

ЦИФРОВАЯ БЕЗОПАСНОСТЬ



Цифровая безопасность

Оценка рисков

Защита акаунтов

Безопасная коммуникация

Защита устройств

Оценка рисков



Оценка рисков: рациональный подход к цифровой безопасности

Почему нельзя защищать все от всего

Компоненты оценки рисков

Перечень активов

Оценка угроз

Модель угроз

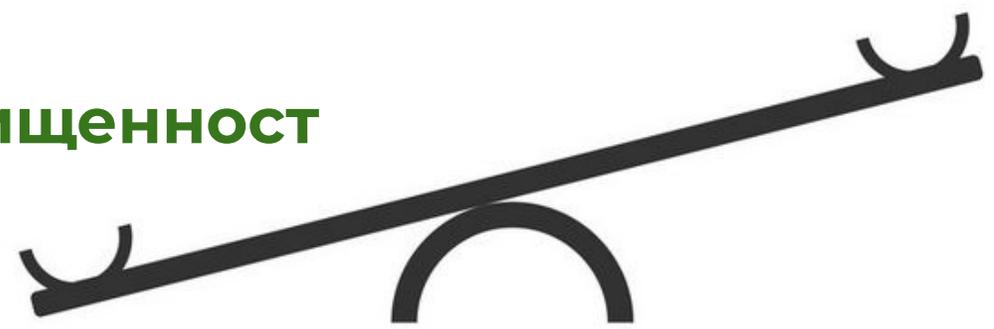
Матрица рисков

Как оценить вероятность

Что делать с рисками

Защищенност
ь

Удобство



Перечень активов: что у нас есть



Комп Windows



Телефон Android



Почта Gmail



Соцсеть Twitter



Мессенджер
Telegram

Оценка угроз: кто может сделать что-то плохое



Комп Windows



Телефон Android



Почта Gmail



Соцсеть Twitter



Мессенджер
Telegram

Кто может нам угрожать



Криминал



Госструктуры



Личные недоброжелатели



Онлайн-хулиганы



Мы сами/физическое старение



thaddeus e. grugq

@thegrugq



Your threat model is not my threat model.



10:42 AM · May 15, 2017 · Tweetbot for iOS

Оценка рисков: вероятность X последствия

		Ймовірність		
		Низька	Середня	Висока
Наслідки	Тяжкі			
	Середні			
	Незначні			

Почему сложно оценить вероятность

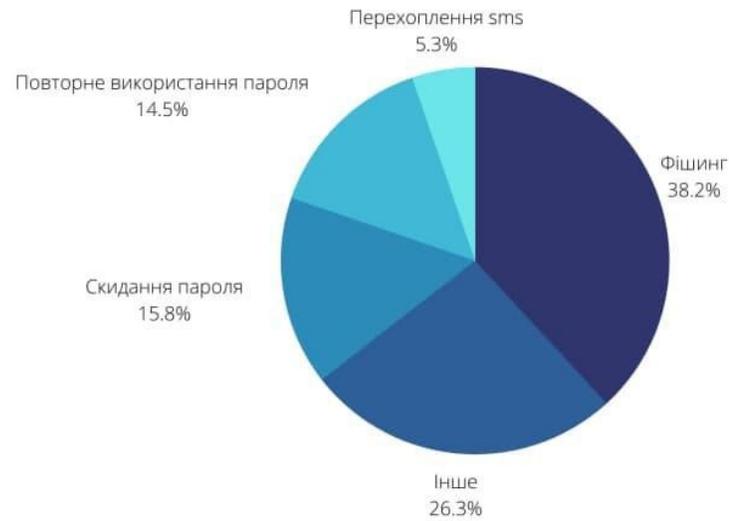
Непонимание модели (мы не понимаем, в чем риск везде использовать одинаковые пароли)

Когнитивные искажения (недооцениваем риски будничных событий, переоцениваем риски непривычных событий)

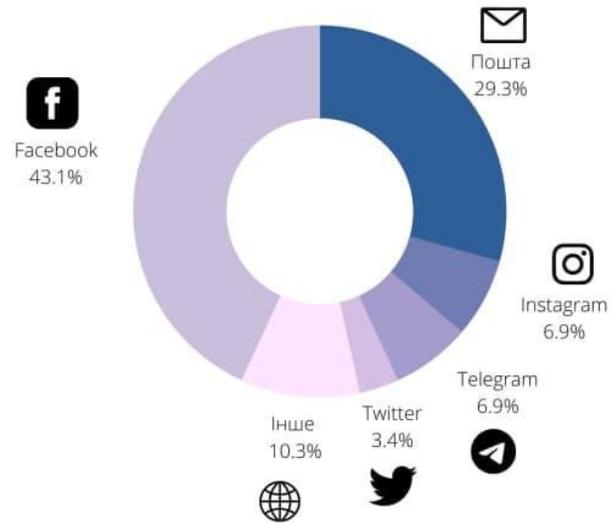
Недостаток информации о том, какие инциденты происходят

НАЙПОШИРЕНІШІ ЦИФРОВІ ЗАГРОЗИ ДЛЯ ЖУРНАЛІСТІВ ТА АКТИВІСТІВ У 2020

Способи атак



Що атакують найчастіше



Что можно делать с рисками

Избегать

Принять

Делегировать

Уменьшить

Защита онлайн аккаунтов



Защита аккаутов

Двухфакторная аутентификация

Уникальные пароли

Надежные способы восстановления

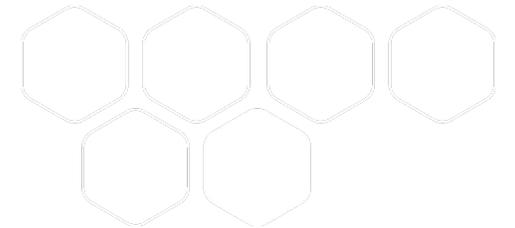
Надежные устройства

Техподдержка

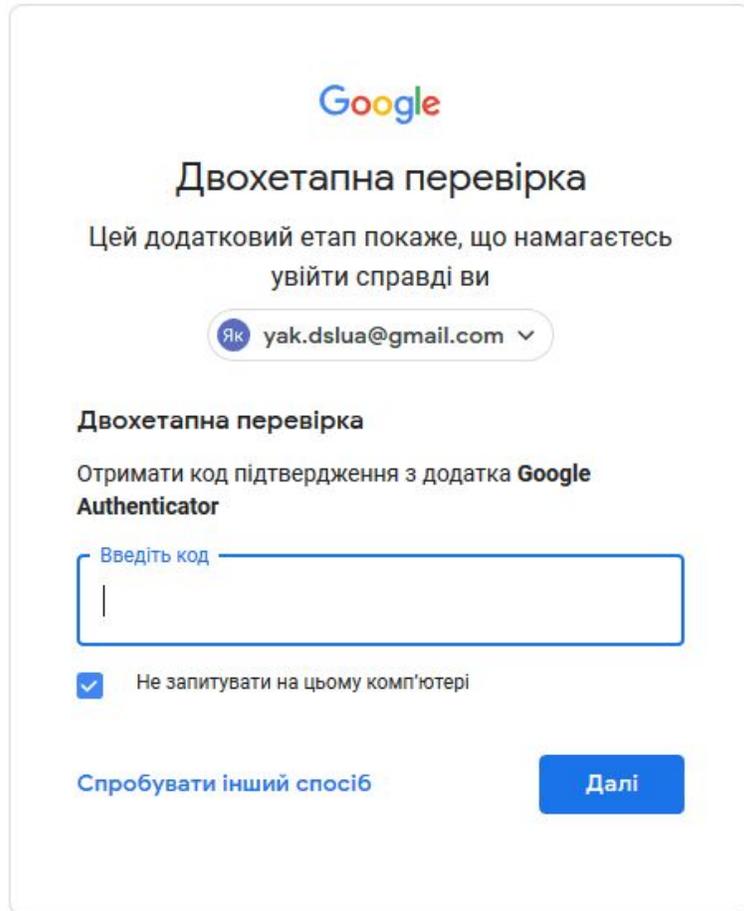
Двухфакторная аутентификация

Существенно повышает защиту учетной записи.
Без нее аккаунт не считается защищенным.

- Код в sms
- Push уведомление
- Приложение на смартфон Генератор кодов
- Резервные коды
- Физический ключ



Двухфакторная аутентификация



The image shows a screenshot of the Google two-step verification process. At the top is the Google logo. Below it, the heading "Двохетапна перевірка" (Two-step verification) is displayed. A sub-heading explains that this is an additional step to verify the user's identity. The user's email address, "yak.dslua@gmail.com", is shown in a dropdown menu. The main heading "Двохетапна перевірка" is repeated, followed by instructions to receive a code from the Google Authenticator app. A text input field is provided for the user to enter the code, with the placeholder text "Введіть код" (Enter code). Below the input field is a checked checkbox with the text "Не запитувати на цьому комп'ютері" (Do not ask on this computer). At the bottom of the form, there is a link "Спробувати інший спосіб" (Try another way) and a blue "Далі" (Next) button.

Українська ▾

Довідка

Конфіденційність

Умови

Двухфакторная аутентификация

← Двохетапна перевірка

Двохетапну перевірку ВВІМКНЕНО з 30 бер. 2021 р.

ВІМКНУТИ

Доступні другі етапи

Після того, як ви ввели пароль, другий етап перевірки підтверджує, що це справді ви.

[Докладніше](#)

Примітка: якщо на сумісному телефоні ввійти в обліковий запис Google, то на нього будуть надходити резервні сповіщення для двохетапної перевірки.



Голосове або текстове повідомлення (за умовчанням) ?

09

1 Підтверджено



Коди підтвердження надсилаються текстовим повідомленням.

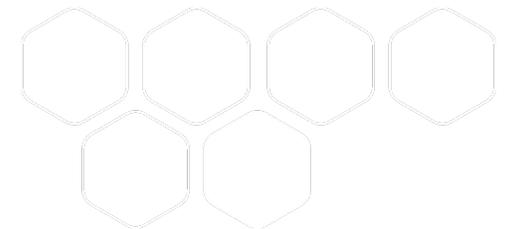


Резервні коди

Зараз активні 10 одноразових кодів, але за потреби можна згенерувати більше.

[ПОКАЗАТИ КОДИ](#)

Додайте інші варіанти другого етапу перевірки, щоб підтверджувати свою особу



Двухфакторная аутентификация

Настройка двухэтапной проверки, чтобы можно было вернуть, навіть якщо щось сталося

← Двохетапна перевірка



Сповіщення від Google

Коли ви вводите пароль, на кожний телефон, на якому ви ввійшли в обліковий запис, приходить сповіщення. Натисніть це сповіщення, щоб переглянути його й увійти. Щоб не отримувати сповіщення на певному телефоні, вийдіть з облікового запису на ньому. [Докладніше](#)

Примітка: якщо на сумісному телефоні увійти в обліковий запис Google, то на нього будуть надходити резервні сповіщення для двухетапної перевірки.

[ДОДАТИ ТЕЛЕФОН](#)



Додаток Google Authenticator

Отримуйте коди підтвердження безкоштовно за допомогою Генератора кодів, навіть коли ваш телефон не під'єднано до Інтернету. Доступно для пристроїв Android та iPhone.

