**ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ**

**КАФЕДРА ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

**Косиченко О.О., Махницький О.В.**

# Захист службової інформації під час використання електронної Web-пошти на основі асиметричного шифрування з відкритим ключем за допомогою програми Mailvelope


*МЕТОДИЧНІ РЕКОМЕНДАЦІЇ*

Дніпро - 2018

Рекомендовано до друку Науково-методичною радою Дніпропетровського державного університету внутрішніх справ (протокол № 8 від 11 листопада 2018 р.)

**Захист службової інформації під час використання електронної пошти на основі асиметричного шифрування з відкритим ключем. Методичні рекомендації**. – Косиченко О.О., Махницький О.В. – Дніпропетровський державний університет внутрішніх справ. – Дніпро, 2018 – 36 с.

Рецензенти:

**Власенко Ю.Є.** - доцент, кандидат технічних наук, доцент кафедри прикладної математики та інформаційних технологій ДВНЗ Придніпровська державна архітектурно-будівельна академія
**Коротенко Г.М.** - професор, доктор технічних наук, професор кафедри "Геоінформаційних систем" Національного технічного університету «Дніпровська політехніка»

Розраховано на курсантів, студентів, слухачів магістратури та слухачів підвищення кваліфікації, фахівців юристів та правоохоронців. Бібліогр. 6 назв.

**Автори:**

***Косиченко Олександр Олександрович*** – доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук, доцент

***Махницький Олександр Васильович*** – старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

**Зміст**

## 1. Вступ. Деякі загальні принципи інформаційної безпеки.

Уперше електронна пошта з'явилася в 1965 році й дотепер залишається одним з основних методів обміну інформацією. У сучасному світі існує дві основні системи шифрування (криптосистеми) – симетрична та асиметрична (система з відкритим ключем). У симетричних системах для шифрування й дешифрування використовується той же самий ключ. Іншими словами: щоб одержувач листа зміг розшифрувати зашифрований текст, він повинен знати ключ, яким його зашифрували. Така система шифрування може використовуватися тільки при повній довірі між усіма її учасниками. При цьому, у випадку росту кількості учасників листування прийдеться збільшувати й кількість ключів. Наприклад, ви листуєтеся з Остапом, Ольгою та Сергієм. Можна, звичайно, шифрувати всі повідомлення одним ключем, який будуть знати всі три адресати. Але це буде неправильно. Буде правильним створити окремі ключі (паролі) для кожного з адресатів. Коли адресатів усього троє, особливих проблем не виникне. Але, коли вам потрібно обмінюватися електронною поштою з десятками адресатів, запам'ятати всі ключі буде важко. Отже, така система шифрування зручна тільки при невеликій кількості адресатів.

Криптосистема з відкритим ключем є більш досконалою. У такій системі використовуються два ключі – відкритий і закритий, які математично зв'язано один з одним. Інформація ( тобто текст повідомлення) шифрується за допомогою відкритого ключа, який доступний усім бажаючим, а розшифрувати повідомлення можна тільки за допомогою закритого ключа, відомого тільки одержувачеві повідомлення. У цьому випадку ви можете роздати всім бажаючим ваш відкритий ключ, наприклад, опублікувати його на своєму сайті, щоб кожний міг написати вам зашифроване повідомлення, розшифрувати яке ви зможете тільки за допомогою вашого закритого (секретного) ключа, який знаєте тільки ви. Цей ключ ви нікуди не посилали й

ніколи його не потрібно куди-небудь посилати. Цей ключ ви повинні зберігати в таємниці.

Ваші електронні комунікації захищені на стільки, на скільки захищена сама слабка ділянка передачі або зберігання інформації.

Якщо ви користуєтеся "наверненою" зашифрованою поштою, а ваш співрозмовник – користується яким-небудь простеньким поштовим сервісом без усякого захисту, ваші листи будуть надходити в його поштову скриньку фактично по відкритому каналу. Організовуючи важливі службові або ділові комунікації, намагайтеся, щоб високий рівень захисту забезпечувався для всіх ділянок та учасників процесу. Це є один з головних фундаментальних принципів інформаційної безпеки.

Змарнувати зусилля по забезпеченню безпеки e-mail може один-єдиний аматор посилати конфіденційні дані у відкритому виді. Це стосується не тільки вмісту листів, але й так званих метаданих (метадані – це інформація про інформацію). Домовтеся зі своїми співрозмовниками про базові правила: яку інформацію всі ви згодні захищати і яким способом.

Суцільно та поруч пошта стає вразливою через недбале поводження людей до паролів. Приклад – запам'ятовування паролів у браузері. Зручно, однак якщо обладнання потрапить у чужі руки або буде мережеве втручання, зловмисник зможе легко зайти у вашу поштову скриньку. Ніколи не дозволяйте браузеру запам'ятовувати паролі, будьте уважні. Ми радимо дотримувати всіх правил відносно паролів. Прямо зараз задайте собі питання: як давно я міняв пароль до своєї електронної пошти? Змінюйте пароль хоч один раз на півріччя.

Захист e-mail можна зробити даремним, усього лише включивши тимчасову переадресацію на іншу, менш захищену поштову скриньку. Ще одна розповсюджена уразливість – потенційна можливість відновити доступ до поштового аккаунту через інший (ненадійний) акаунт, номер мобільного

телефону, відповідь на "секретне питання". Перевірте настроювання й переконаєтеся, що нічого такого у вас немає.

У деяких людей існує звичка зберігати електронні листи із захищеної поштової скриньки у відкритому виді на диску свого комп'ютера (або на змінних носіях). Шкідлива звичка, позбудьтеся її. Якщо потрібно зберігати листа на комп'ютері, використовуйте шифрування, наприклад за допомогою програми Veracrypt або подібної. Радимо не перетворювати вашу поштову скриньку на сервері в особистий архів e-mail. Ви, строго говорячи, не контролюєте сервер, і якщо зловмисник добереться до вашого аккаунту, він може одержати доступ не тільки до останнього листування, але й архіву пошти за кілька років.

## Обробка спама

Видалося б, що ще ми *не* знаємо про спам? Найважливіше: як з ним управляється конкретний поштовий провайдер. Ми не говоримо про ті повідомлення, які (справедливо або помилково) фільтруються в папку "Спам"; ми говоримо про ті листи, які навіть не попадають у наші поштові скриньки, тому що антиспамерский фільтр провайдера порахував ці листи як сміття. Уникайте провайдерів, що використовують для цих цілей зовнішні "чорні списки", які самі провайдери навіть не контролюють. Віднесіть із обережністю до сервісів, які застосовують незрозумілу для вас техніку фільтрації та не пояснюють, як це відбувається. Якщо в поштовому сервісі без повідомлення пропадають листа, що не є спамом, про надійність говорити не можна.

## Шифрування e-mail

Шифрування e-mail використовується, звичайно, не тільки для захисту від надто допитливого провайдера, але й для забезпечення конфіденційності листування в цілому. Шифрування може забезпечуватися:

- Поштовим провайдером. У цьому випадку провайдер надає відповідну послугу ( про що, звичайно, не забуде розповісти на своєму веб-сайті). Переважніше сервіс із наскрізним шифруванням. У деяких випадках

шифрування, забезпечуване провайдером, може виявитися зручним варіантом. Наприклад, якщо потрібно налагодити листування з адресатами, у принципі не схильними встановлювати/освоювати які-небудь програмні засоби захисту.

- Самим користувачем. Ви шифруєте повідомлення на своєму комп'ютері перед тем, як відправити по електронній пошті. Це більш універсальний спосіб, а якщо для шифрування вибрати який-небудь популярний стандарт (наприклад, Openpgp), ви зумієте зберегти гнучкість підходу: учасники листування зможуть самі вибирати шифрувальні засоби, що використовують цей стандарт.

Слід також знати, що саме по собі використання шифрування в деяких державах якщо і не є протизаконним, але здатне провокувати зайву увагу з боку спецслужб. Перед тем, як налагоджувати зашифроване листування з колегами/друзями з інших країн, з'ясуєте, наскільки це буде для них соціально безпечно.

При виборі сервісу електронної пошти є сенс звернути увагу також на популярність сервісу, готовність технічної підтримки прийти на допомогу й відкликання користувачів. Як бачите, умов багато, і навіть саму *захищену* пошту можна двома клацаннями миші зробити безпомічної перед звичайним зломщиком. Проте, одна пошта може бути більш безпечна, ніж інша, тому треба пам’ятати декілька порад:

- Якою би поштою ви не користувалися, є сенс пройти по зазначених вище пунктах і перевірити, чи все буде нормально.
- Поштовий сервіс Gmail є одним із самих популярних і освоєних. Якщо ваш нинішній поштовий акаунт у сумнівній юрисдикції, перехід на Gmail не розв'яже всіх проблем, але виразно стане кроком уперед.
- У загальному випадку наскрізне шифрування e-mail дозволяє забезпечити конфіденційність листування, навіть якщо поштовий сервіс і практика роботи з поштою не відповідають усім переліченим вище умовам.

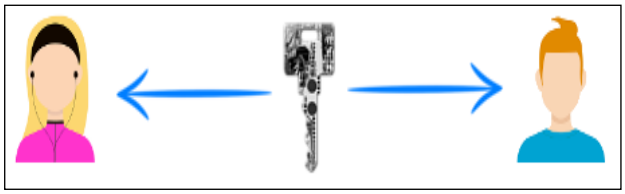
## 2. Mailvelope: шифрування електронної пошти

Mailvelope – це програмне доповнення ("плагін") до браузерів Google Chrome або Mozilla Firefox для шифрування Web-mail.

В основі роботи Mailvelope лежить принцип асиметричного шифрування з відкритим ключем. З початку ми розберемо основні загальні принципи шифрування.

### 2.1. Звичайне (симетричне) шифрування.

Остап та Ганна вирішили захистити своє службове листування по Web-mail за допомогою шифрування. Щоб зашифрувати лист, Ганна використовує спеціальний код – шифрувальний ключ. Зашифрований лист може бути прочитано тільки той людиною, у який є цей ключ. Тому перед тем, як починати листування, в обох наших друзів повинен бути цей ключ.



