**Міністерство освіти та науки України**

**Державний торговельно-економічний університет**

***Кафедра інженерії програмного забезпечення та кібербезпеки***

**ЗВІТ**

***З ЛАБОРАТОРНОЇ РОБОТИ № 4***

*з дисципліни*

**«ОСНОВИ КІБЕРБЕЗПЕКИ»**

**НА ТЕМУ:**

ВІЗУАЛІЗАЦИЯ «ЧОРНИХ» ХАКЕРІВ

(назва теми)

**Виконала:** студентка факультету інформаційних технологій

Групи 4 курсу 3

Авєріна Наталія Ігорівна

**Викладач:** Ковальова Людмила Ігорівна

Київ 2024

**Лабораторна робота №5**

**Цілі та задачі**: Проаналізувати можливості функцій безпеки, які використовують такі організації, як Google та Cisco, для захисту даних.

**Хід роботи:**

**Part 1:Захист даних**

1. Захист даних Google
   1. Як Google гарантує, що сервери, які вони встановлюють у своїх центрах обробки даних (ЦОД), не заражені зловмисним програмним забезпеченням виробниками обладнання?

Машини створюються компанією Google на замовлення відповідно до власних специфікацій. Щороку Google створює тисячі серверів, але всі вони створені виключно для роботи в цих центрах обробки даних. Встановлено лише необхідні служби операційної системи та обладнання.

* 1. Як Google здійснює захист від фізичного доступу до серверів, розташованих у центрах обробки даних Google?

Доступ до центрів обробки даних Google жорстко контролюється. Політика Google забороняє публічні екскурсії чи відвідування сайтів. Охорона чергує 24 години на добу, сім днів на тиждень. Центри обробки даних Google контролюються повним набором камер відеоспостереження. Отримавши доступ до закладу, уповноважений персонал повинен зареєструватися в зоні прийому.

* 1. Як Google захищає дані клієнта, що знаходяться на серверах?  
     Файли, у яких зберігаються дані, отримують випадкові імена і не зберігаються відкритим текстом. Тому вони нерозбірливі для людини.

1. Визначення вразливостей даних.
   1. Де ще можна знайти дані під час використання пошукової системи Google?

Навіть якщо дані у центрах обробки даних Google захищені, є кілька інших місць, де можуть зберігатися дані під час використання пошукової системи Google:

* + 1. Кешовані копії на пристроях користувачів
    2. Послуги третіх сторін
    3. Аналітичні і рекламні інструменти
    4. Партнери Google
  1. Є декілька заходів, які можна вжити для захисту даних при використанні пошукової системи Google:
     1. Використання захищеного з'єднання (HTTPS)
     2. Керування налаштуваннями конфіденційності
     3. Використання приватного режиму
     4. Вимкнення збереження історії пошуку
     5. Використання двофакторної аутентифікації

**Part 2:Підвищення безпеки облікового запису Google**

1. Ключі безпеки та двоетапна автентифікація
   1. Що таке двоетапна аутентифікація? Як ким чином вона захищає обліковий запис Google?  
      Двоетапна аутентифікація (2FA) - це метод захисту облікового запису, який вимагає від користувача подвійного підтвердження своєї ідентичності під час входу в обліковий запис. Зазвичай цей процес включає в себе щось, що ви знаєте (наприклад, пароль) і щось, що ви маєте (наприклад, код з смс або згенерований одноразовий код).