[ЗГЕНЕРУВАТИ](#)



Резервний номер телефону

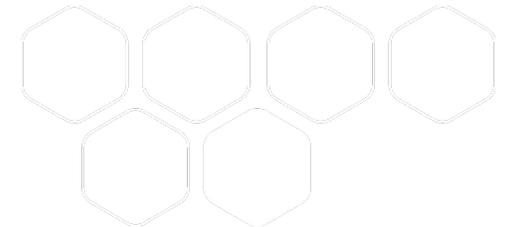
Додайте резервний номер телефону, щоб ви могли увійти в обліковий запис, якщо загубите телефон.

[ДОДАТИ ТЕЛЕФОН](#)



Ключ безпеки

Ключ безпеки — це найкращий спосіб підтвердження особи від користувача облікового

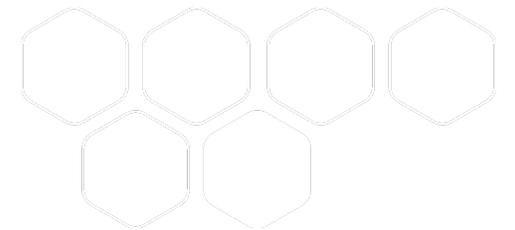


Пароли

Уникальные для важных аккаунтов.

Где хранить?

- блокнот?
- браузер?
- менеджер паролей?



Способы восстановления

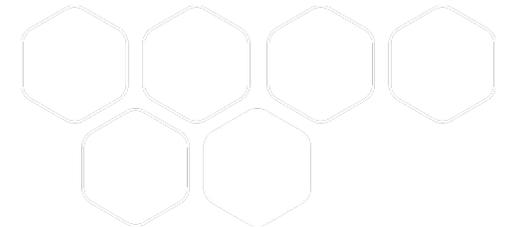
Пароль	Остання зміна: 20 січ.	>
Двохетапна перевірка	<input checked="" type="checkbox"/> Увімк.	>
Паролі додатків	Немає	>

Способи підтвердження вашої особи

Це допоможе підтвердити вашу особу під час входу або зв'язатися з вами, якщо ми виявимо підозрілу активність в обліковому записі



Номер телефону для відновлення	063	>
Електронна адреса для відновлення	cy @gmail.com	>



Контроль устройств и приложений

Ваші пристрої

Ви ввійшли в обліковий запис Google на цих пристроях

-  Windows
Україна
 Цей пристрій
-  Windows
Україна – 24 бер.
-  Windows
8 лют.

 Знайти втрачений пристрій

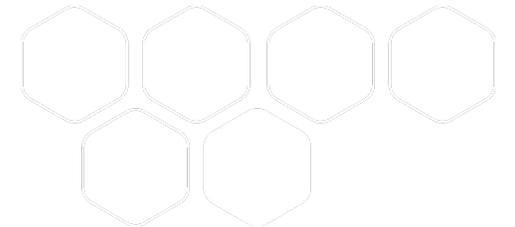
[Керувати пристроями](#)

Додатки Google, які мають доступ до облікового запису

Це сертифіковані додатки Google, установлені на ваших пристроях. Видаліть ті, якими ви більше не користуєтеся.

-  Google Chrome
Повний доступ до вашого облікового запису Google

[Керувати доступом](#)



Учетная запись защищена от взлома

У вас уникальные пароли для важных аккаунтов

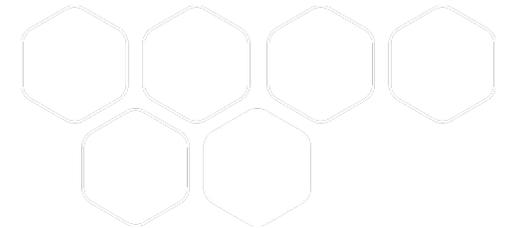
Включена двухфакторная (и сохранены резервные коды)

Зарегистрирована на доверенную почту (СОРМ)

Вам есть к кому обратиться для проверки подозрительных сообщений

Надежные способы

Входите в учетную запись только с надежных устройств





Як? Практичні поради з цифрової безпеки

Детальні інструкції допоможуть крок за кроком оптимізувати безпеку ваших пристроїв та сервісів.

[Обрати пристрій](#)

[f](#) [t](#) - приєднуйтесь

Оберіть пристрій або сервіс


Windows
7 порад


MacOS
6 порад


Android
8 порад


iOS
6 порад

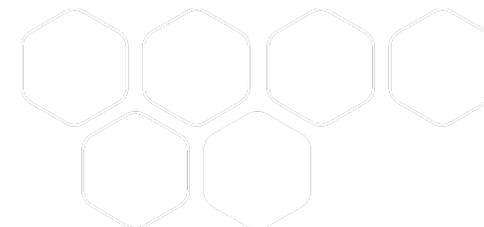

Telegram
3 поради


Twitter
6 порад


Facebook
7 порад


Gmail
6 порад


WhatsApp
4 поради





Оберіть пристрій або сервіс



Windows
7 порад



MacOS
6 порад



Android
8 порад



iOS
6 порад



Telegram
3 поради



Twitter
6 порад



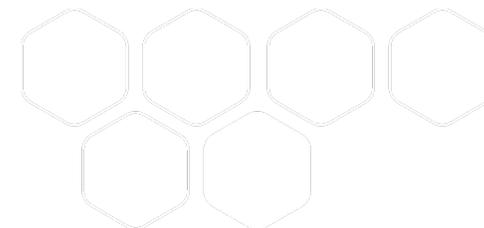
Facebook
7 порад



Gmail
6 порад



WhatsApp
5 порад





★ Пріоритетно

Двофакторна аутентифікація

Додатковий рівень захисту для вашого облікового запису на той випадок, якщо зловмисник дізнається ваш пароль.



★ Пріоритетно

Фішинг

Фішинг – найпоширеніша атака на обліковий запис.



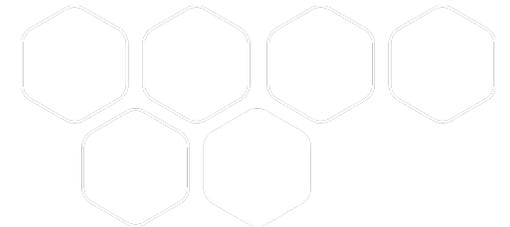
Відкриті сесії

Якщо ви закрили вкладку чи вікно браузера, це не означає, що ви вийшли зі свого облікового запису.



Контроль додатків

Додатки – це сторонні сервіси та програми, які мають певний доступ до вашого облікового запису.



Двофакторна аутентифікація

Оновлено 06.05.2019

Двофакторна аутентифікація — додатковий рівень захисту для вашого облікового запису на той випадок, якщо зловмисник якимось чином дізнається (підглядає, вгадає тощо) ваш пароль.

Вона передбачає, що при вході в обліковий запис з нового пристрою та браузера Google, окрім пароля, вимагатиме додаткове підтвердження вашої ідентичності.

Таким підтвердженням може бути sms з одноразовим кодом; додаток для смартфона (iOS або Android), який автоматично генеруватиме такі коди; набір із 10 одноразових резервних кодів, які ви можете роздрукувати чи переписати в блокнот; сповіщення на смартфон Google Prompt; фізичний ключ безпеки, який треба вставляти в USB-порт, наприклад, [YubiKey](#).

Якщо зловмисник знає ваш пароль, не маючи другого фактора (якогось із перерахованих вище), він не зможе зайти у ваш обліковий запис. І навпаки: маючи лише другий фактор, зловмисник не отримає доступ до вашого облікового запису — йому потрібно буде також дізнатись ваш пароль.

Як налаштувати двофакторну аутентифікацію на Google?

1. Зайдіть у налаштування вашого облікового запису. Для цього у вікні Gmail натисніть на фото користувача чи ініціали у верхньому правому куті, а у віконці, що з'явиться, на кнопку «Обліковий запис Google».

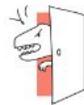
 Gmail 6 порад



★ Двофакторна аутентифікація



★ Фішинг



★ Відкриті сесії



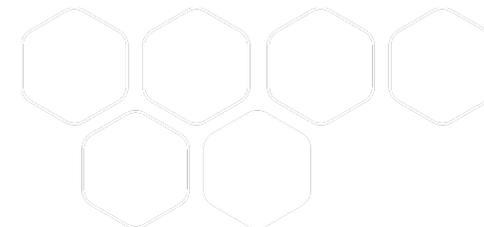
★ Контроль додатків



★ Пароль до облікового запису

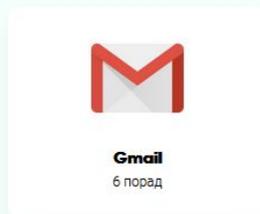
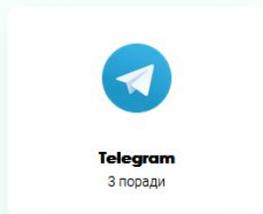
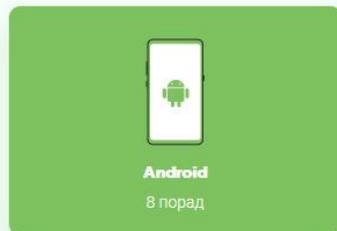
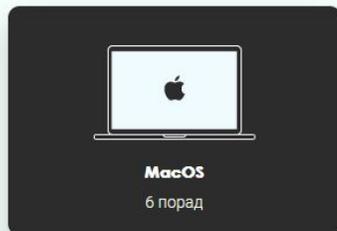
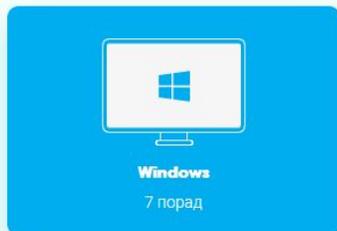