Якщо Ганна та Остап працюють у різних містах і не можуть зустрітися, хтось із них (наприклад, Ганна) створює ключ і відправляє його співрозмовникові – Остапу по Інтернету.

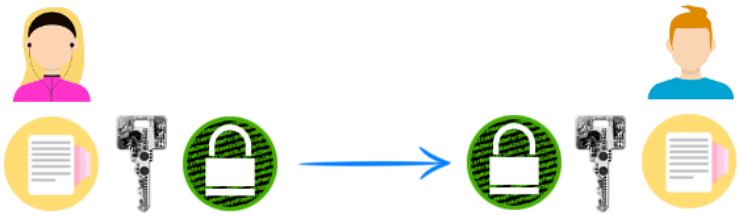
Тепер Ганна може:

- скласти лист,
- зашифрувати його за допомогою ключа,
- відправити шифровку Остапу.

Остап:

- одержить шифровку,
- розшифрує її за допомогою того ж ключа,
- прочитає лист Ганни.

От так:

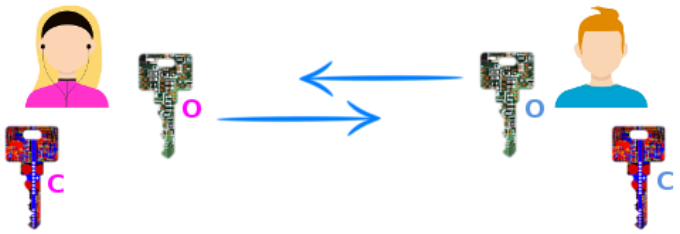


Представимо, що в плани друзів втручається хакер-лиходій Захар. У нього є технічні можливості перехоплювати будь-які дані, які Ганна й Остап посилають один одному. Фахівці з інформаційної безпеки називають такий вид втручання "людина усередині" *(man-in-the-middle - MITM).* Якщо Ганна відправить Остапу шифрувальний ключ по e-mail, Захар його скопіює. Потім Захар скопіює й шифровку. Ніщо не може перешкодити йому читати все зашифроване листування.

## 2.2. Асиметричне шифрування (з відкритим ключем)

Щоб перешкодити втручанню лиходія Захара, Ганна ( за допомогою спеціальної програми) створює **не один, а два ключі**. Ці ключі унікальні, парні та мають особливість: **те, що зашифровано одним ключем, може бути розшифроване тільки парним йому ключем**. Назвемо один із ключів секретним (С), а інший - відкритим ( В). Те ж саме на своєму комп'ютері зробить Остап. У нього теж з'явиться унікальна пара ключів.

Свої секретні ключі Ганна та Остап захистять надійними паролями й будуть тримати кожний при собі. Відкритими ключами друзі обміняються – прямо по e-mail, а може бути, навіть розмістять їх на сервері в Інтернеті (є спеціальні сервери ключів).

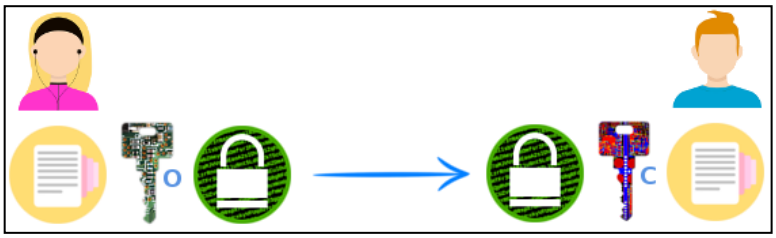



Щоб написати Остапу, Ганні потрібно:

- скласти лист,
- зашифрувати його за допомогою відкритого ключа Остапа,
- відправити шифровку Остапу.

Остап:

- одержить шифровку,
- розшифрує її за допомогою свого секретного ключа (єдиного ключа у світі, який це дозволить),
- прочитає лист Ганни.




От як це виглядає:

Свою відповідь Остап зашифрує відкритим ключем Ганни. Одержавши шифровку, Ганна розшифрує її своїм секретним ключем.

Що може лиходій  Захар? Він може перехоплювати відкриті ключі Ганни та Остапа, а також усі шифровані листи, але ніякої користі це не принесе йому: відкриті ключі ні як не годяться для розшифрування листів.

Ця  схема дозволяє не тільки надійно захистити листування між співрозмовниками: кожний з них може в будь-який момент створити нову пару ключів, якщо колишня пара загублена або є якийсь сумніви.

Шифрування з відкритим ключем у цивільній сфері одержало широке поширення завдяки зусиллям американського програміста Філа Циммермана і його однодумців. Створена Циммерманом програма називається PGP (Pretty Good Privacy). Далі  була розроблена безкоштовна програма з відкритим кодом Gnupg, і сьогодні багато програм і мобільних додатків використовують стандарт Open pgp.

Якщо ви тільки починаєте шифрування e-mail, спробуйте Mailvelope. Це програмне доповнення до браузерів (Google Chrome, Mozilla Firefox). Mailvelope призначений тільки для Web-пошти. Неважливо, які поштові провайдери у вас і у вашого адресата. Ви можете використовувати ті адреси, до яких звикли. Mailvelope дозволяє шифрувати й розшифровувати зміст електронних листів і файли, які потім можна відправляти як вкладення.

Для зашифрованого спілкування ваш співрозмовник може користуватися Mailvelope або будь-якою іншою програмою на основі PGP/Gnupg. Mailvelope – програмне доповнення до браузера (Google Chrome, Mozilla Firefox) і призначений для веб-пошти.

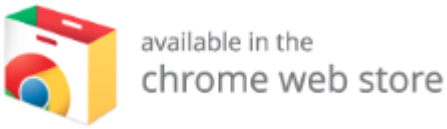
## 3. Установка та використання програмного додатку Mailvelope

1. Запустіть браузер.

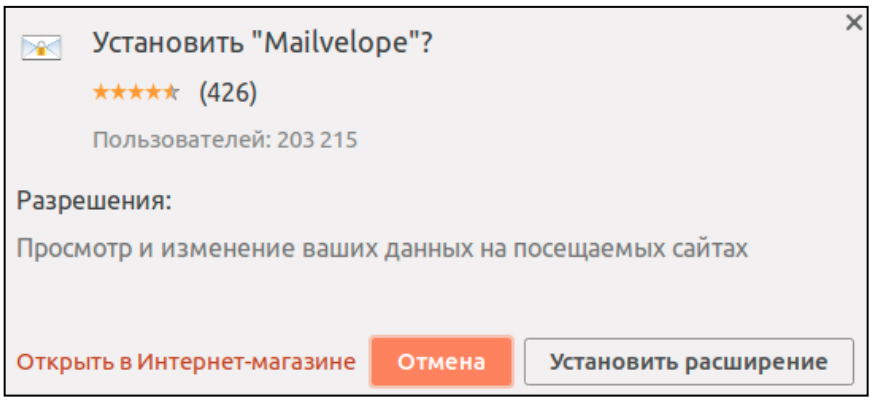
2. Зайдіть на сайт розробника Mailvelope (**https://www.mailvelope.com/**).

Якщо у вас Google Chrome (якщо у вас Firefox, див. нижче):

3. Прокрутите униз, знайдіть на сторінці заголовок "Chrome Extension" і натисніть кнопку "**available in the chrome web store**".




4. З'явиться спливаюче вікно із запитом. Натисніть кнопку "**Установить расширение**".



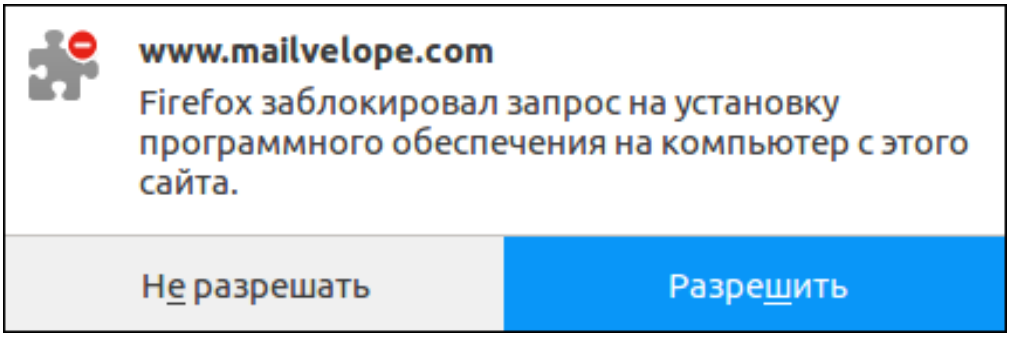

5. Розширення встановлене. У правому верхньому куті браузера Chrome ви

побачите маленький замочок – значок Mailvelope.

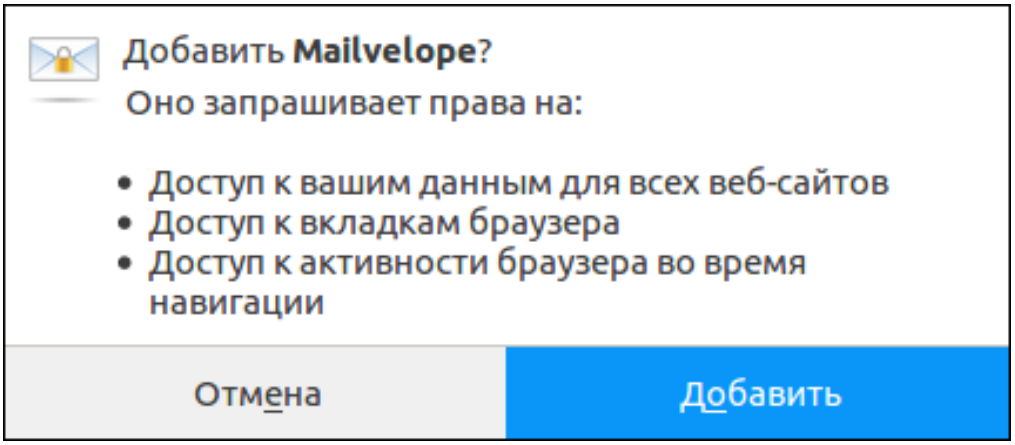
Якщо у вас Mozilla Firefox:

3. Прокрутите униз, знайдіть на сторінці заголовок "Firefox Addon" і натисніть кнопку "Get the add-on".


