, учень чи вчитель натискає «Попросити доступ». Запит з'являється на сторінці «Запити на доступ», а адміністратор школи отримує лист. Натисніть «Дозволити…» і оберіть, де діятиме дозвіл (лише на цьому комп'ютері чи на всіх комп'ютерах школи) і на який строк. Комп'ютери отримають зміну протягом 2 хвилин. Сайти обов'язкових категорій дозволити не можна.



6 Формуйте звіти

На сторінці «Звіти» є три звіти за обраний період. «Звіт для перевірки» містить усе, що потрібно перевіряльнику за Наказом №103. Також є «Журнал блокувань» і «Комп'ютери: охоплення і стан».



7 **Запросіть учителів**

На сторінці «Користувачі» запросіть учителів електронною поштою. Учитель бачить стан комп’ютерів своїх кабінетів, недавні блокування й запити на доступ, але не змінює правил.

8 **Дайте посилання батькам**

На сторінці «Школа» створіть «Посилання для батьків». За ним батьки бачать статистику захисту школи й правила фільтрації без даних про окремих дітей. Посилання можна відкликати й створити нове.

Регулярний перегляд налаштувань

Наказ №103 радить перевіряти налаштування фільтрації не рідше ніж раз на 3–6 місяців. SafeGate нагадує про перегляд раз на 3 місяці: на 90-й день адміністратор школи отримує лист, а на сторінці «Огляд» з’являється нагадування.

На сторінці «Школа» в блоці «Перегляд налаштувань» натисніть «Провести перегляд», перевірте й позначте кожен пункт і натисніть «Перегляд проведено». Дата перегляду потрапляє у звіт для перевірки, а відлік 3 місяців починається знову.

Пункти перегляду

- профіль школи й режими додаткових категорій актуальні;
- дозволи, які вже не потрібні, прибрано;
- комп’ютери, що потребують уваги, розглянуто;
- стан мережевого рівня підтверджено: роутер підключено до фільтра SafeGate або він досі роздає адреси сімейної служби перевірки сайтів;
- контакти відповідальної особи актуальні.

Нові користувачі Ubuntu і Debian

На Ubuntu і Debian фільтрація діє для всього комп’ютера, хоч би хто ним користувався.

Значок і вікно програми SafeGate бачать користувачі її групи. Пакет додає до групи користувачів, які вже є на комп'ютері. Користувача, створеного після встановлення, додайте командою від імені адміністратора комп'ютера, замінивши «користувач» на його ім'я входу:

```
sudo adduser користувач safegate
```

Зміна діє після наступного входу цього користувача в систему.

Налаштування роутера закладу

Телефони, планшети й комп'ютери без програми SafeGate у мережі школи захищає роутер закладу. Так радить п. 6.2 Наказу №103. Роутер можна підключити до фільтра SafeGate або налаштувати на сімейну службу перевірки сайтів.

Під час встановлення SafeGate інженер SUIT T налаштовує або перевіряє роутер разом зі школою, а результат позначає в панелі: «Перевірено інженером SUIT T».

Підключення роутера до фільтра SafeGate

Рекомендований спосіб. Роутер надсилає запити з мережі закладу до фільтра SafeGate, а той перевіряє сайти за категоріями й заборонами школи, як програма на комп'ютерах.

У панелі на сторінці «Школа» в блоці «Мережа закладу» натисніть «Підключити роутер» і оберіть спосіб підключення. Панель покаже дані для підключення й готові команди для поширених роутерів.

Найпростіше підключити роутер ключем: роутер надсилає шифровані запити, тож адреса закладу може бути будь-якою. Роутер без шифрованих запитів підключають за постійною публічною адресою закладу або динамічним ім'ям роутера.

Сайт, який дозволила школа, у мережі закладу може лишатися заблокованим сімейною службою. Винятки повністю діють на комп'ютерах із програмою SafeGate.

Налаштування на сімейну службу перевірки сайтів

Якщо роутер не можна підключити до фільтра SafeGate, налаштуйте його на сімейну службу перевірки сайтів, яку названо нижче. Вона блокує сайти для дорослих і шкідливі сайти, але правил школи не знає.

DNS — служба, яка перетворює назву сайту на його адресу. Сімейна служба DNS не повертає адрес сайтів для дорослих і шкідливих сайтів, тож вони не відкриваються.

Сімейна служба перевірки сайтів

Вкажіть обидві адреси служби: основну й резервну.