★ Способи відновлення облікового запису

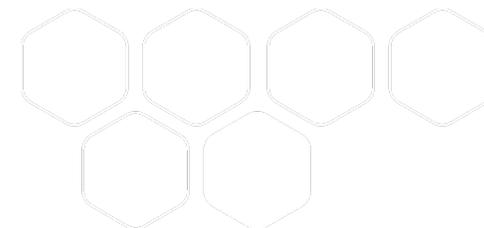




Оберіть пристрій або сервіс



yak.dslua.org



Безопасная коммуникация

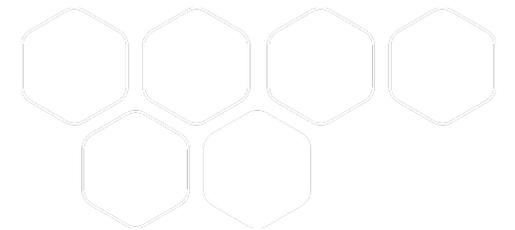
Защита коммуникации

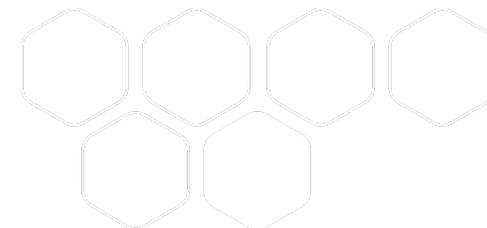
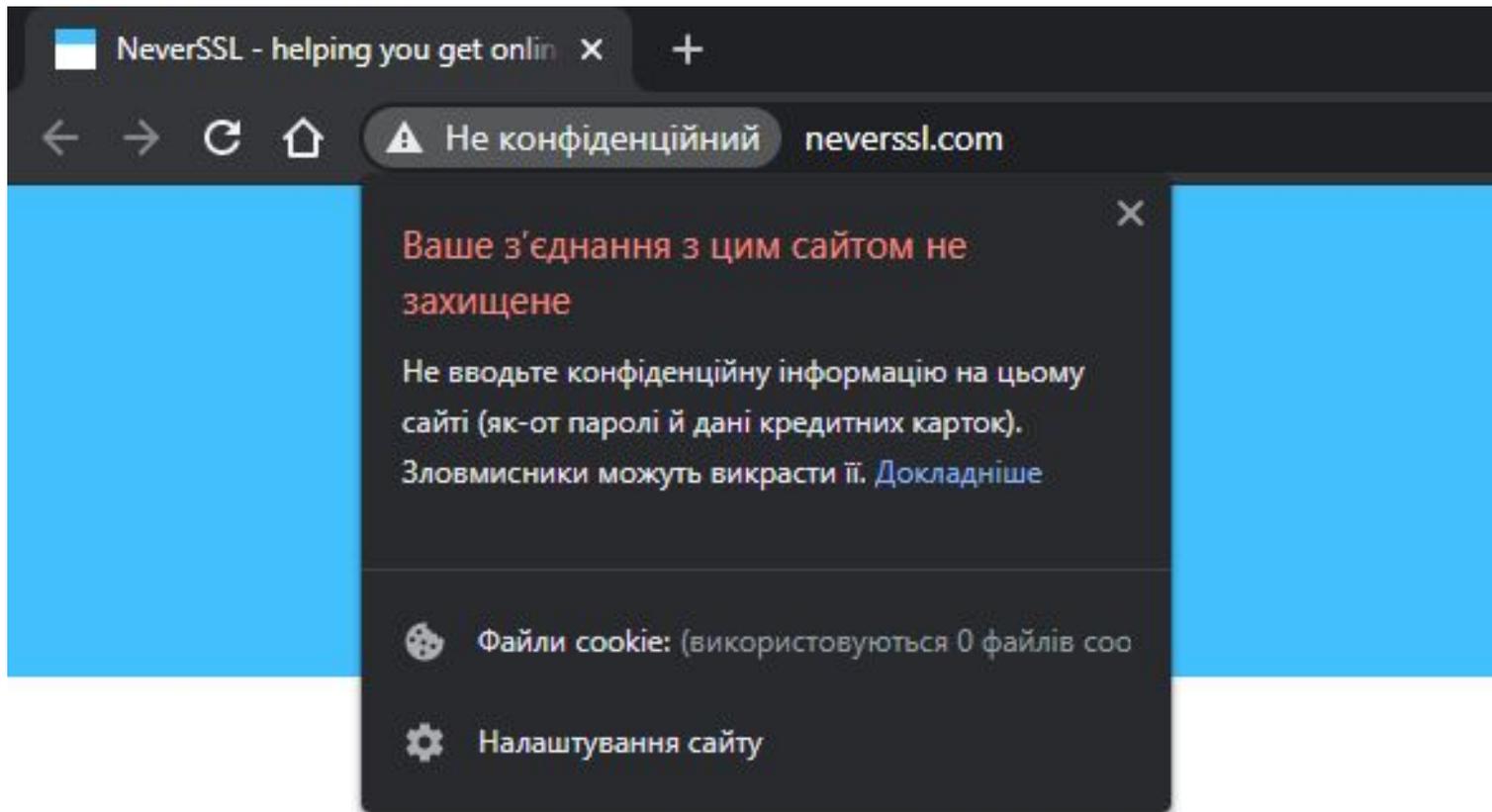
Безопасность коммуникации в Интернете

Защита мессенджеров от взлома

Угрозы мобильной связи

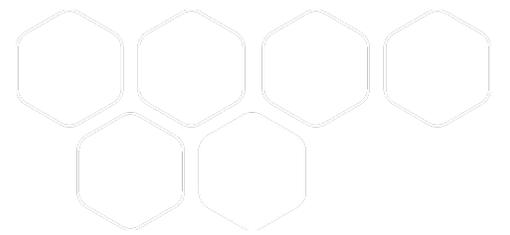
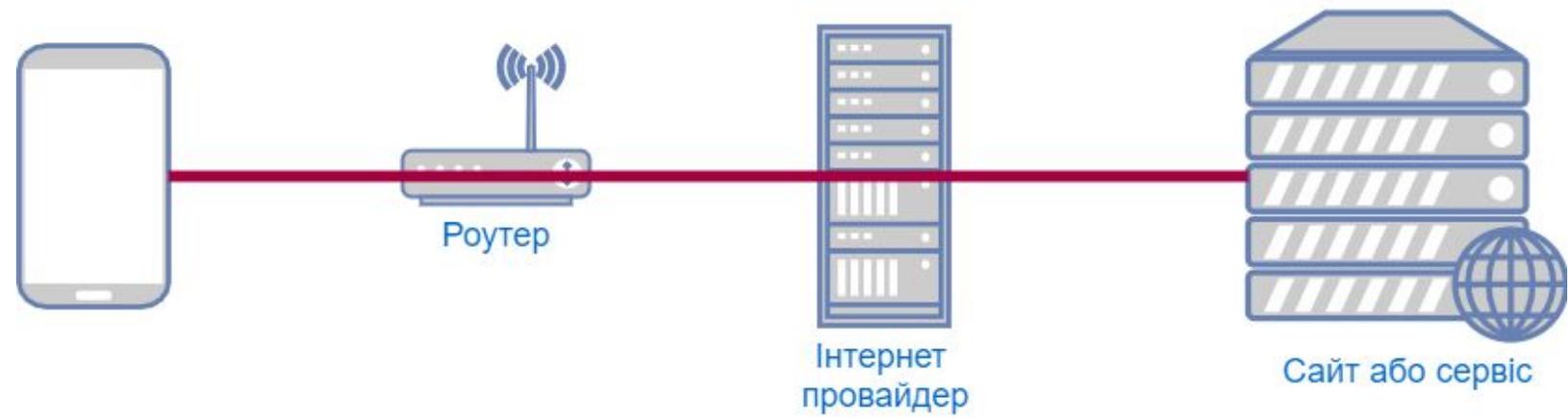
Безопасность коммуникации в Интернете





HTTP – незащищенное соединение

HTTP - незахищене з'єднання



З'єднання безпечне ×

Ваша інформація (як-от паролі та номери кредитних карток) залишається конфіденційною, коли надсилається на цей сайт. [Докладніше](#)

📄 Сертифікат (Дійсний)

🍪 Файли cookie: (використовуються 6 файлів соо

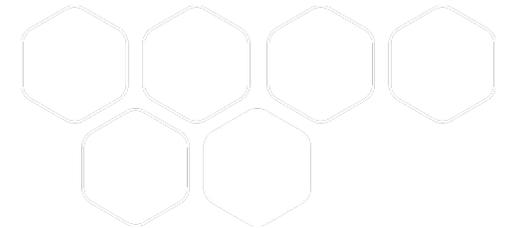
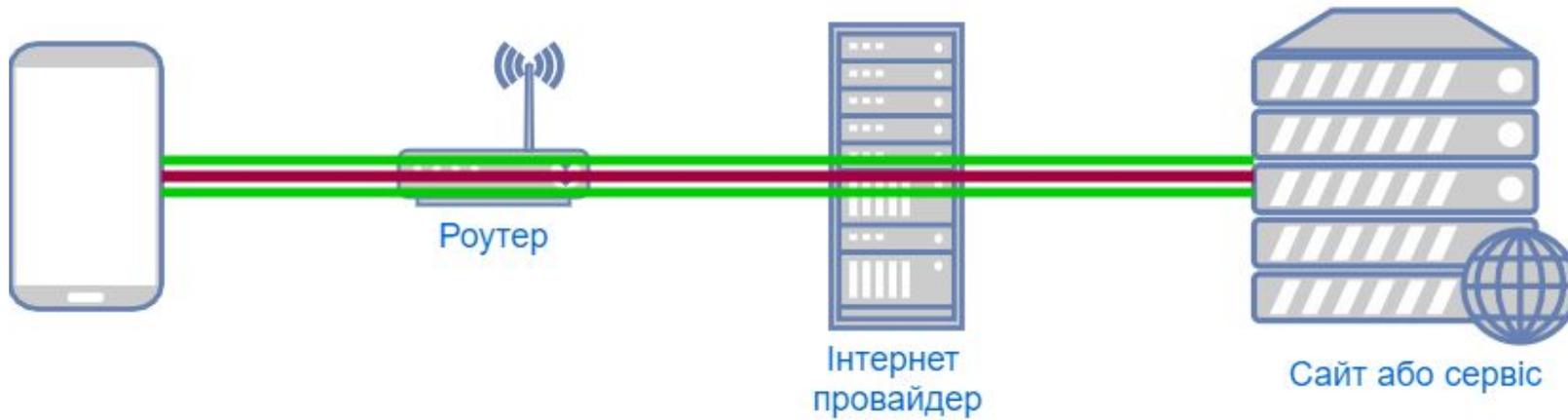
⚙️ Налаштування сайту