4. Ви можете побачити попередження браузера, який заблокував автоматичну установку з незнайомого йому сайту. Натисніть кнопку “**Разрешить**”.




5. Доповнення Firefox буде скачано, і з'явиться ще один запит від браузера; потрібно погодитися.




6. Розширення встановлене. У правому верхньому куті браузера Firefox ви побачите маленький замочок – значок Mailvelope.

## 4. Інтеграція Mailvelope у систему веб-пошти.

Mailvelope за замовчуванням інтегрується з деякими поштовими сервісами, включаючи популярний Gmail. Ви можете використовувати Mailvelope і в іншій веб-пошті.

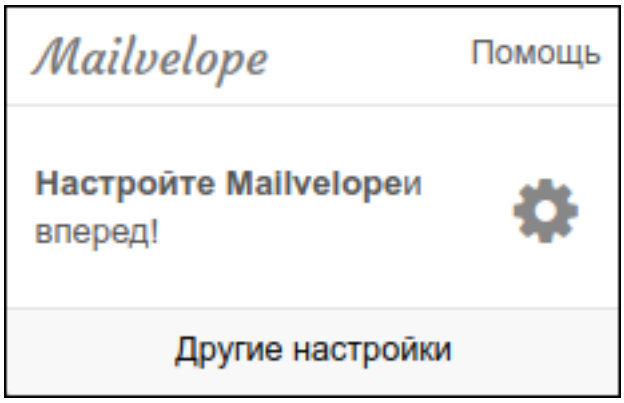
1. Відкрийте свою звичну сторінку веб-пошти для написання нового повідомлення й зверніть увагу на правий верхній кут вікна редактора (поле, у

якім ви звичайно пишете текст свого листа). Бачите кнопку Mailvelope – от таку?

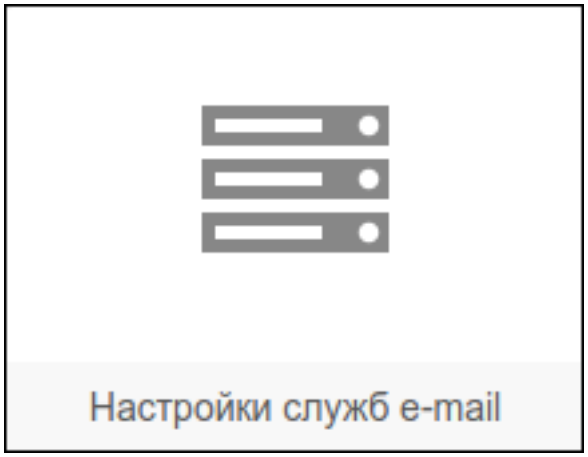
Якщо кнопка видна, Mailvelope інтегрований у вашу веб-пошту за замовчуванням. Нічого робити не потрібно. Можете перейти до пункту **5. Створення пари шифрувальних ключів**

Якщо кнопки немає:

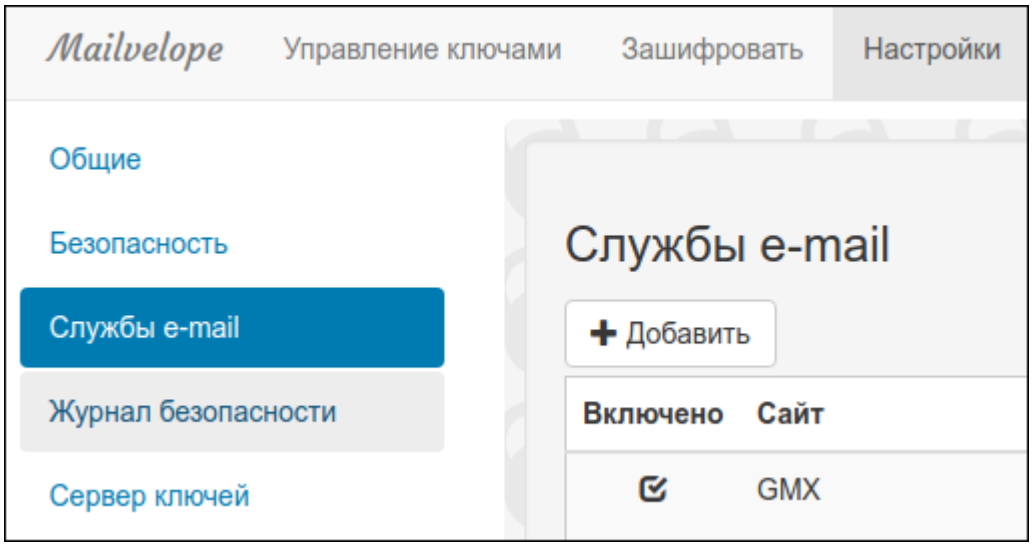
2. Натисніть кнопку Mailvelope у панелі браузера. З'явиться початкове меню.




3. Натисніть “Інші налаштування". На сторінці, що відкрився, виберіть пункт "Настройки служб e-mail".

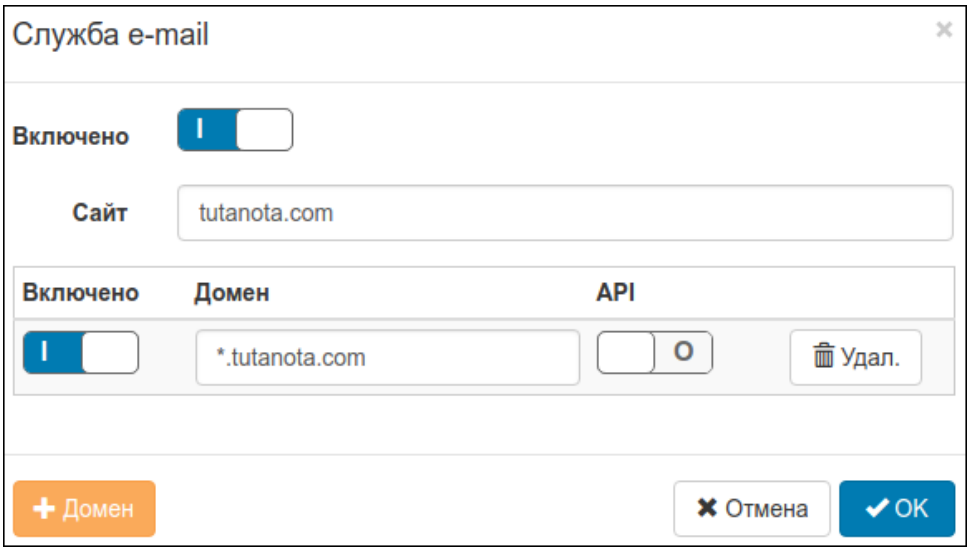



4. У лівому стовпці висвітиться пункт "Служби e-mail", а праворуч з'явиться список підтримуваних за замовчуванням провайдерів e-mail.




Натисніть кнопку "+ **Добавить**".

5. Відкриється вікно з формою додавання сайту. Уведіть у поле "Сайт" назву вашого поштового провайдера (формат не має значення), а в поле "Домен" – ваш поштовий домен з маскою "*.", як на малюнку. Натисніть кнопку "ОК". Ваш поштовий провайдер буде доданий в Mailvelope, і в редакторі e-mail з'явиться потрібна кнопка.



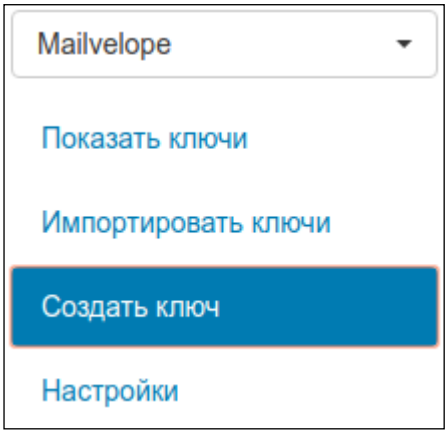

## 5. Створення пари шифрувальних ключів

Щоб користуватися шифруванням, спочатку потрібно створити власну пару ключів.

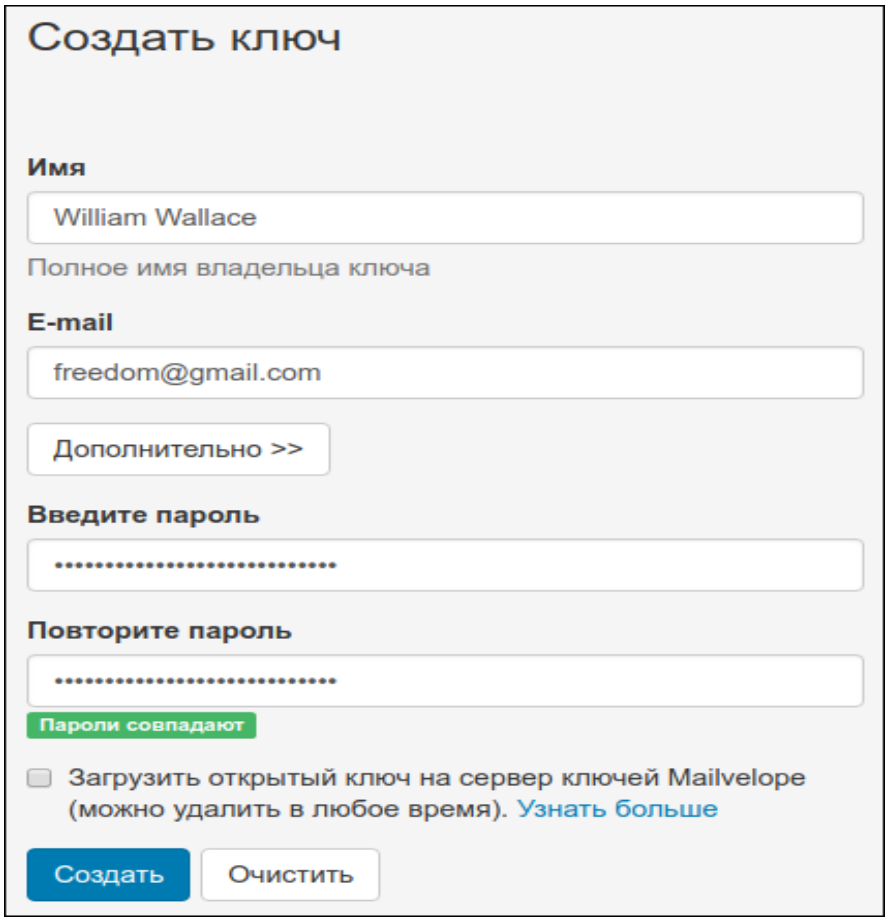
1. Натисніть кнопку Mailvelope у панелі браузера.