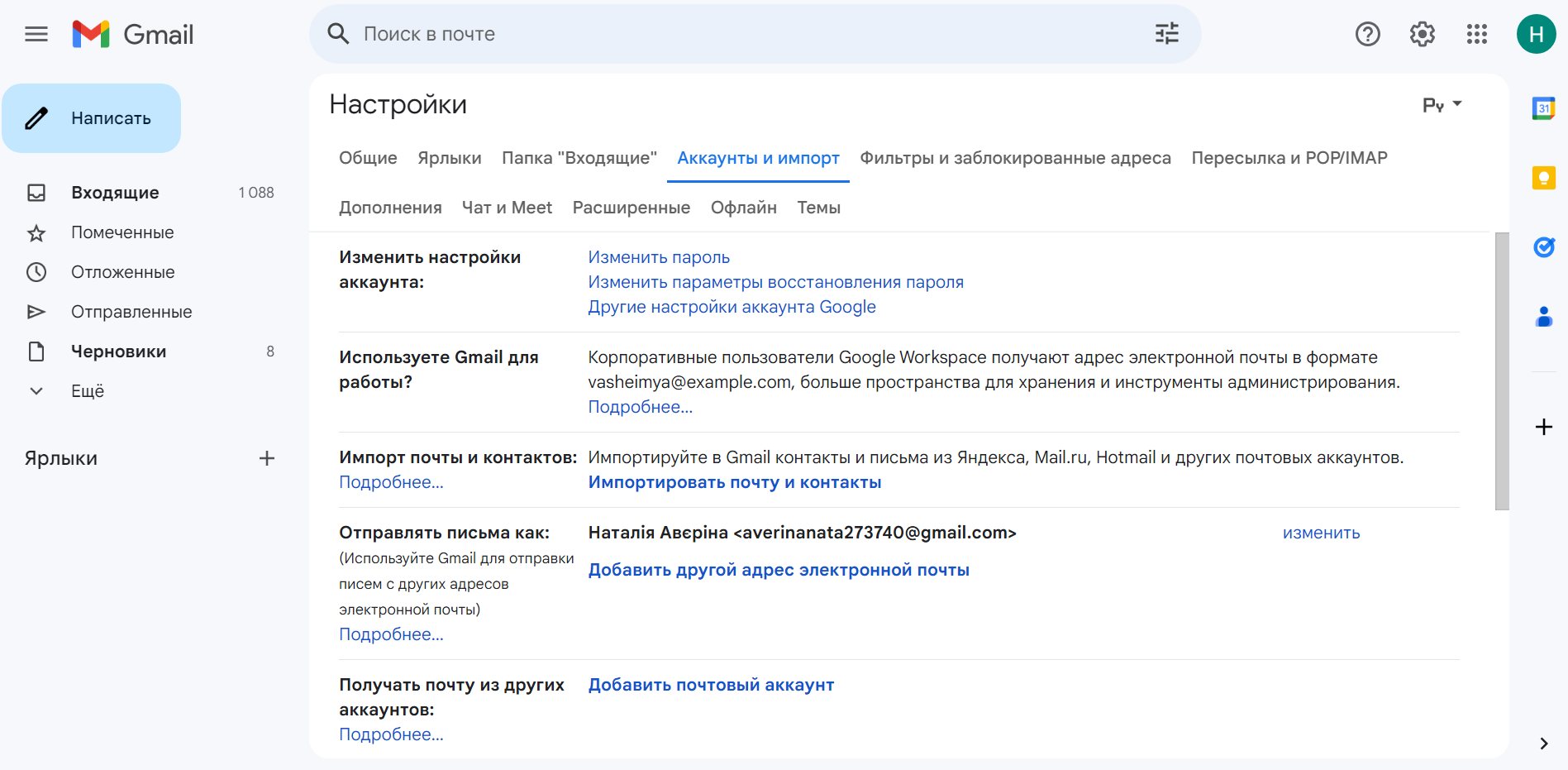
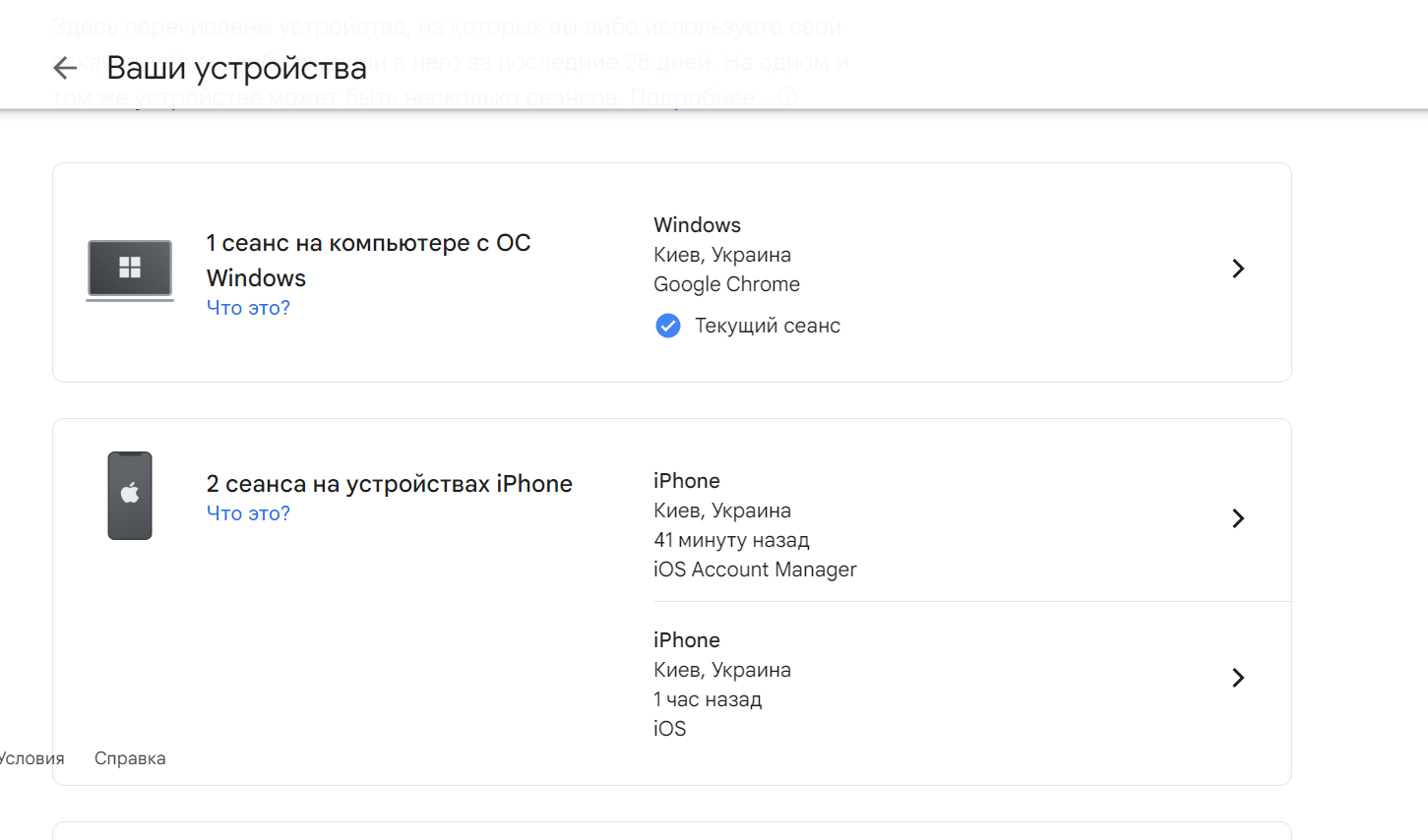
Двоетапна аутентифікація робить обліковий запис Google значно більш захищеним від несанкціонованого доступу, оскільки навіть якщо зловмисник знатиме ваш пароль, він все одно не матиме доступу до вашого облікового запису без додаткового підтвердження вашої ідентичності.