face

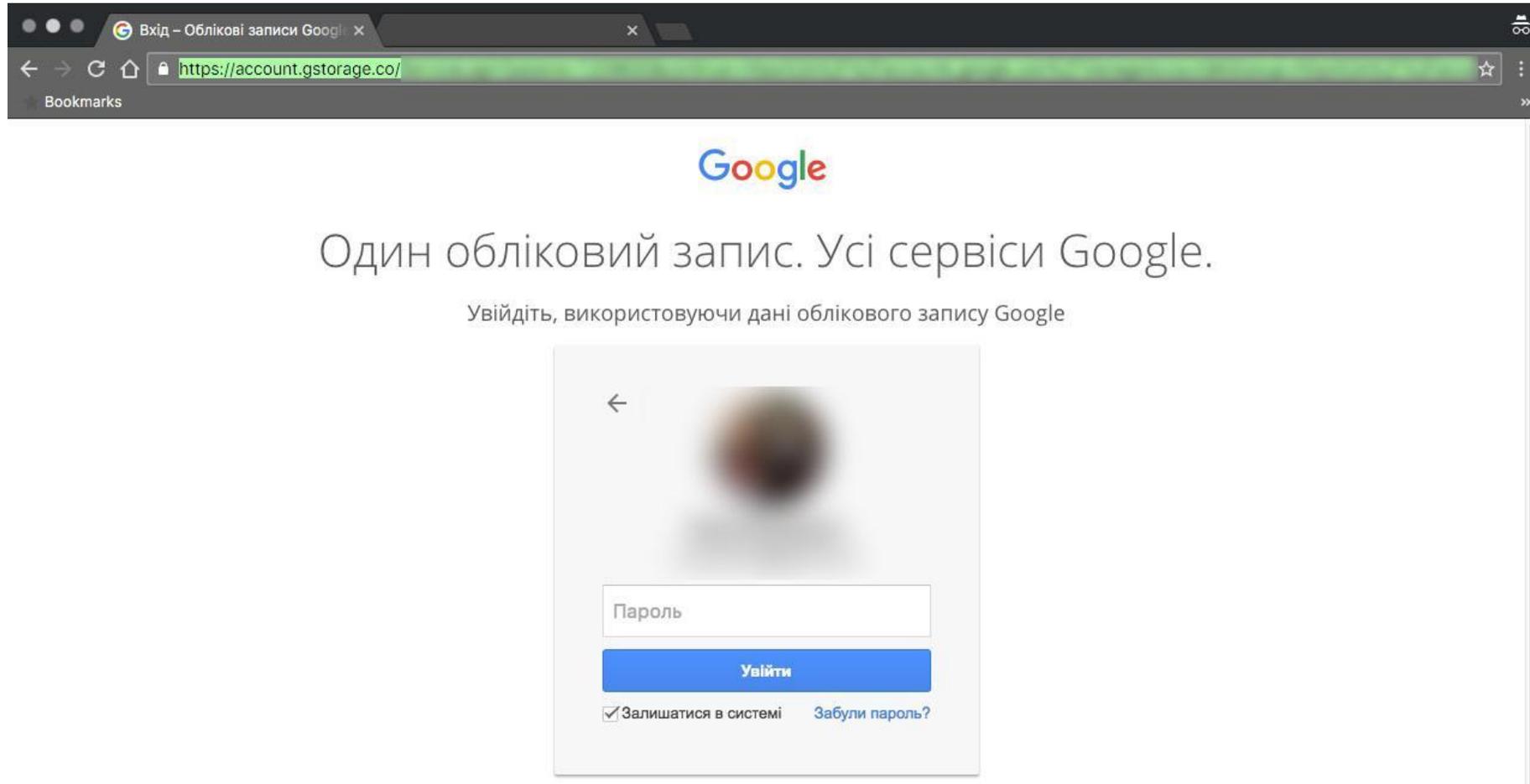
Facebo

HTTPS – защищенное соединение

HTTPS - захищене з'єднання

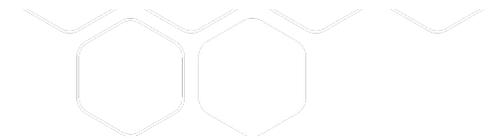
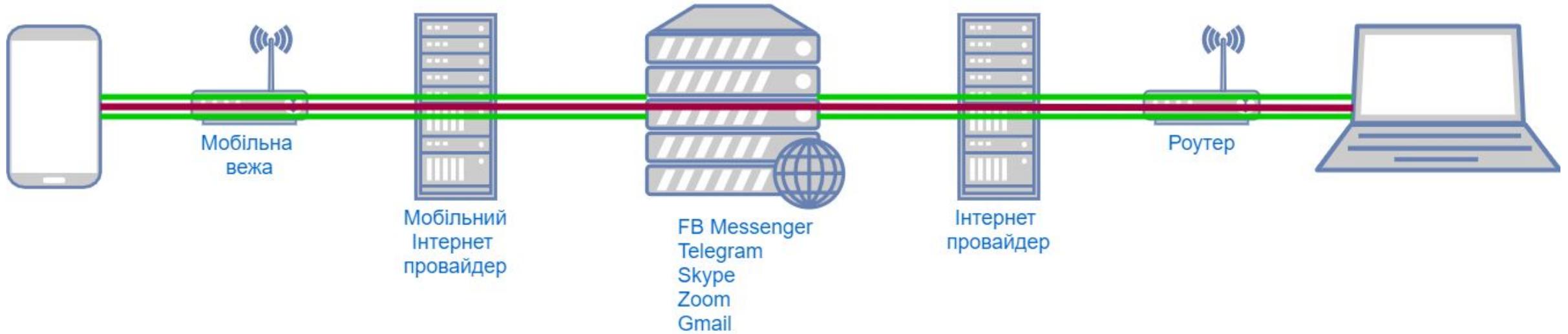


Защищенное соединение не означает, что сам сайт безопасный



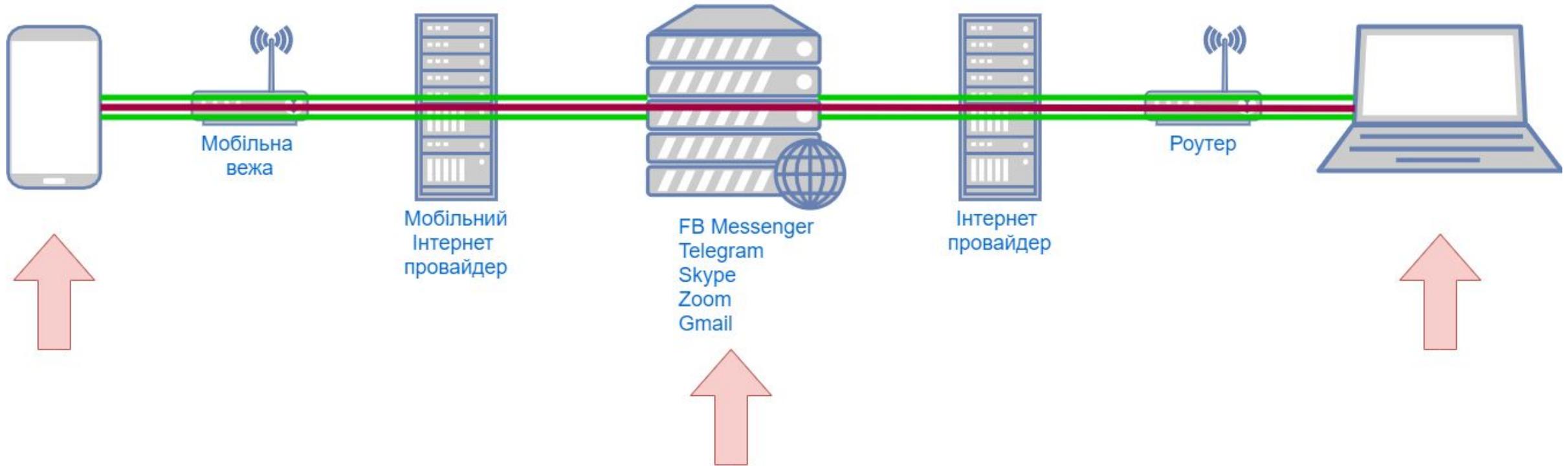
HTTPS – захищеное соединение

HTTPS - захищеное з'єднання



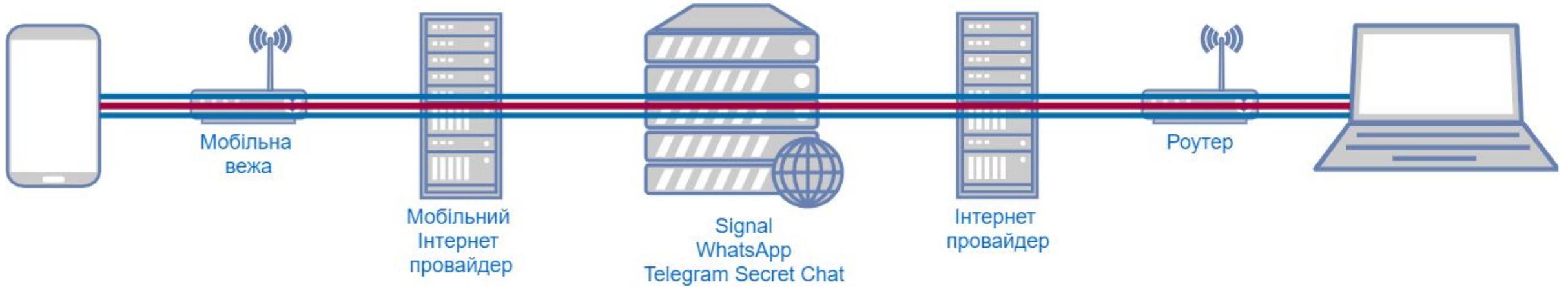
HTTPS – захищеное соединение

HTTPS - захищеное з'єднання



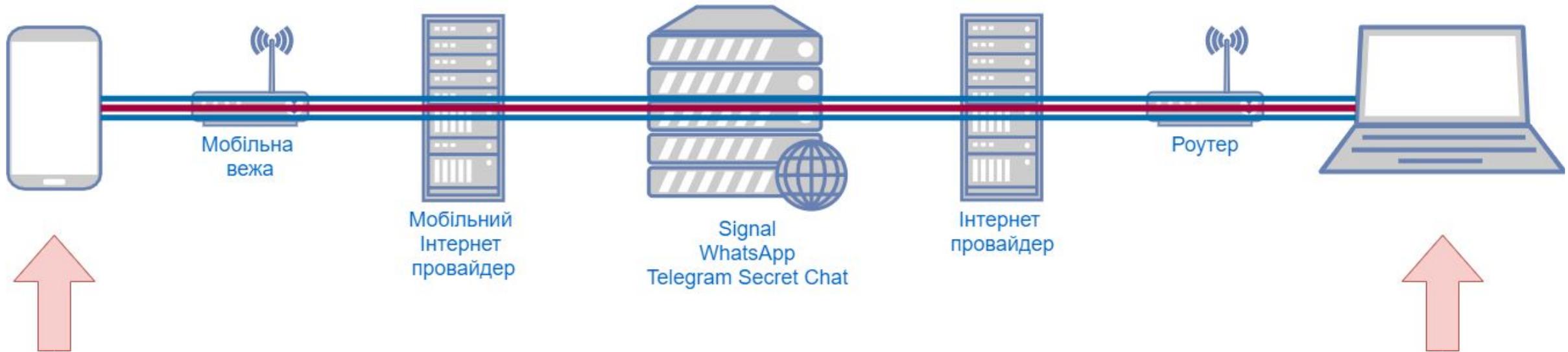
End to End (сквозное) зашифрованное соединение