2. Натисніть "Настройте Mailvelope и вперед!". Відкриється головне вікно настроювань Mailvelope.

3. У меню ліворуч виберіть “Создать ключ” (синяя кнопка "Создать ключ" кнопка в правій частині веде туди ж).

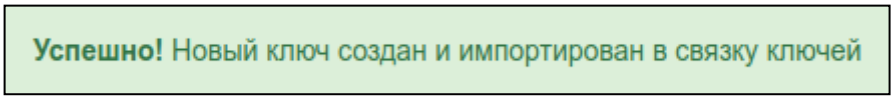



4. Заповните форму й натисніть кнопку "Створити".

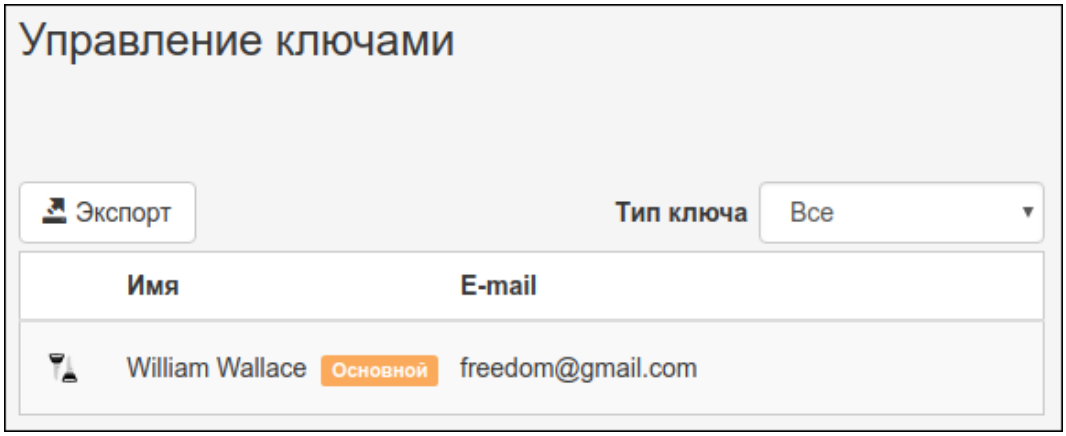


- **Ім'я.** Указуючи справжнє ім'я, ви допомагаєте адресатам визначити, чий це ключ. Так їм легше буде вибирати потрібний ключ для зв'язку з вами. Якщо ви не бажаєте вказувати своє справжнє ім'я, можете придумати псевдонім, але помніть: вашому співрозмовникові прийде тримати в пам'яті, що “Baba Yaga” – це ви. Не всяка пам'ять упорається із цим завданням. Який би варіант ви не вибрали, уводите текст англійською мовою, оскільки дотепер існують програми, що не цілком точно відображають кирилицю, і не виключене, що хто-небудь із адресатів користується саме такою програмою.
- **Адреса e-mail.** Краще вводити реальну адресу e-mail, оскільки багато шифрувальних програм (включаючи Mailvelope) використовують його для "упізнання" ключів.
- Кнопку **“Дополнительно”** можна пропустити.
- Уведіть **пароль.** Це повинен бути гарний пароль. Він буде захищати ваш секретний ключ і знадобиться при розшифруванні повідомлень. Запам'ятаєте цей пароль (або збережіть в надійному місці, наприклад, у програмному менеджері паролів Keepassxc).
- Повторите пароль. Уведені паролі повинні збігатися.
- Заберіть галочку з поля “**Загрузите открытый ключ на сервер ключей Mailvelope**…”
- Натисніть кнопку “**Создать**”.

5. По закінченню створення ключів ви побачите повідомлення про успішне створення/імпорт (на ясно-зеленім тлі).



Щоб побачити тільки що створений ключ у списку (зв'язці) ключів, натисніть у лівому меню “**Показать ключи**”. Відкриється вікно “**Управление ключами**”.



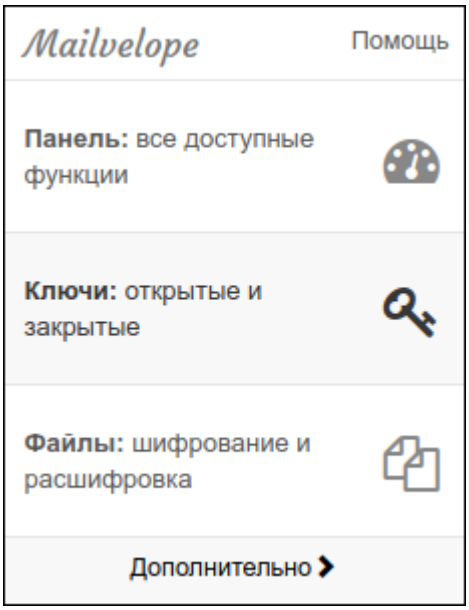

Пара ключиків ліворуч від імені означає, що є присутнім парний секретний ключ. Напис "**Основной**" поруч із іменем – означає що ця пара ключів буде використана за замовчуванням (у принципі, ніщо не заважає вам створити й використовувати декількох пар ключів).

## 6. Експорт відкритого ключа

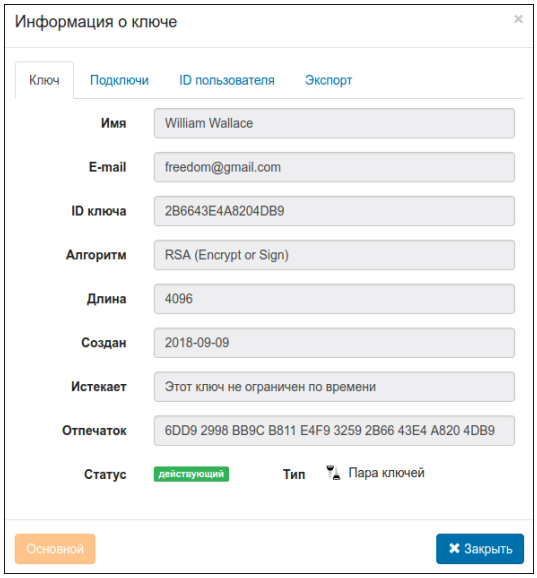
Потрібно експортувати відкритий ключ і поділитися їм із друзями, щоб вони змогли відправляти вам свої зашифровані листи.

1. Натисніть на значок Mailvelope у панелі браузера.

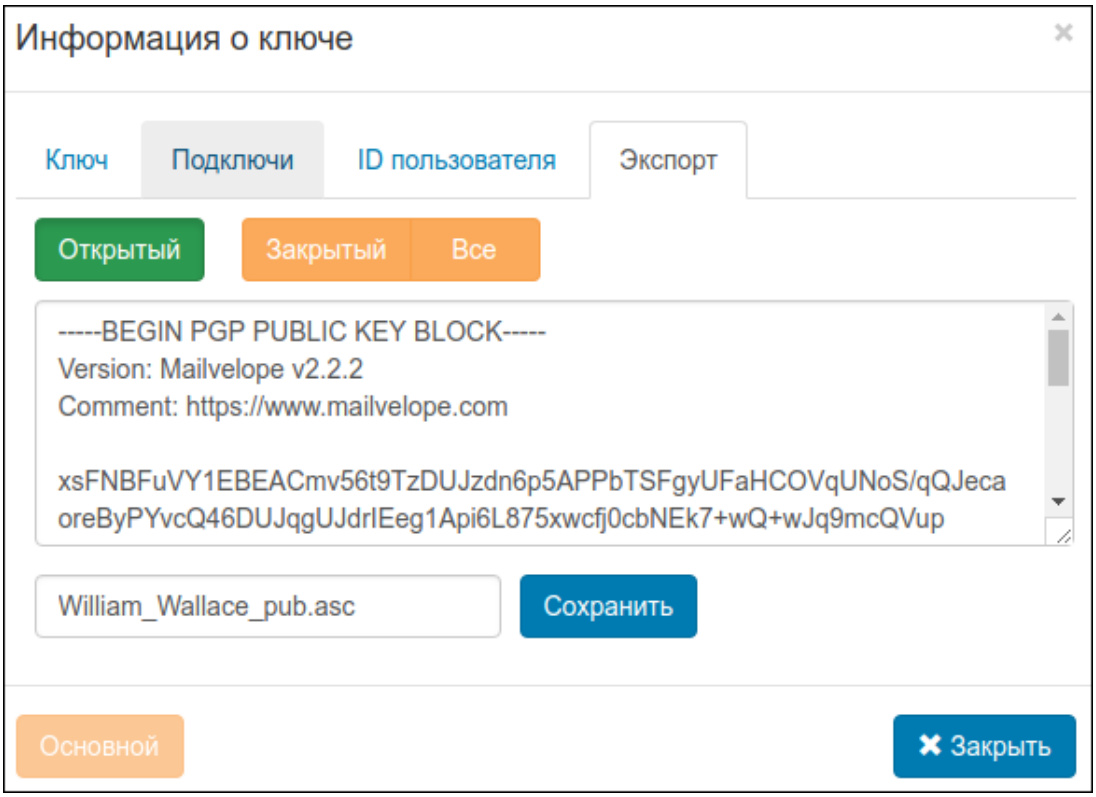
2. У головному меню Mailvelope виберіть "**Ключи**: открытые и закрытые".