Cloudflare for Families

Названа в п. 6.2 Наказу МОН № 103

Адреси IPv4	`1.1.1.3` `1.0.0.3`
Адреси IPv6	`2606:4700:4700::1113` `2606:4700:4700::1003`

Що налаштувати

1. DHCP: роздавайте основну й резервну адреси обраної служби як DNS-сервери для IPv4 і IPv6.
2. Перехоплення: правило NAT спрямовує всі запити на порт 53 (UDP і TCP) до обраної служби, навіть якщо на телефоні вручну вказано інший DNS-сервер (п. 6.2.1.2 Наказу).
3. Зашифрований DNS: заблокуйте з'єднання на порт 853 (TCP і UDP).
4. QUIC: заблокуйте UDP на порт 443. Браузери й програми перейдуть на звичайні з'єднання TCP.
5. DNS через HTTPS: заблокуйте з'єднання на порт 443 до відомих публічних служб DNS. Їхні адреси — у командах для MikroTik нижче. Перелік охоплює найпоширеніші служби, але не всі, що існують.

Не блокуйте адрес, через які програма SafeGate на шкільних комп'ютерах відкриває сайти, дозволені школою:

```
1.1.1.2
1.0.0.2
9.9.9.9
149.112.112.112
2606:4700:4700::1112
2606:4700:4700::1002
2620:fe::fe
2620:fe::9
```

MikroTik (RouterOS 7)

Команди розраховано на стандартну конфігурацію, у якій мережа школи входить до списку інтерфейсів LAN. Відкрийте термінал (у WinBox — New Terminal) і вставте блоки по черзі. Команди налаштовують Cloudflare for Families.

1. Списки адрес: сімейні служби і відомі публічні служби DNS.

```
/ip firewall address-list
add list=sg-family address=1.1.1.3
add list=sg-family address=1.0.0.3
add list=sg-doh address=8.8.8.8
add list=sg-doh address=8.8.4.4
add list=sg-doh address=1.1.1.1
add list=sg-doh address=1.0.0.1
add list=sg-doh address=9.9.9.10
add list=sg-doh address=149.112.112.10
add list=sg-doh address=208.67.222.222
add list=sg-doh address=208.67.220.220
add list=sg-doh address=94.140.14.14
add list=sg-doh address=94.140.15.15
/ipv6 firewall address-list
add list=sg-family address=2606:4700:4700::1113
add list=sg-family address=2606:4700:4700::1003
add list=sg-doh address=2001:4860:4860::8888
add list=sg-doh address=2001:4860:4860::8844
add list=sg-doh address=2606:4700:4700::1111
add list=sg-doh address=2606:4700:4700::1001
add list=sg-doh address=2620:fe::10
add list=sg-doh address=2620:fe::fe:10
add list=sg-doh address=2620:119:35::35
add list=sg-doh address=2620:119:53::53
add list=sg-doh address=2a10:50c0::ad1:ff
add list=sg-doh address=2a10:50c0::ad2:ff
```

2. DNS для DHCP і для оголошень IPv6.

```
/ip dhcp-server network
set [find] dns-server=1.1.1.3,1.0.0.3
/ip dhcp-client
set [find] use-peer-dns=no
/ip dns
set servers=1.1.1.3,1.0.0.3,2606:4700:4700::1113,2606:4700:4700::1003
/ipv6 nd
set [find] advertise-dns=yes
```

3. Перехоплення запитів на порт 53 до інших DNS-серверів.

```
/ip firewall nat
add chain=dstnat in-interface-list=LAN protocol=udp dst-port=53 dst-address-l
ist=!sg-family action=dst-nat to-addresses=1.1.1.3 comment="SafeGate: DNS"
add chain=dstnat in-interface-list=LAN protocol=tcp dst-port=53 dst-address-l
ist=!sg-family action=dst-nat to-addresses=1.1.1.3 comment="SafeGate: DNS"
```

4. Блокування зашифрованого DNS, QUIC і DNS через HTTPS.

```
/ip firewall filter
add chain=forward in-interface-list=LAN protocol=tcp dst-port=853 action=reje
ct reject-with=tcp-reset comment="SafeGate: DoT"
add chain=forward in-interface-list=LAN protocol=udp dst-port=853 action=drop
comment="SafeGate: DoQ"
add chain=forward in-interface-list=LAN protocol=udp dst-port=443 action=drop
comment="SafeGate: QUIC"
add chain=forward in-interface-list=LAN protocol=tcp dst-port=443 dst-address
-list=sg-doh action=reject reject-with=tcp-reset comment="SafeGate: DoH"
```