End to End - зашифроване з'єднання

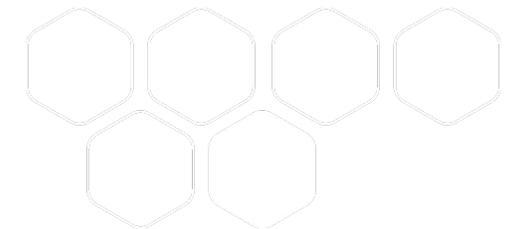
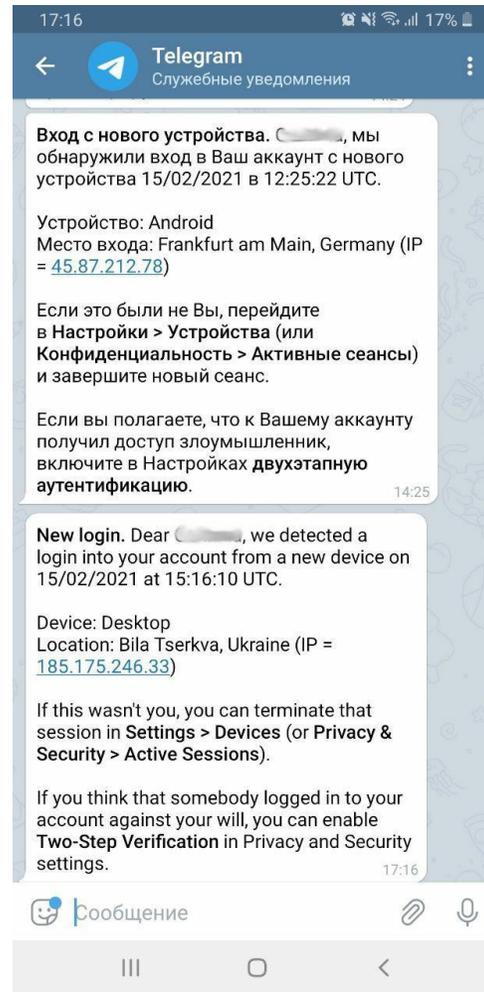
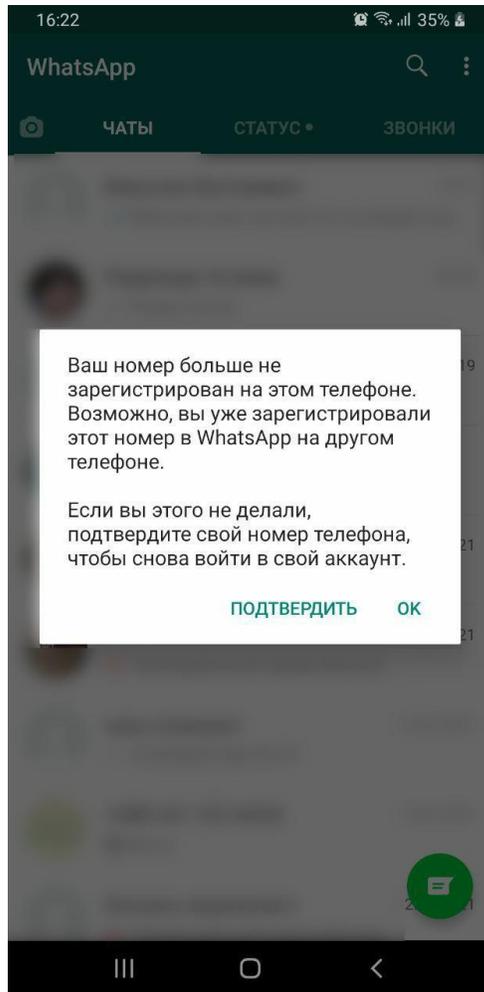


End to End (сквозное) зашифрованное соединение

End to End - зашифроване з'єднання



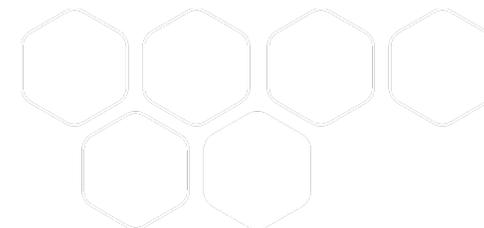
Как взламывают мессенджеры



Как взламывают мессенджеры

Будут не пробовать «подслушать», а зайти в ваш мессенджер таким же образом, как заходите вы (код в СМС)

От этого защищает двухфакторная аутентификация (вам нужно придумать пароль/PIN-код)



Важные моменты в мессенджерах

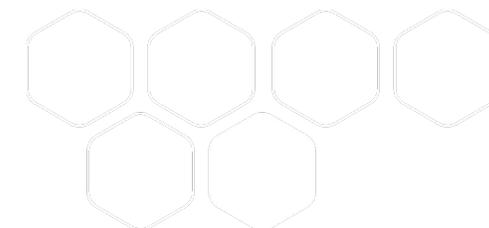
Где хранится история переписки

Автоудаление сообщений

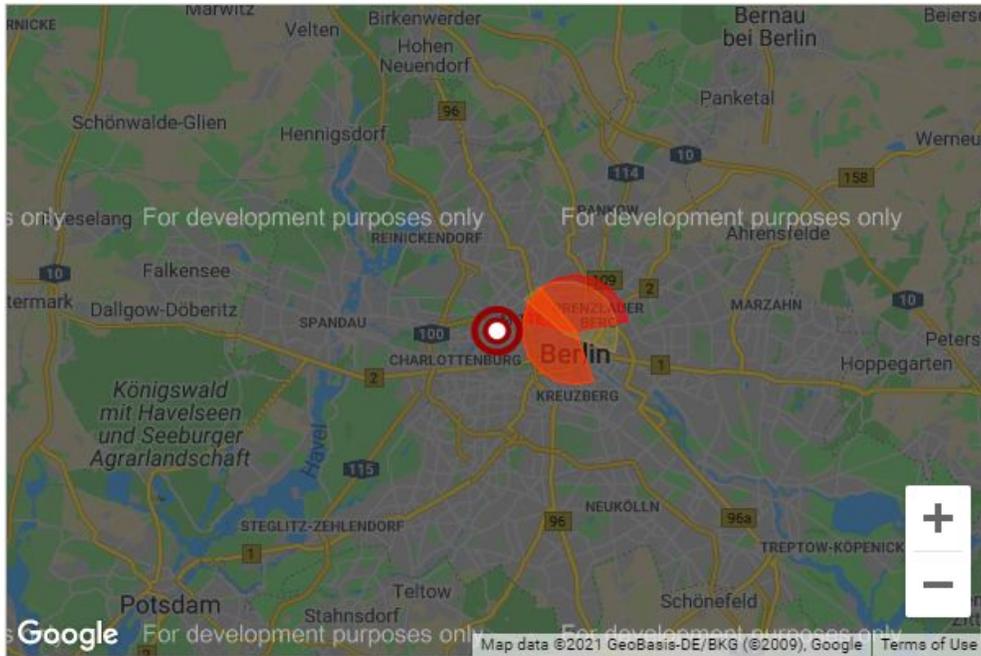
Автозагрузка медиа в галерею телефона

Защита от людей, которые взяли ваш телефон в руки (блокирование приложений, «спрятанные чаты»): важно не путать с двухфакторной

Где вы залогинены сейчас (контроль сессий)



<https://www.zeit.de/datenschutz/malte-spitz-data-retention>



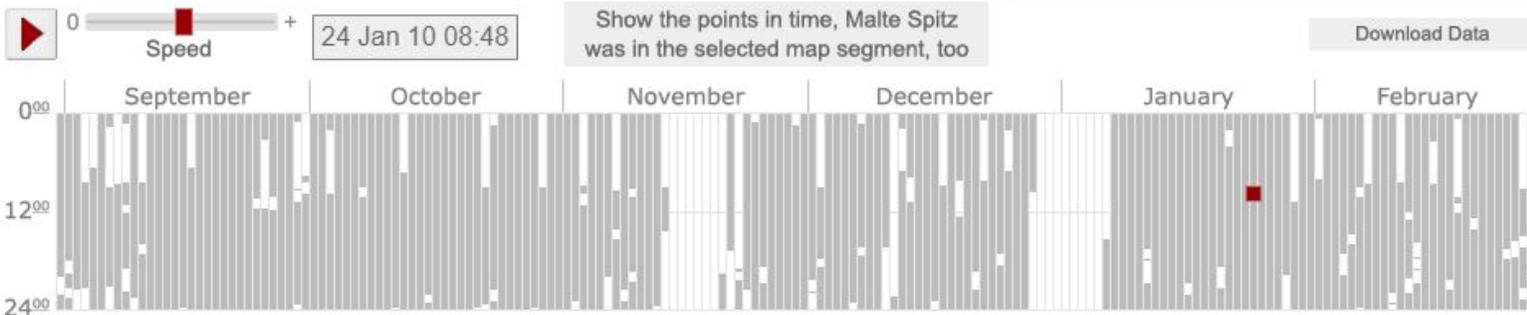
Sunday, 24 January 2010

i After a round-trip journey to Mühlheim in one day, Spitz tweets that he has traveled 5,000 kilometres by train over ten days. (source: [Twitter](#))

📞 2 incoming calls
7 outgoing calls
total time: 0h 13min 26s

SMS 46 incoming messages
29 outgoing messages

🌐 duration of internet connection:
23h 45min 23s

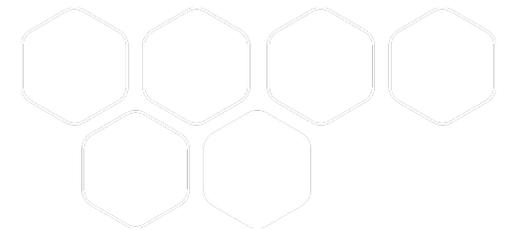


Что сохраняют мобильные провайдеры?

Историю звонков (метаданные)

Историю СМС (данные)

Историю местонахождения



Защита устройств



От чего защищаемся

Кто-то получит доступ к информации с телефона или компьютера

Мы потеряем доступ к информации с телефона или компьютера

Кто-то получит доступ

Дистанционно: при помощи зловредного ПО («вирусы»)

Физически: будет иметь кратковременный или длительный доступ к устройству

Мы потеряем информацию с устройства

Дистанционно: кто-то заразит вирусом-шифровальщиком

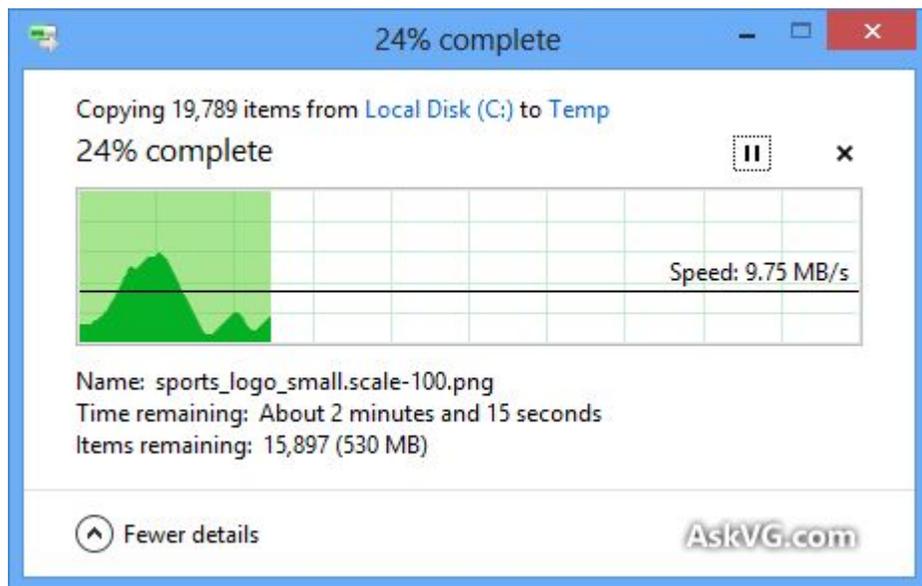
Физически: устройство украдут, конфискуют, сгорит жесткий диск

Защита информации от потери

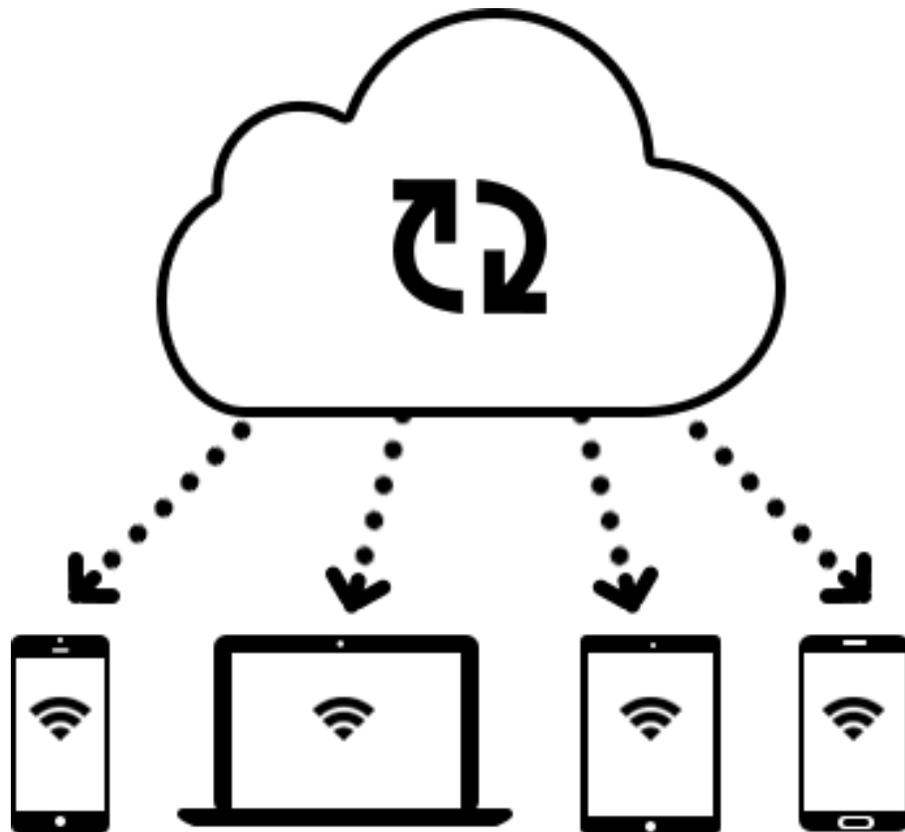
Регулярное копирование на внешние носители

Автоматическая синхронизация в облачное хранилище (Google Drive, iCloud, Mega.nz та ін.)