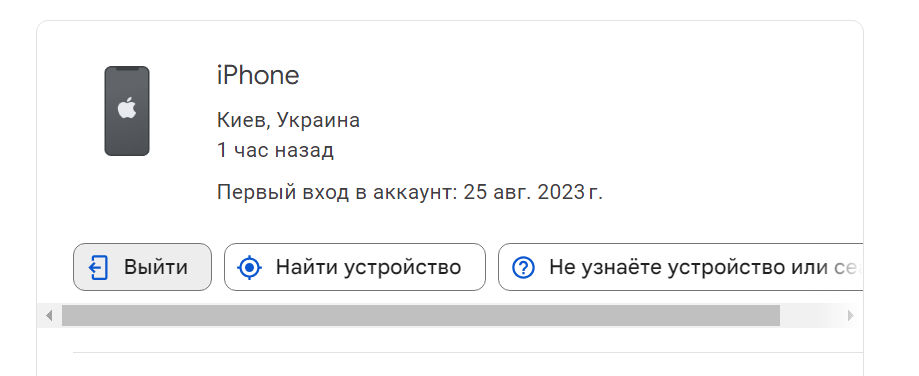
* 1. Що таке ключ безпеки і яку функцію він виконує? Чи можна використовувати ключ безпеки у кількох системах?