5. Те саме для IPv6: запити на порт 53 до інших DNS-серверів відкидаються.

```
/ipv6 firewall filter
add chain=forward in-interface-list=LAN protocol=udp dst-port=53 dst-address-
list=!sg-family action=drop comment="SafeGate: DNS"
add chain=forward in-interface-list=LAN protocol=tcp dst-port=53 dst-address-
list=!sg-family action=drop comment="SafeGate: DNS"
add chain=forward in-interface-list=LAN protocol=tcp dst-port=853 action=drop
comment="SafeGate: DoT"
add chain=forward in-interface-list=LAN protocol=udp dst-port=853 action=drop
comment="SafeGate: DoT"
add chain=forward in-interface-list=LAN protocol=udp dst-port=443 action=drop
comment="SafeGate: QUIC"
add chain=forward in-interface-list=LAN protocol=tcp dst-port=443 dst-address
-list=sg-doh action=drop comment="SafeGate: DoH"
```

Правила блокування мають стояти вище за правила, що дозволяють увесь вихідний трафік мережі. У стандартній конфігурації MikroTik таких правил немає.

Інші роутери

Назви пунктів меню залежать від моделі й версії роутера. Порядок той самий:

1. у налаштуваннях DHCP-сервера мережі школи вкажіть основну й резервну адреси обраної служби як DNS-сервери;
2. правилом NAT для вихідних з'єднань спрямуйте UDP і TCP на порт 53 до основної адреси служби;
3. правилами міжмережевого екрана заблокуйте порт 853, UDP на порт 443 і з'єднання на порт 443 до відомих публічних служб DNS;
4. якщо роутер не вміє перехоплювати й блокувати такі з'єднання, зверніться до SUIT T.

- Ubiquiti (UniFi, EdgeRouter): DNS для DHCP задається в налаштуваннях мережі, перехоплення порту 53 і блокування портів — правилами NAT і міжмережевого екрана.
- Cisco (IOS): DNS для DHCP задається в пулі DHCP-сервера, перехоплення порту 53 — правилом NAT, блокування портів — списками доступу на інтерфейсі мережі школи.
- TP-Link: DNS задається в налаштуваннях DHCP-сервера мережі школи. Якщо модель має правила контролю доступу, заблокуйте ними порти 53 і 853 до всіх адрес, крім обраної служби, і UDP на порт 443. Без таких правил роутер не завадить вручну змінити DNS на телефоні.
- Keenetic: DNS задається в налаштуваннях домашнього сегмента мережі, блокування портів — правилами міжмережевого екрана для цього сегмента.

Перевірка

Перевірте налаштування з телефона, підключеного до шкільного Wi-Fi, і з комп'ютера мережі школи:

1. на телефоні не відкривається тестова сторінка служби для дорослого контенту — для Cloudflare for Families це nudity.testcategory.com;
2. запит до стороннього DNS-сервера повертає ту саму відповідь блокування (на комп'ютері з Windows):

```
nslookup nudity.testcategory.com 8.8.8.8
```

3. з’єднання на порт 853 не встановлюється: команда показує TcpTestSucceeded зі значенням False

```
Test-NetConnection 1.1.1.1 -Port 853
```

Відмітка в панелі

Після налаштування відкрийте в панелі сторінку «Школа», блок «Рівні захисту за Наказом №103». Для пункту «Мережа закладу» вкажіть службу, хто налаштував роутер, і дату перевірки. Перевіряйте роутер під час кожного перегляду налаштувань.

Звернення до постачальника інтернету

П. 6.1 Наказу №103 радить звернутися до постачальника інтернету щодо послуги централізованої фільтрації («Чистий Інтернет»).

Запитайте постачальника письмово, чи надає він таку послугу. Відповідь або договір збережіть. У панелі на сторінці «Школа», блок «Рівні захисту за Наказом №103», вкажіть постачальника, дати звернення й підключення і додайте файл підтвердження.

Окрема мережа для комп’ютерного класу й гостей

П. 6.2.2 Наказу №103 радить розділити мережу закладу на частини:

- комп’ютери учнів — в окремій мережі, відокремленій від комп’ютерів адміністрації й бухгалтерії;
- гостьовий Wi-Fi — окремо від внутрішньої мережі й з ізоляцією клієнтів, щоб телефони й ноутбуки гостей не бачили одне одного;
- сімейна служба перевірки сайтів — для всіх частин мережі, зокрема гостьової.

Поділ мережі налаштовує фахівець, який обслуговує мережу закладу.

Антивірус і оновлення

SafeGate не замінює антивірус. За п. 6.4 Наказу №103 на всіх комп’ютерах закладу має працювати антивірус з актуальними базами, а система й програми мають регулярно оновлюватися. Не вимикайте автоматичних оновлень Windows, Ubuntu і Debian. Програма SafeGate оновлюється сама.