Резервное копирование на внешние накопители



Автоматическая синхронизация файлов в облако



iCloud Drive

Автоматическая синхронизация фото и видео с телефона

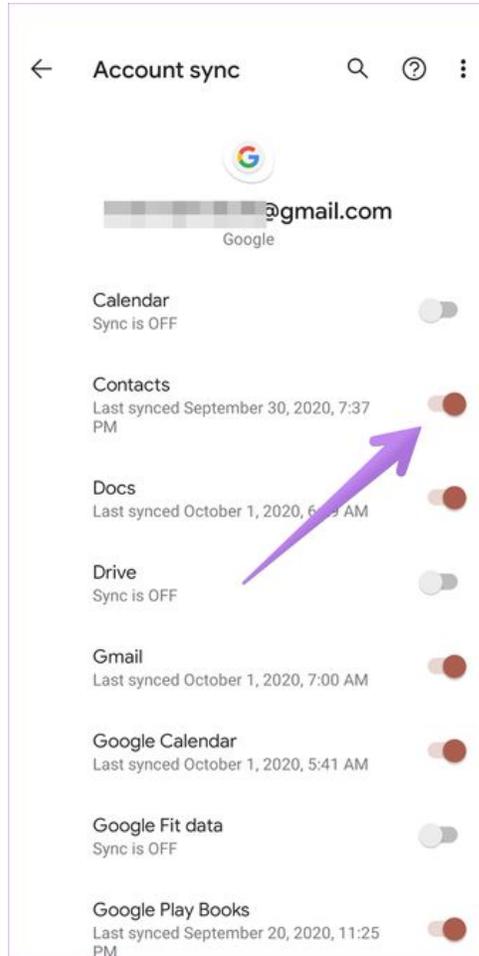


Google Photos



iCloud Drive

Автоматична синхронізація контактів



Защита от «вирусов»

Использование легального ПО
(<https://www.teplodigital.org>)

Регулярное обновление ПО

Антивирусное ПО

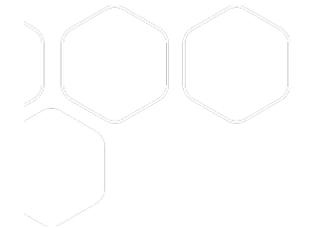
Разделение учетных записей (не админ)

Легальное ПО: terplodigital.org/product-catalog

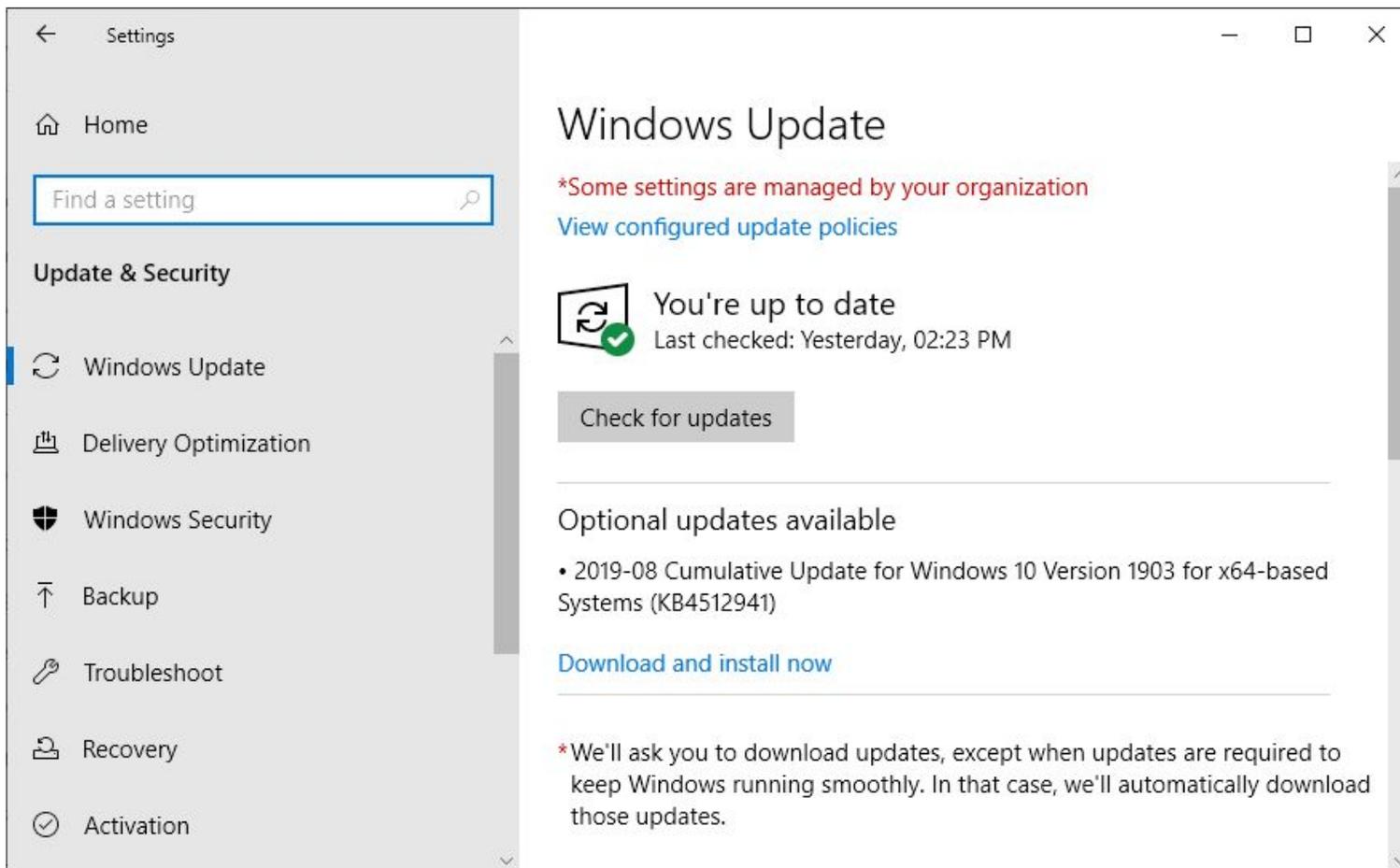
Каталог

ФИЛЬТРЫ Showing 20 of 57 Сортировать по Самые популярные

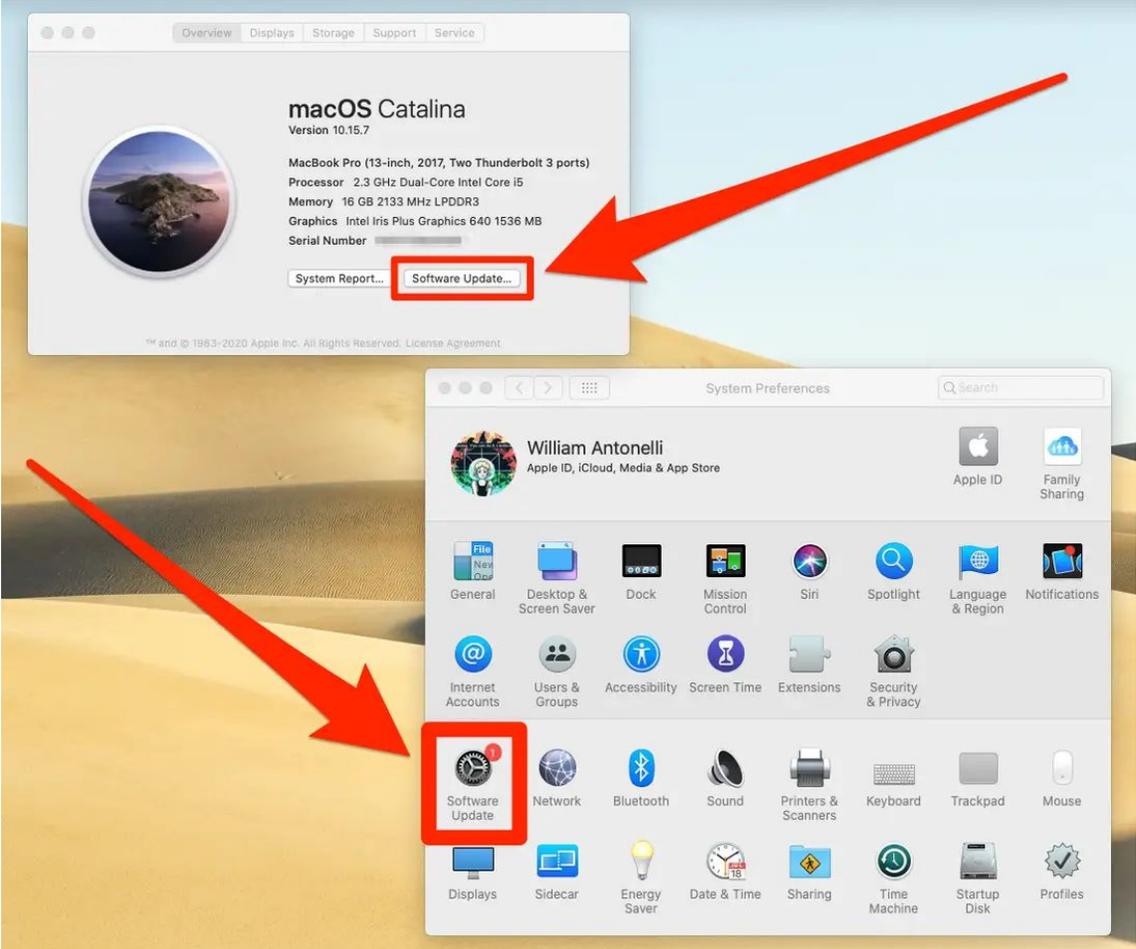
<p>Донор или компания (57) > Все</p>				
<p>Категория (42) > Все</p>	<p>Windows Get Genuine with COA</p> <p>Microsoft Get Genuine Windows для малых и средних организаций предлагает полноценную</p>	<p>Zoom Meetings на 1 год - Доступ к скидке 50% на план и дополнения</p> <p>Zoom Meetings объединяет видео-и аудиоконференции, простые онлайн-встречи и групповые чаты на одной</p>	<p>Office Standard</p> <p>Пожалуйста, обратите внимание на то, что все пакеты и отдельные приложения Office 2019, включая</p>	<p>Windows Operating System Upgrade</p> <p>Windows OS Upgrade - это новейшая версия операционной системы Microsoft корпоративного уровня</p>
<p>Форма установки (44) > Все</p>	<p>Административный сбор: 940,00 Р</p>	<p>Административный сбор: 4869,00 Р</p>	<p>Административный сбор: 3331,00 Р</p>	<p>Административный сбор: 1708,00 Р</p>
<p>Платформа (27) > Все</p>				
<p>Язык (389) > Все</p>	<p>Windows Server Standard</p> <p>Важно: срок получения</p>	<p>Windows Server Device CAL</p> <p>Windows Server пред-</p>	<p>Windows Server User CAL</p> <p>Windows Server пред-</p>	<p>Exchange Server Standard Edition</p> <p>Данная лицензия кли-</p>