Ключ безпеки – це маленький ключ, який ви вставляєте в комп’ютер і натискаєте. Це надсилає зашифрований код на сервери Google, навіть не потрібно нічого вводити на екрані. Також можна використовувати один ключ безпеки для доступу до кількох систем, якщо ці системи підтримують стандартні протоколи аутентифікації, такі як TOTP (Time-Based One-Time Password) або FIDO U2F (Universal Second Factor).

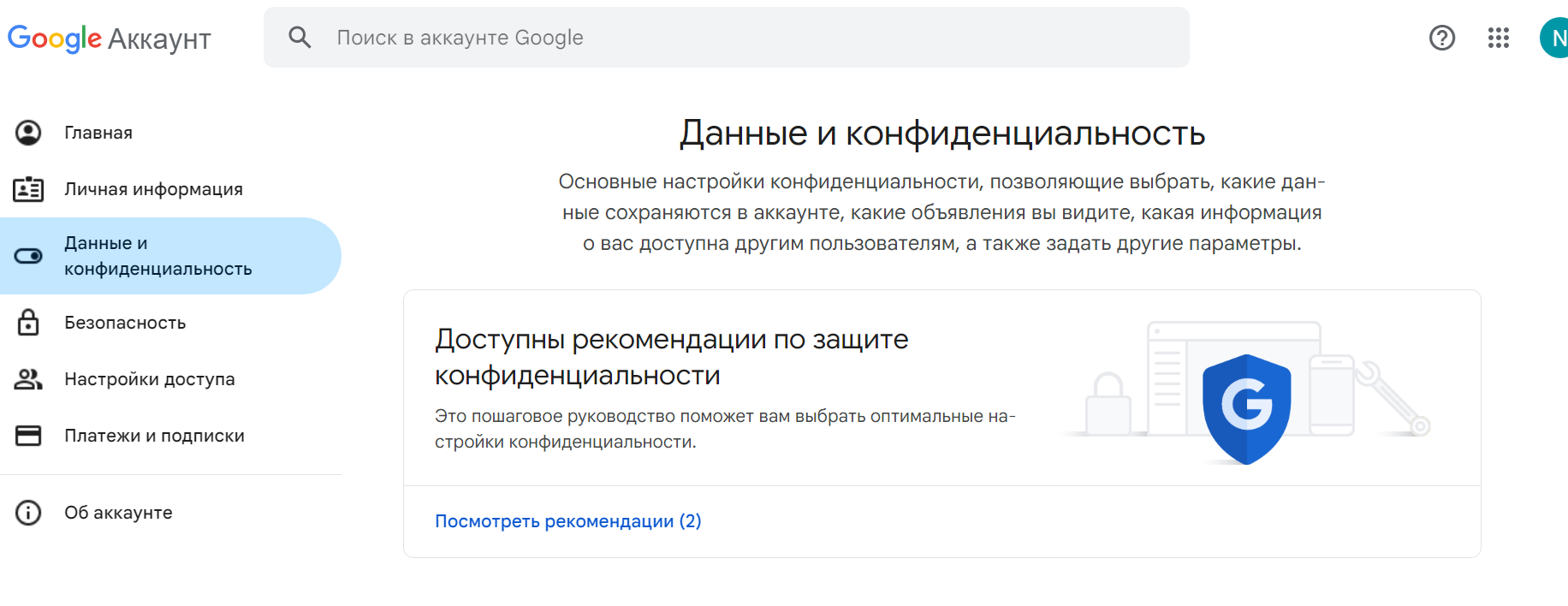
* 1. Якщо ви налаштували свій обліковий запис, щоб використовувати ключ безпеки, чи можете ви все ще входити в цей обліковий запис не маючи ключа безпеки?  
     Якщо ви не можете використовувати свій ключ безпеки, ви можете створити код безпеки для двоетапної перевірки. Також можна увійти за допомогою резервних кодів. Можливо є зареєстрований пристрій, який не попросить верифікації – можна зайти через нього в акаунт. Або звернутися до служби підтримки.