Паролі й двоетапна перевірка

П. 7 Наказу №103 радить унікальні паролі щонайменше з 8–12 символів різних груп і зміну паролів кожні 3 місяці. Двоетапна перевірка — для корпоративної пошти, електронних журналів і соціальних мереж, для зберігання паролів — менеджери паролів.

У панелі SafeGate двоетапна перевірка обов’язкова для адміністратора школи, а пароль має щонайменше 12 символів. Вчитель без двоетапної перевірки задає пароль щонайменше

з 15 символів.

Для педагогів

На шкільних комп'ютерах програма SafeGate блокує сайти 10 обов'язкових категорій Наказу №103 і додаткові категорії, які обрала школа. Вона також вмикає безпечний пошук Google і Bing та обмежений режим YouTube і не дає запускати відомі VPN, Tor і проксі.

Що бачить учень

Коли сайт заблоковано, у куті екрана з'являється сповіщення SafeGate з назвою сайту й причиною. Браузер при цьому може показати й власну помилку з'єднання: так він реагує на заблокований сайт.

Як попросити доступ до сайту для уроку

1. У сповіщенні SafeGate або на сторінці «Сайт заблоковано» натисніть «Попросити доступ».
2. Оберіть, для чого потрібен доступ: «Для уроку», «Для домашнього завдання» чи «Інше». Коментар необов'язковий; не пишіть у ньому прізвищ і телефонів.
3. Запит розгляне адміністратор школи. Відповідь з'явиться в SafeGate на цьому комп'ютері; дозволений сайт відкриється протягом 2 хвилин.

Для сайтів обов'язкових категорій кнопки «Попросити доступ» немає. Якщо такий сайт заблоковано помилково, повідомте адміністратора школи: він передасть звернення до SUIT T.

Якщо адміністратор школи запросив вас до панелі SafeGate, ви бачите стан комп'ютерів своїх кабінетів, недавні блокування й запити на доступ. Змінює правила лише адміністратор школи.

Посібники, курси й тренажери для педагогів, батьків і учнів перелічено в п. 8 Методичних рекомендацій, затверджених Наказом МОН №103.

Текст Наказу МОН №103 на сайті osvita.ua

Для батьків

SafeGate захищає шкільні комп’ютери, а якщо роутер закладу підключено до фільтра SafeGate, — і телефони й планшети в мережі школи. Що блокується в школі й скільки спроб заблоковано, видно на сторінці школи за посиланням для батьків, яке дає школа. Даних про окремих дітей там немає.

Батьківський контроль удома

Для домашніх комп’ютерів і телефонів п. 6.3.2 Наказу №103 радить вбудований батьківський контроль з обмеженнями за віком:

- Windows — Microsoft Family Safety («Сімейна безпека Microsoft»);
- iPhone, iPad і комп’ютери Apple — «Екранний час» у налаштуваннях;
- Android і Chromebook — Google Family Link.

Ці засоби батьки налаштовують самі, SafeGate з ними не пов’язаний. Пам’ятку для учнів нижче можна обговорити з дитиною й удома.

Рекомендовані ресурси для батьків — у п. 8 Методичних рекомендацій до Наказу МОН №103.

Текст Наказу МОН №103 на сайті osvita.ua

Для учнів: пам’ятка для комп’ютерного класу

Що блокується і чому

На шкільних комп’ютерах працює програма SafeGate. Вона блокує сайти, які можуть зашкодити: з насильством, для дорослих, з азартними іграми, наркотиками й зброєю, шахрайські сайти й засоби обходу фільтрації. Так школа дбає про безпечне освітнє середовище.

Якщо потрібний сайт заблоковано

Натисніть «Попросити доступ» у сповіщенні SafeGate й оберіть, для чого потрібен сайт. Запит розгляне адміністратор школи, відповідь з’явиться на цьому комп’ютері.

Не намагайтеся обійти фільтр: спроби обійти захист бачить адміністратор школи.

Правила безпечної поведінки

- Нікому не повідомляйте своїх паролів і не входьте в чужі облікові записи.
- Не завантажуйте й не запускайте невідомих програм і файлів.
- Не відкривайте посилань з підозрілих повідомлень і не вводьте там паролів.
- Не публікуйте своєї адреси, телефону й фото документів.
- Пишіть у листуванні й коментарях так, як сказали б особисто.
- Якщо щось у мережі налякало чи образило вас, скажіть учителю або батькам.
- Наприкінці уроку виходьте зі своїх облікових записів.