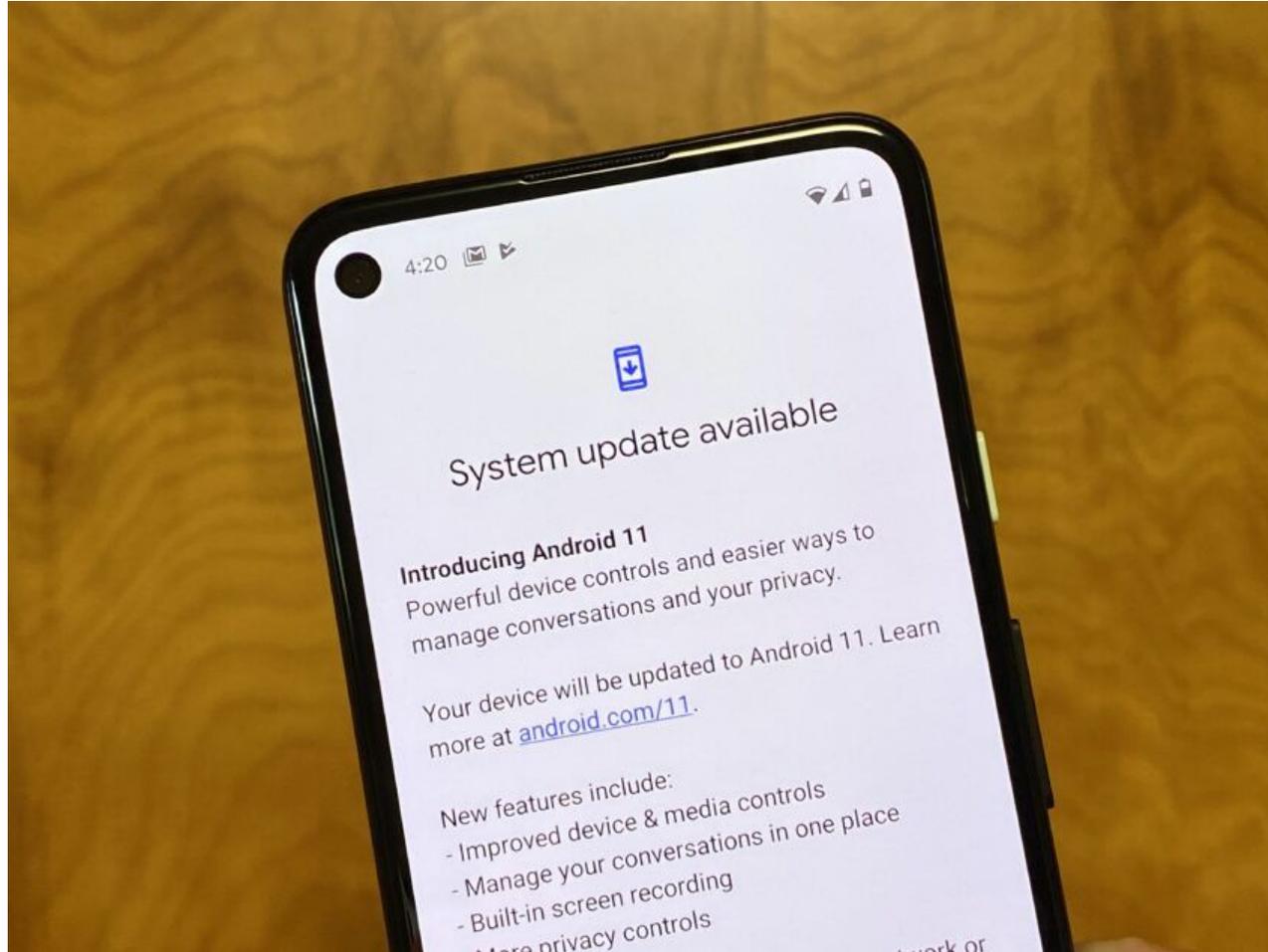
Обновление ОС и программ



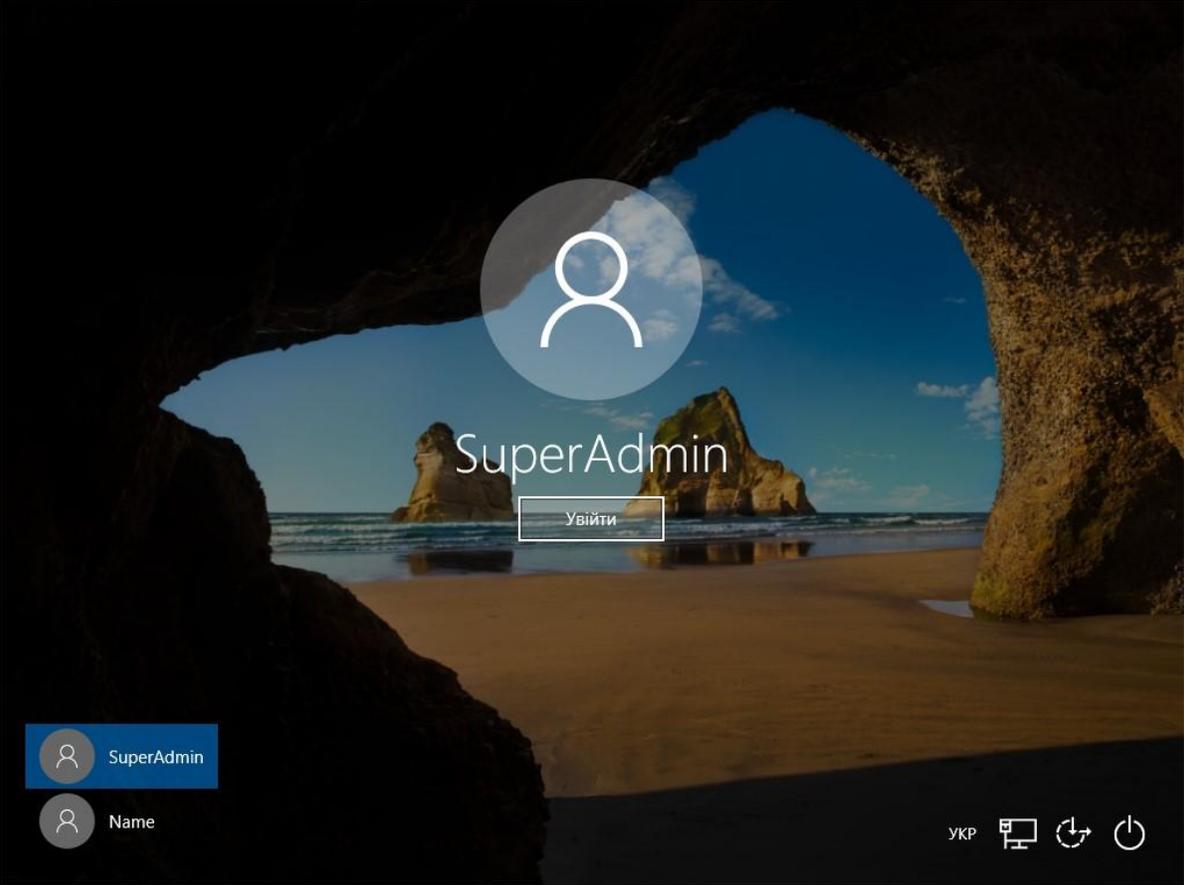
Обновление ПО и программ



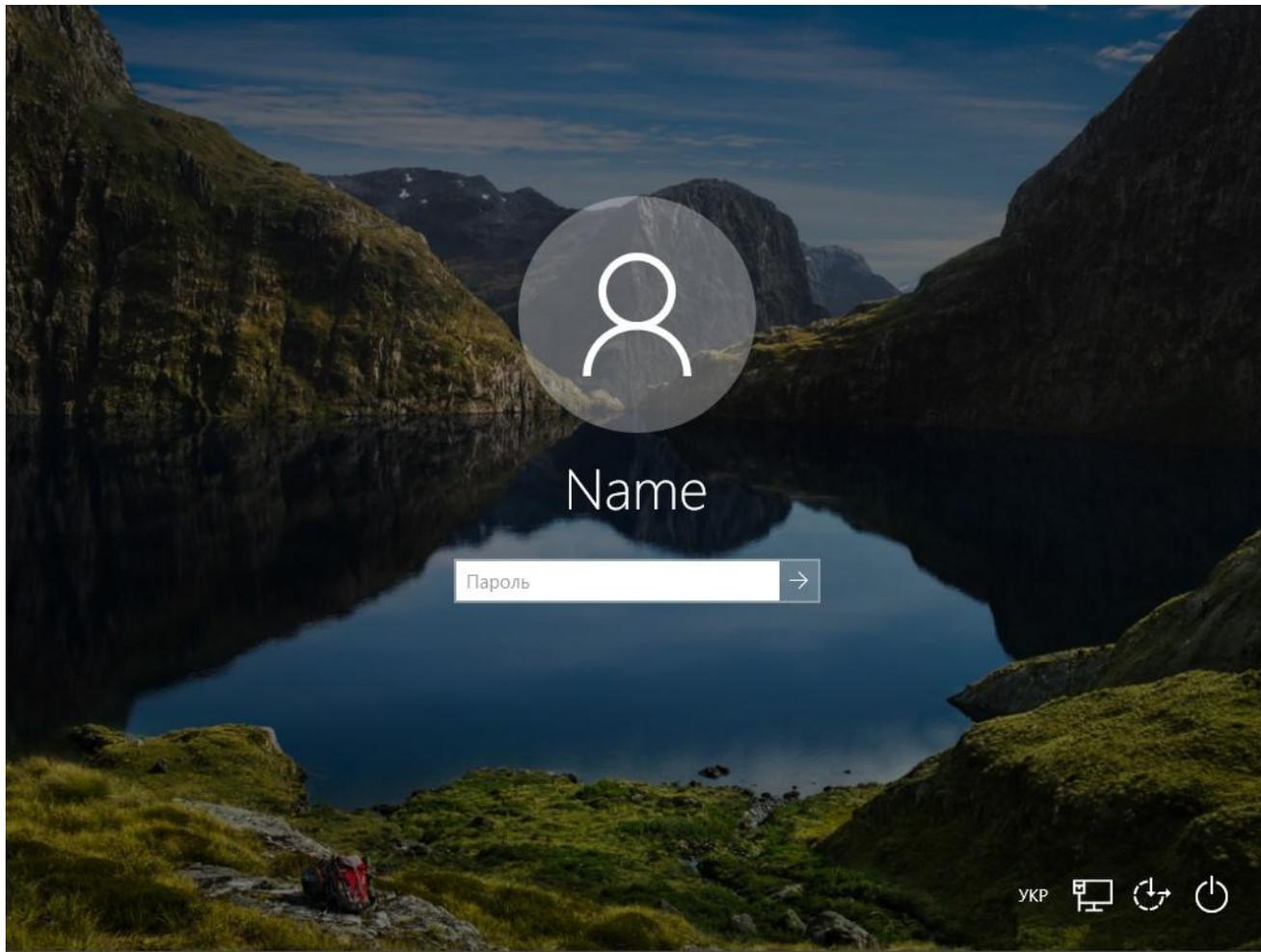
Обновление ПО и программ



Разделение учетных записей



Блокировка экрана



Блокировка экрана

The image shows a Windows Settings window titled "Екран блокування" (Screen Locking). The "Параметри заставки" (Wallpaper Settings) dialog box is open, showing the following options:

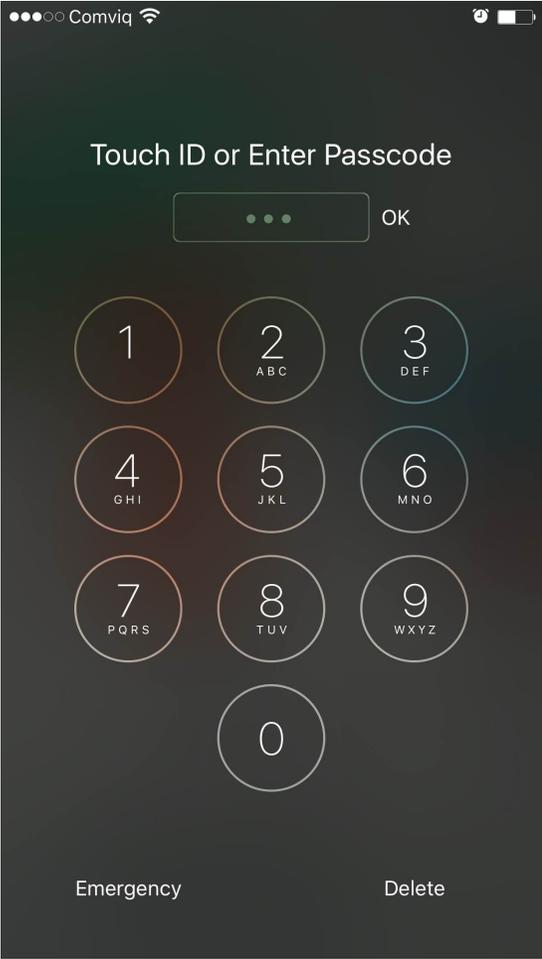
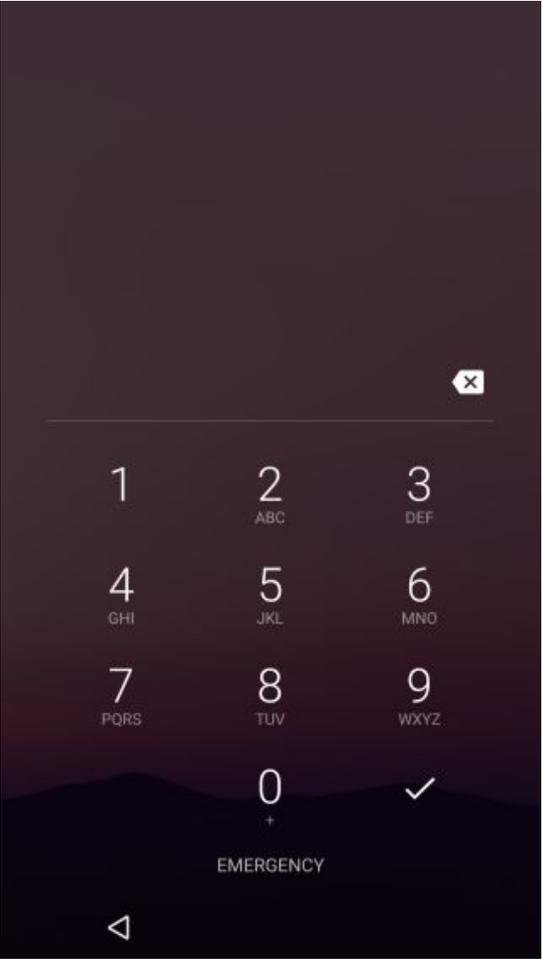
- Заставка:** (none) selected, with "Настройки..." and "Перегляд" buttons.
- Інтервал:** 10 хв (minutes).
- Починати з екрана входу до системи (Start with the sign-in screen).

Below these settings, there is a section for "Керування живленням" (Power Management) with a description: "Можна збалансувати збереження електроенергії та підвищення продуктивності за допомогою налаштування яскравості дисплея та інших параметрів живлення." (You can balance power savings and performance by adjusting display brightness and other power settings.) A link "Змінити параметри живлення" (Change power settings) is provided.

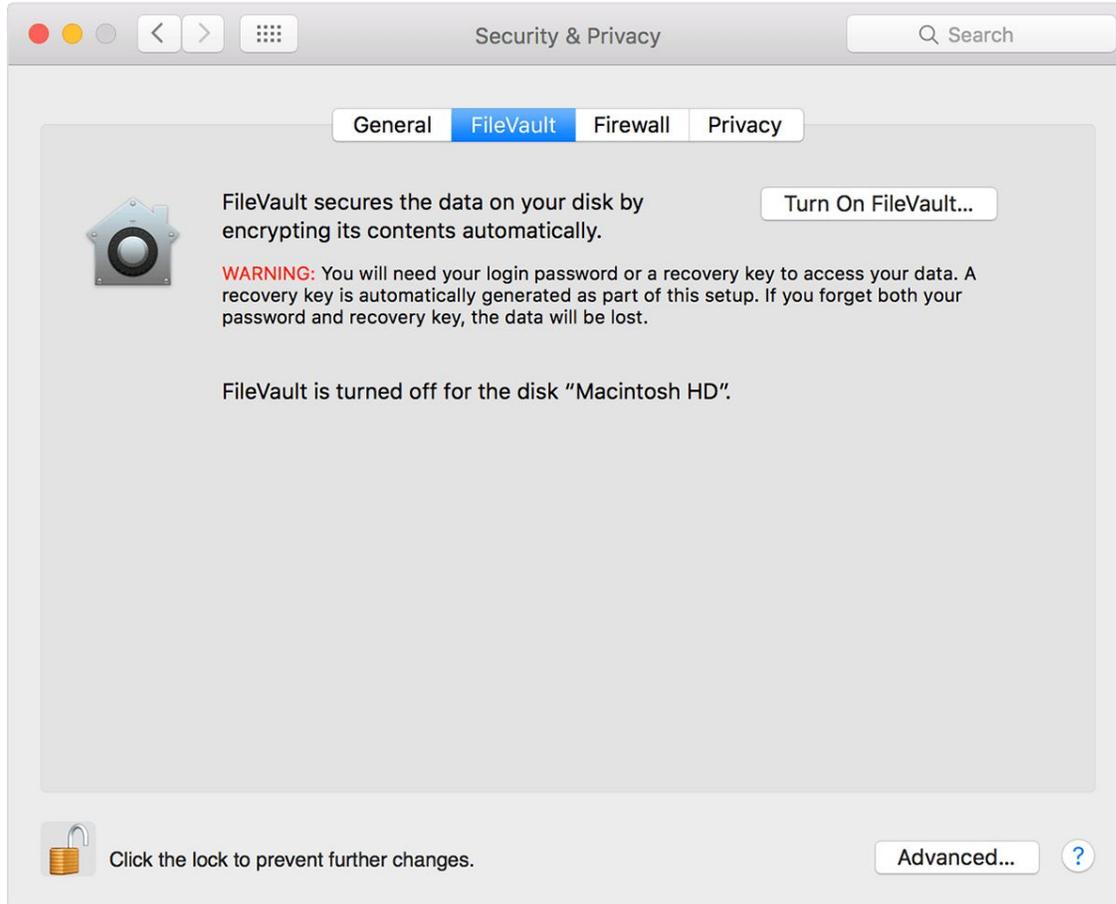
At the bottom of the dialog are "ОК", "Скасувати", and "Застосувати" buttons. The background settings window shows a toggle for "Увімкнуто" (On) and links for "Налаштування часу очікування екрана" (Screen timeout settings) and "Параметри заставки" (Wallpaper settings).

The Windows taskbar at the bottom shows the time as 13:20 on 17.12.2018, with system icons for network, volume, and language (ENG).

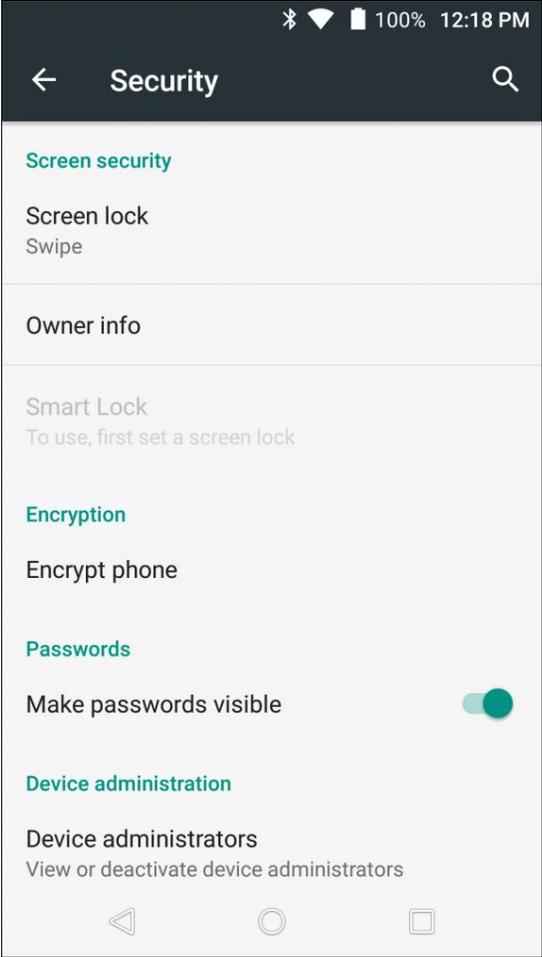
Блокировка экрана



Шифрование MacOS



Шифрование Android



Защита информации на компе

Легальное ПО

Обновление ПО

Резервные копии важной информации

Разделение учетных записей

Блокировать экран

Полнодисковое шифрование

Защита информации на мобильных

Последние версии Android OS или iOS

Обновление приложение

Резервные копии

Блокировка экрана (пароль, TouchID\FaceID)

Полнодисковое шифрование