3. Виберіть у списку (зв'язці ключів) потрібний ключ (у нашому прикладі ключ поки всього один). Ви побачите вікно з докладною інформацією про ключ.




4. Натисніть вкладку “Экспорт”:




За замовчуванням обрана опція “**Открытый**” (зеленого кольору): ви експортуєте тільки відкритий ключ. Так і повинне бути. Про це також нагадує суфікс "**_pub**" ("public") у імені файлу з розширенням .asc.

5. Натисніть кнопку “**Сохранить**” і збережіть файл на диску. Натисніть кнопку “**Закрыть**”.

Збережений файл містить ваш відкритий шифрувальний ключ. Відправте його (наприклад, звичайним вкладенням e-mail) тому, з ким збираєтеся листуватися.

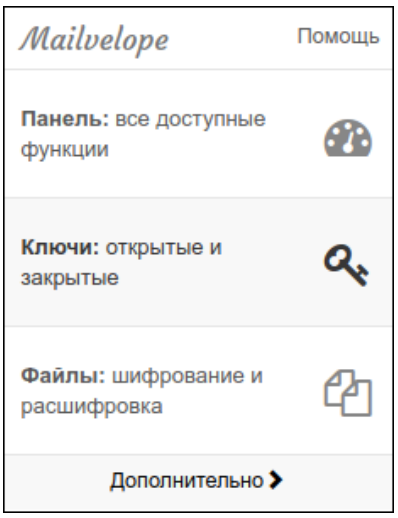
## 7. Імпорт відкритого ключа співрозмовника.

Перед початком листування потрібно одержати та імпортувати відкриті ключі друзів і колег. Тоді ви зможете посилати їм зашифровані листи.

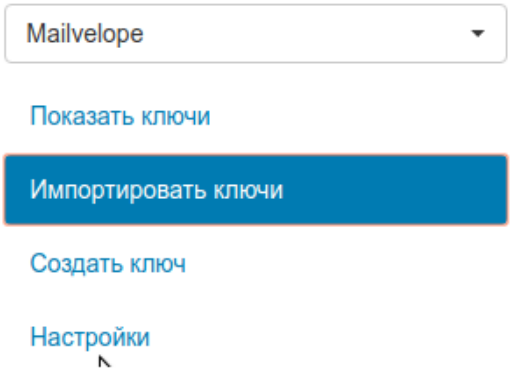
1. Попросите співрозмовника надіслати вам відкритий ключ.

2. Натисніть на значок Mailvelope у панелі браузера.

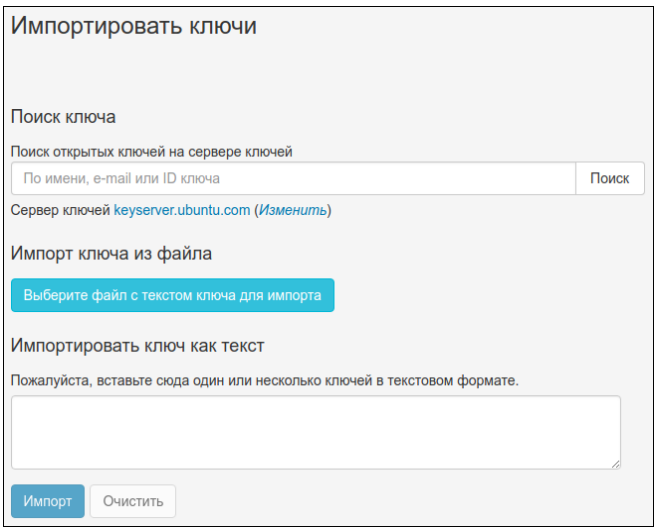
3. У головному меню Mailvelope виберіть "**Ключи: открытые и закрытые**".



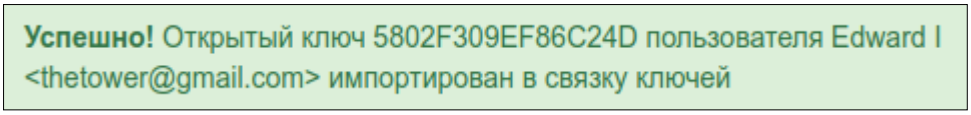

4. Виберіть у стовпці ліворуч пункт “**Импортировать ключи**”.



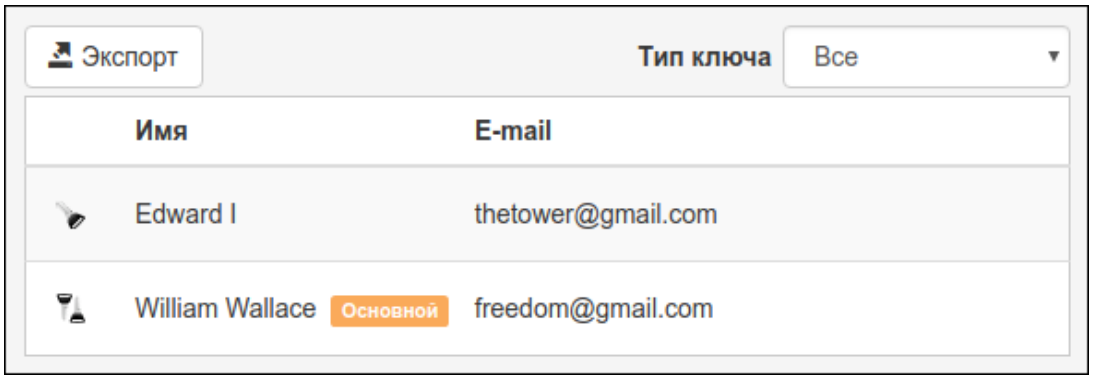

З'явиться вікно імпорту.




5. Натисніть довгу кнопку “**Выберите файл с текстом ключа для импорта**” і виберіть на диску присланий вам файл. Якщо із ключем усе в порядку, ви повинні побачити повідомлення:




Тепер натисніть у лівому стовпці “**Показать ключи**”. Переконайтеся, що присланий вам ключ перебуває в списку (зв'язці).



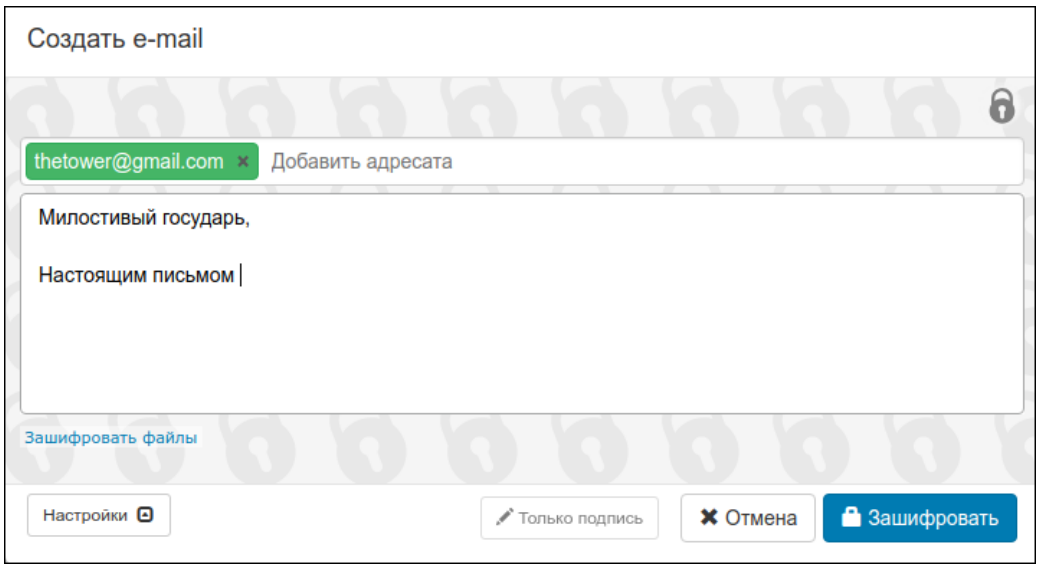

Зверніть увагу на різницю між ключами: створений вами ключ має значок із двома ключиками. Це пари ключів, відкритий і секретний. На значку присланого ключа – лише один ключик. Цей ключ – відкритий.

## 8. Шифрування електронних листів.

Спробуємо зашифрувати електронний лист.

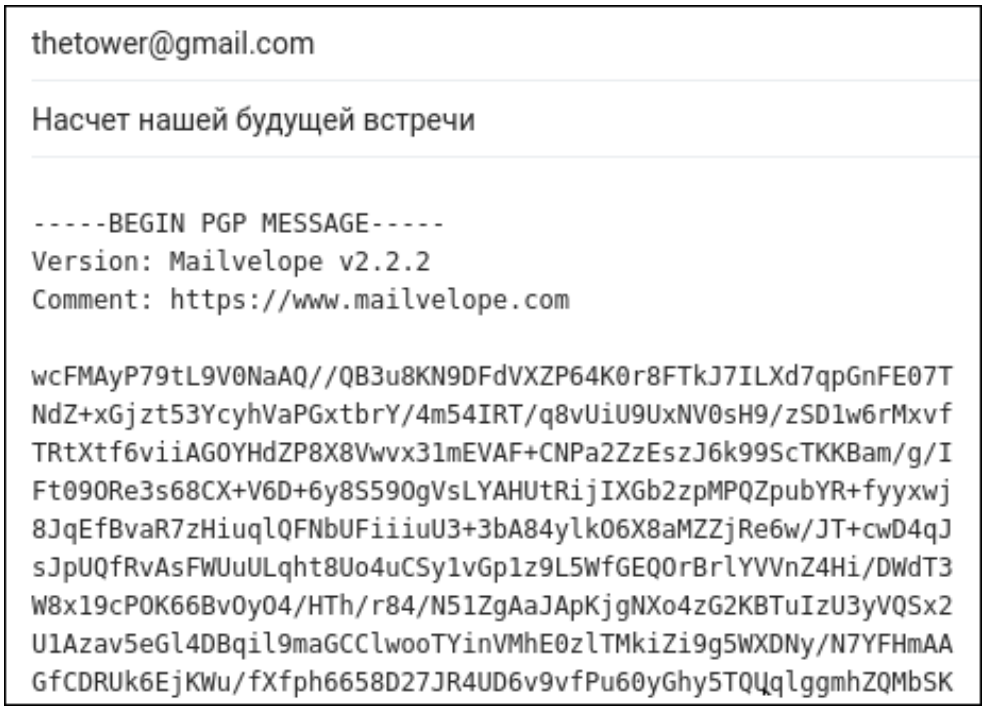
1. Відкрийте веб-пошту, щоб написати нове повідомлення.
2. Заповните поля “Кому” і “Тема”, як звичайно.
3. Натисніть кнопку Mailvelope у правому верхньому куті редактора.