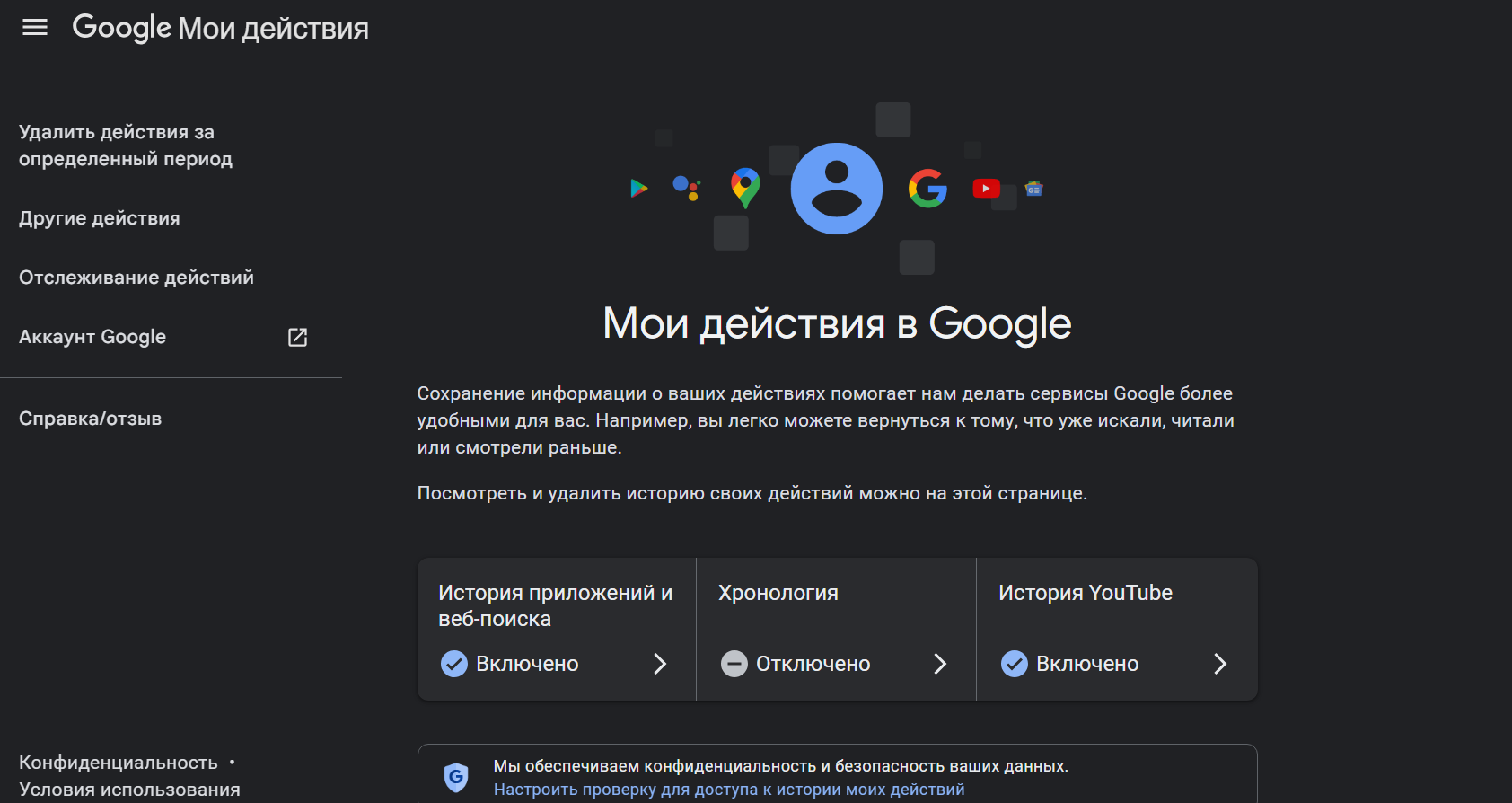
1. Захист доступу до облікового запису Gmail.
   1. Видаляємо неавторизованих користувачів облікового запису.



1. Перевірка активності облікового запису Gmail





Висновок: в ході виконання лабораторної роботи було переглянуто можливості функцій безпеки, які використовує Google. Було вивчено різноманітні заходи та сервіси для захисту конфіденційної інформації в онлайн-середовищі.