4. Відкриється вікно редактора Mailvelope. Наберіть адресу вашого співрозмовника у верхньому полі. (У даному прикладі це *thetower@gmail.com*). Як тільки ви почнете це робити, Mailvelope запропонує варіанти часткових збігів, так що ви зможете вибрати адресу зі списку, не прийдеться набирати його повністю. Помніть: Mailvelope може запропонувати шифрування тільки тім одержувачам, чиї ключі були раніше імпортовані й перебувають у вашому зв'язуванні ключів.




При необхідності можете вказати відразу декількох адресатів. Ваше повідомлення буде зашифровано декількома ключами.

5. Коли закінчите писати повідомлення, натисніть кнопку “Зашифровать”. У вікні редактора вашої веб-пошти з'явиться зашифроване повідомлення.



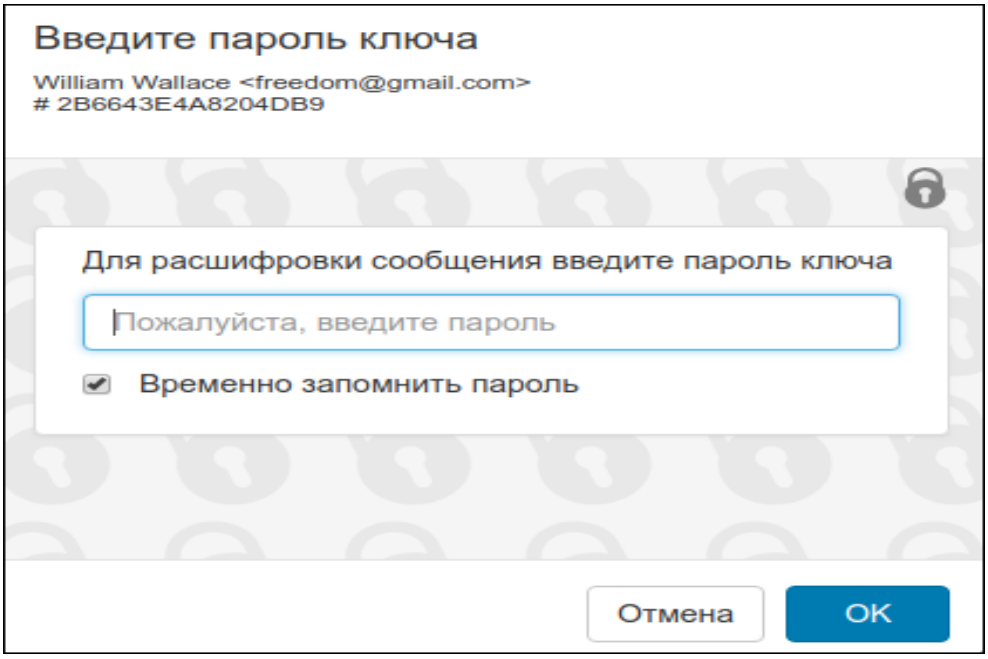

6. Натисніть кнопку відправлення повідомлення.

## 9. Розшифрування електронних листів

Зашифрований лист, який надійшов вам на пошту, виглядає як сторонній набор символів.

1. Відкрийте цей лист у своїй веб-пошті. При перегляді в редакторі ви побачите поверх абракадабри значок іконка конвертик Mailvelope:


2. Натисніть на значок. У вікні, що відкрилося, уведіть пароль до свого секретного ключа й натисніть кнопку “ОК”.




3. Розшифроване повідомлення буде показано у вікні редактора.

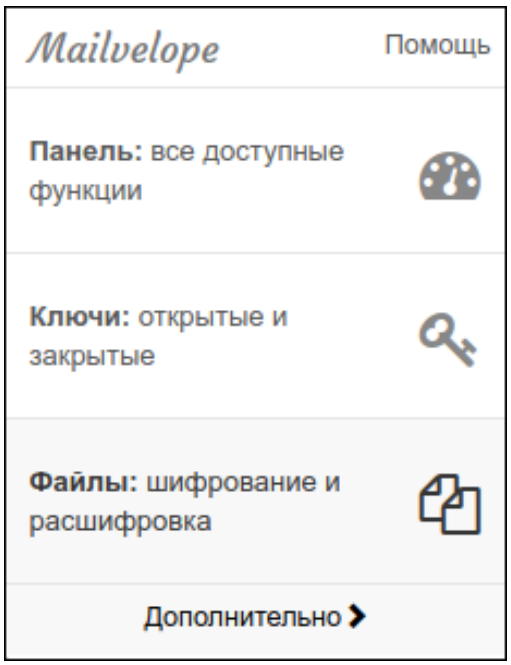
Зверніть увагу: саме по собі розшифрування не створює нових копій повідомлення. Якщо ви перейдете до іншого листа або закриєте інтерфейс веб-пошти, зашифроване повідомлення так і залишиться зашифрованим. Щоб знову побачити його зміст, потрібно повторити розшифрування.

Mailvelope запам'ятовує пароль до вашого секретного ключа на короткий час (за замовчуванням 30 хвилин, але можна змінити в настроюваннях Mailvelope). Це зручно, якщо вам доводиться переглядати підряд кілька зашифрованих листів. Але якщо ви зберігаєте цю можливість, не залишайте свій комп'ютер без догляду й без захисту, поки Mailvelope тримає ключ у своїй пам'яті, інакше випадкова людина зможе прочитати вашу зашифровану листування.

**10. Шифрування файлів**

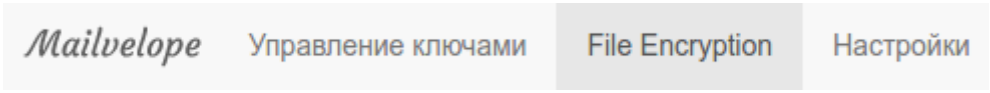
По де куди виникає завдання відправити конфіденційний документ, який не є простим текстом – наприклад, презентацію, електронну таблицю, файл PDF або фотографію. Mailvelope уміє шифрувати файли.

1. Натисніть на значок Mailvelope у панелі браузера.

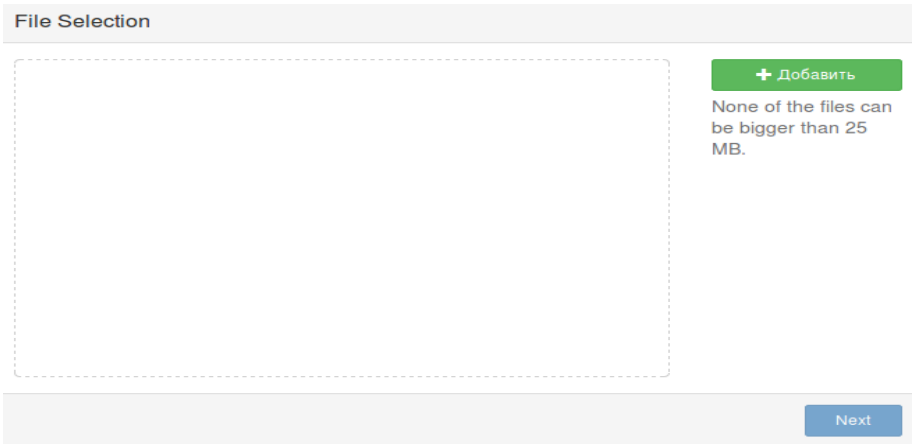



2. У головному меню Mailvelope виберіть пункт "Файли: шифрування й розшифрування".

3. У верхньому горизонтальному меню натисніть “File Encryption”.



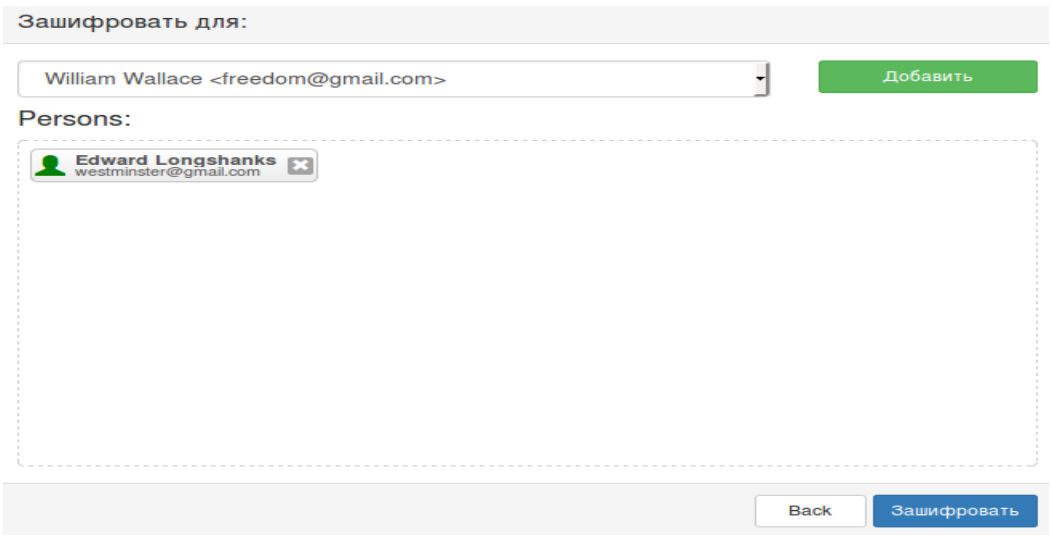
Відкриється вікно для роботи з файлами.



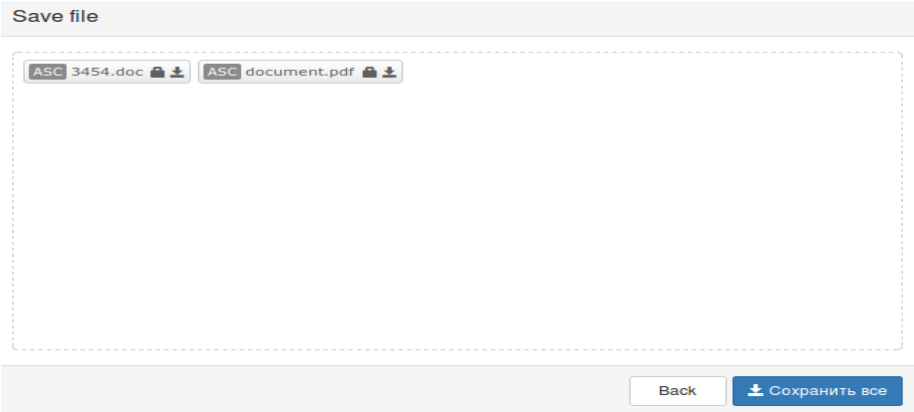

4. Натисніть зелену кнопку “Додати”. При необхідності можете додати кілька файлів.


5. Натисніть кнопку “Next”.

6. Виберіть ключ адресата, кому збираєтеся відправити зашифровані файли. Як і для текстових повідомлень, ви можете вибрати кілька ключів.




7. Натисніть кнопку “Зашифрувати”.




8. Натисніть кнопку “Зберегти всі”, щоб зберегти зашифровані файли на диску. Імена файлів залишаться колишніми, але додасться розширення .asc.

9. Після збереження можна закрити вкладку Mailvelope.

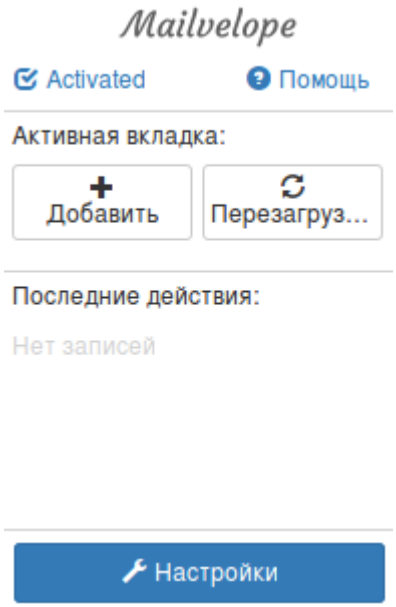
10. Прикріпите зашифровані файли до вашого листа в якості вкладень ( як ви це робите звичайно) і відправте одержувачеві.

**11. Розшифрування файлів**

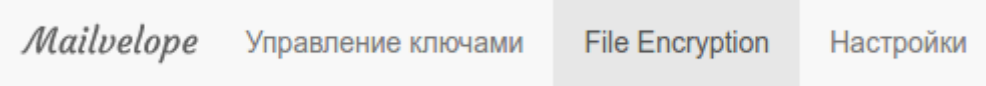
1. Збережіть отриманий вами зашифрований файл (за замовчуванням він має розширення .asc) у папку на диску.

2. Натисніть на значок Mailvelope у панелі браузера.

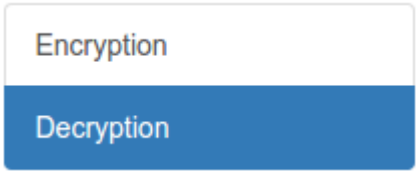
3. Натисніть кнопку “Настроювання” у меню, що випадає.



4. У верхньому горизонтальному меню натисніть “File Encryption”.




5. У лівому стовпці виберіть “Decryption”.




6. Натисніть зелену кнопку “Додати” і виберіть файл, який потрібно розшифрувати. Натисніть кнопку “Next”.


7. У вікні, що відкрилося, уведіть пароль до свого секретного ключа й натисніть кнопку “OK”.


8. Розшифрований файл поміщений у вікно Mailvelope. Натисніть кнопку “Зберегти всі” і збережете файл на диск.

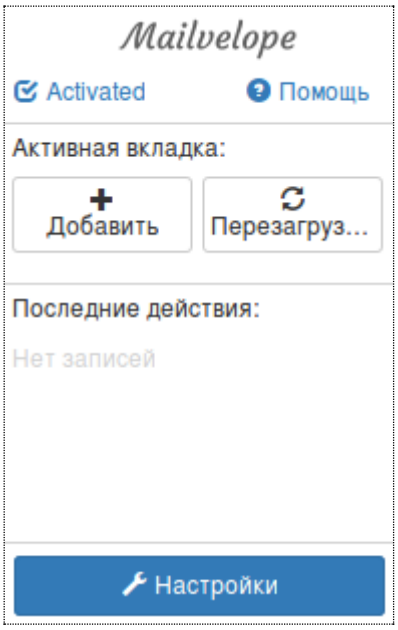
## 12. Створення резервної копії зв'язаних ключів

Одна з найпоширеніших помилок – втрата ключів. Причиною може бути непоправний вихід з ладу жорсткого диска комп'ютера, випадкове форматування, крадіжка або вилучення ноутбука. Буває, що людей відправляється в поїздку й забуває свої ключі на робочому комп'ютері. Втрата ключів порівнянна із втратою адресної книги. Втрата власного секретного ключа приведе до того, що ви не зможете прочитати усе раніше отримані вами зашифровані повідомлення. Крім того, ваш секретний ключ виявиться скомпрометований, його знадобиться терміново замінити новим.

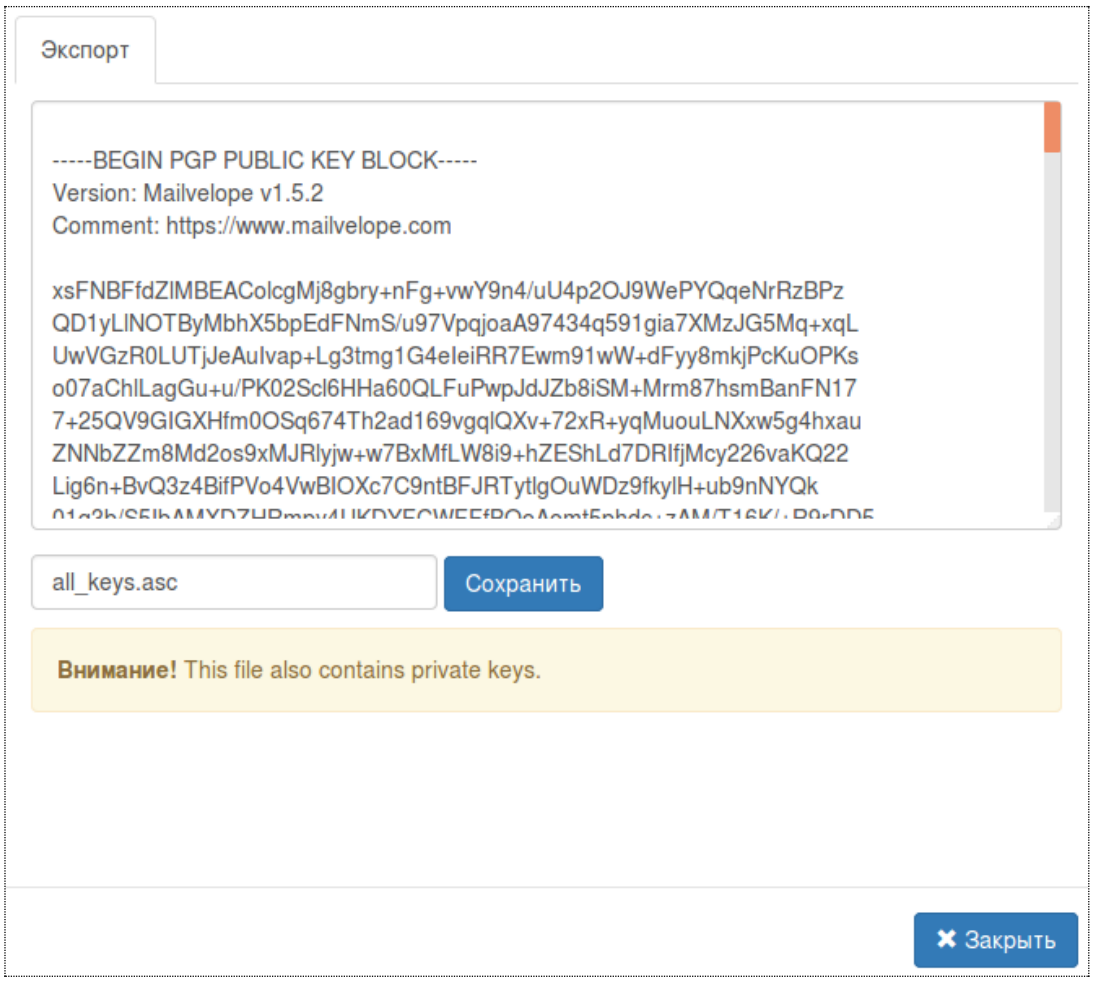
Ключі можна експортувати поодинці, як описано вище, але Mailvelope дозволяє виконати експорт усього зв'язування ключів. Ми рекомендуємо робити резервні копії вашої зв'язки ключів періодично, щоб ураховувати відновлення.

1. Натисніть на значок Mailvelope у панелі браузера.

2. Натисніть кнопку “Настроювання” у меню, що випадає.




3. Натисніть кнопку “Експорт” (над списком ключів). Відкриється вікно, у якім усе готове для експорту. Зверніть увагу: ви експортуєте всі ключі у вашому зв'язуванні, включаючи свій секретний ключ.




4. Натисніть кнопку “Зберегти” і збережете файл із ключами на диску.

**13. Верифікація (перевірка) ключа**

Повернемося до Ганни та Остапу. Представте, що лиходій Захар створив пару ключів і, перехопивши відкритий ключ Остапа, підсунув замість нього свій власний відкритий ключ. Є ризик, що Ганна, не помітивши підміни, почне шифрувати листа відкритим ключем Захара, думаючи, що це ключ Остапа. У такий спосіб Захар одержить доступ до зашифрованого листування.

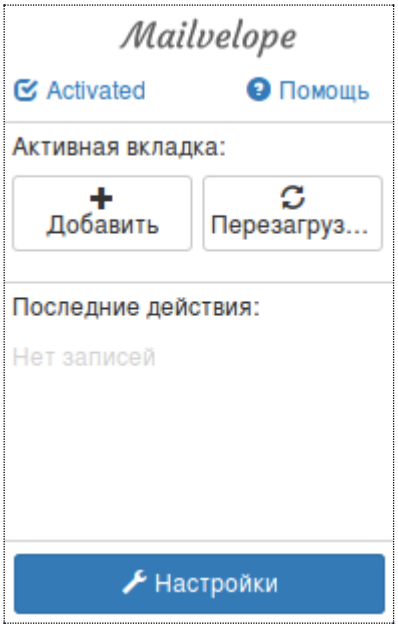
Щоб цього уникнути, використовується верифікація (перевірка дійсності) ключів.

Кожний шифрувальний ключ має "відбиток" – унікальний код, послідовність знаків. Відбитки використовують при верифікації.

1. Зв'яжіться зі своїм адресатом по іншому каналу (наприклад, у захищеному чаті Viber або іншому). Важливо, щоб цей канал був якісно іншим, а ви могли бути впевнені, що розмовляєте саме з вашим респондентом. (Наприклад, по голосу або відео).

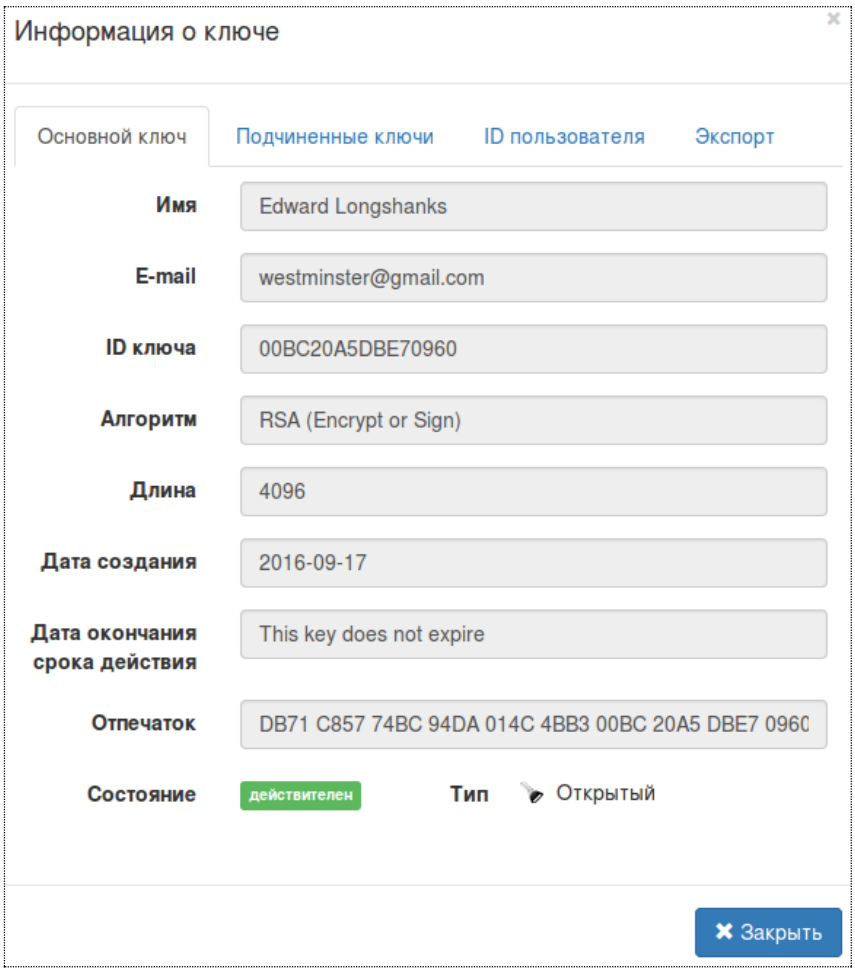
2. Натисніть на значок Mailvelope у панелі браузера.

3. Натисніть кнопку "Настроювання" у меню, що випадає.




4. У рядку, відповідної до ключа вашого адресата, клацніть кнопку зі значком "і":

5. З'явиться вікно властивостей ключа.




6. Попросите свого співрозмовника зробити те ж саме.

7. Знайдіть у властивостях ключа поле “Відбиток" і продиктуйте його вміст (довгу послідовність знаків) співрозмовникові. Якщо значення збіжаться, ключ справжній.

## 14. Питання й відповіді

***Питання.*** Якщо я вилучу Mailvelope з комп'ютера, що стане із зашифрованими листами й файлами?

**Відповідь.** З ними нічого не відбудеться. І листа, і файли залишаться зашифрованими. Ви зможете їх розшифрувати ( при наявності

відповідного секретного ключа), якщо знову встановите Mailvelope або іншу програму, яка підтримує той же стандарт шифрування.

**Питання.** Чи всі типи файлів можна шифрувати?

**Відповідь.** Так. Ви можете зашифрувати будь-який файл: і текстовий документ, і електронну таблицю, і архів, і фотографію, і звуковий файл.

***Питання.*** Я забув пароль до свого секретного ключа. чи Можу я як-небудь відновити пароль?

**Відповідь.** Немає. Відповідно, ви не зможете розшифровувати отримані листи, які були зашифровані парним відкритим ключем.

***Питання.*** У мене вийшов з ладу жорсткий диск, загинули всі дані, у тому числі шифрувальні ключі. чи Можна як-небудь одержати доступ до зашифрованих текстів і файлам?

**Відповідь.** Немає. Це ще один наочний урок на тему “чому необхідно регулярно робити резервні копії”.

***Питання.*** Я прагну відправити другові свій відкритий ключ, але випадково відправив також і секретний ключ. Що робити?

**Відповідь.** Уважати цю пару ключів скомпрометованої й створити нову.

***Питання.*** Я створив пару ключів, але тепер прагну поміняти пароль. чи Можна це зробити?

**Відповідь.** Це можливо в принципі, але не в Mailvelope.

***Питання.*** Я прагну зашифрувати лист, але Mailvelope не пропонує ключ адресата. У чому справа?

**Відповідь.** Можливі різні причини. Найпростіша – невірно набрана адреса. Найпоширеніша – відкритий ключ адресата відсутній у вашому зв'язці ключів (не був імпортований). Mailvelope шукає у зв'язці ключів потрібний, орієнтуючись на адресу e-mail. Були випадки, коли адресат при створенні ключа вказував фальшиву адресу e-mail, або вказував додаткову адресу e-mail (яким ви звичайно не користуєтеся для зв'язку із цією людиною), або робив помилку в адресі. Нарешті, можлива ситуація, коли в ключа виявлявся обмежений термін дії. Якщо ви вірно набрали адресу, але проблема залишається, переконайтесь, що актуального відкритого ключа адресата у вашої зв'язці не має, і попросите вашого співрозмовника надіслати свій відкритий ключ.

***Питання.*** Мені надіслали зашифрований лист. Я намагаюся його розшифрувати, але Mailvelope говорить, що на моєму комп'ютері немає потрібного ключа для розшифрування. У чому справа?

**Відповідь.** Можливі дві причини. Менш імовірно, що ваші ключі якимсь образом виявилися вилучені з вашої зв'язки ключів. Переконайтесь, що ваша актуальна пара ключів перебуває у зв'язці. Але найчастіше виявляється, що помилку допустив відправник: зашифрував лист НЕ вашим відкритим ключем (а, наприклад, своїм власним). Попросите його відправити лист знову, нагадавши, що йому слід скористатися вашим відкритим ключем.

***Питання.*** Може чи Mailvelope працювати на інших браузерах, крім Firefox і Chrome? Наприклад, Opera або Safari?

**Відповідь.** Немає. Тільки Firefox і Chrome.

***Питання.*** Де Mailvelope зберігає мої ключі?

**Відповідь.** На вашому комп'ютері, у папці профілю. Mailvelope автоматично не завантажує ключі на сервер, у хмару і т.д.

***Питання.*** Чи можна сховати сам факт установки/наявності Mailvelope на комп'ютері?

**Відповідь.** Оскільки Mailvelope – доповнення до браузера, він присутній у панелі браузера й у списку встановлених доповнень. Ви не зможете “просто” сховати Mailvelope у браузері, якщо той установлений звичайним способом. Однак, ви можете завантажити портативну версію браузера, установити Mailvelope для цієї версії, а сам браузер (разом з Mailvelope) сховати в захищеному від лиходіїв місці, наприклад, у зашифрованому контейнері Veracrypt.

## Використані джерела


1. Денісова О.О. Інформаційні системи і технології в юридичній діяльності: Навч.-метод. посібник для самост. вивч. дисципліни. – К.: КНЕУ, 2009.
2. Камский В.А. Защита личной информации в интернете, смартфоне и компьютере. – СПб: Наука и Техника, 2017 с. – 272 с.
3. Інформатика в юридичній діяльності (частина 2) [Текст]: І-741 [Підручник] / [Кудінов В.А., Мельников І.М., Пакриш О.Є. та ін.]; за заг редакцією В.А. Кудінова. – К.: Нац. акад.. внутр.. справ, 2017. – 332с.
4. Mailvelope – шифрование OpenPGP для веб-почты // [Електронній ресурс]. - Режим доступу: https://securityinabox.org/ru/guide/mailvelope/web/
5. Mailvelope – Wikipedia // [Електронній ресурс]. - Режим доступу: https://en.wikipedia.org/wiki/Mailvelope
6. Open PGP Encryption for Web-mail // Сайт розробника програмного додатку Mailvelope) [Електронній ресурс]. - Режим доступу: http://www.mailvelope.com.