МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки комп’ютерної та програмної інженерії

Кафедра безпеки інформаційних технологій

**Технології забезпечення конфіденційності і цілісності інформаційних ресурсів**

**Лабораторна робота №3**

Тема: Управління паролями. Засоби збереження та доступу до паролів. Правила роботи з паролями

Тривалість заняття: 180 хв.

Київ 2023

**Тема**: Управління паролями. Засоби збереження та доступу до паролів. Правила роботи з паролями. Генератор паролів

**Мета**: ознайомитися з поняттям паролю, основними засобами збереження та доступу до паролів, правилами роботи з паролями.

**Теоретичні відомості**

Паролі - це ключі, які відкривають доступ до особистих даних, що зберігаються на комп'ютері та в облікових записах в Інтернеті.

Якщо зловмисники вкрадуть ці дані, вони можуть скористатися ними для відкриття нових рахунків кредитних карт, отримання кредиту або виконання через Інтернет інших дій від вашого імені. Дуже часто ви можете не підозрювати про такі дії до тих пір, поки не стане занадто пізно.

З величезною кількістю системних паролів та сайтів, доступ до яких надається лише зареєстрованим користувачам, неможливо запам'ятати всі пари «ім'я користувача / пароль», якщо тільки ви не використовуєте одні й ті самі ім'я та пароль для всіх облікових записів або не записуєте їх. Обидва ці методи мають зниженим рівнем безпеки.

Той, хто використовує одні й ті ж ім'я користувача та пароль, починаючи електронною поштою і закінчуючи особистими банківськими рахунками, надають повний доступ до власного життя кожному, хто зможе зламати один з використовуваних акаунтів, так як таким чином, зловмисники зможуть використовувати отримані дані для будь-яких інших облікових записів. Отримати доступ до важливої інформації можна через файли cookie, які зберігаються на комп'ютері (це залежить від ступеня уразливості використовуваного браузера), і за допомогою сайтів, які не можуть використовувати протокол http або технологію SSL (відкритий стандарт для створення безпечних каналів підключення, які запобігають витік важливих конфіденційних відомостей, таких як номери кредитних карт). В даному випадку, ваші ім'я користувача та пароль виявляються у відкритому доступі в Інтернеті і можуть бути отримані будь-якою кількістю комп'ютерів.

При записуванні ім'я користувача та пароль на папір завжди існує можливість втратити цей листок, або хто-небудь може знайти його і отримати доступ до ваших акаунтів. Ймовірність такої загрози значно зростає, якщо ви залишаєте листок з даними під клавіатурою, приклеюєте його на монітор, ноутбук або просто залишаєте його на столі. Пароль використовується для забезпечення безпеки комп'ютерних програм, і тому, записуючи його на папір, ви просто видаляєте всяку безпеку. З іншого боку, ім'я користувача та пароль можуть бути легко викрадені, якщо вони надсилаються через Інтернет відкритим текстом, але зазвичай ті користувачі, які записують дані на папір для різних акаунтів, використовують різні паролі. Тому при втраті листка з паролем вони не втратять контроль над усіма обліковими записами.

Одним з кращих способів забезпечити безпеку при відкритті акаунтів є використання різних ім'я користувача та пароль при кожній реєстрації. Запам'ятати їх буває дуже складно (тому часто використовуються методи, описані вище). Все ж існує кращий спосіб збереження паролів - використання інструменту управління паролями. Таким чином, значно спрощується збереження паролів для кожного облікового запису. Іншою важливою перевагою використання менеджера паролів є те, що можна використовувати безпечніші паролі і не боятися забути їх.

Існує безліч менеджерів паролів, доступних в Інтернеті, - деякі платні, інші безкоштовні. Вибір типу програм залежить від користувача.

Менеджер паролів - програмне забезпечення, яке допомагає користувачеві працювати з паролями і PIN-кодами. У подібного програмного забезпечення зазвичай є в наявності місцева база даних або файли, які містять зашифровані дані пароля. Багато менеджерів паролів також працюють як заповнювач форми, тобто вони заповнюють поле користувач і дані пароля автоматично в формах. Зазвичай вони реалізовані як розширення браузера.

Менеджери паролів діляться на три основні категорії:

Десктоп - зберігають паролі до програмного забезпечення, встановленого на жорсткому диску комп'ютера. Портативні - зберігають паролі до програмного забезпечення на мобільних пристроях, таких як КПК, смартфон або до портативних додатків на USB флеш-накопичувачі.

Мережеві - менеджери паролів онлайн, де паролі збережені на веб-сайтах провайдерів.

Менеджери паролів можуть також використовуватися як захист від фішингу. На відміну від людей, програма менеджер паролів може звертатися з автоматизованим скриптом логіна не сприйнятливі до візуальних імітацій, які схожі на веб-сайти. З цією вбудованою перевагою використання менеджера паролів вигідно, навіть якщо у користувача є всього кілька паролів, які він пам'ятає. Однак не всі менеджери паролів можуть автоматично звертатися з більш складними процедурами ідентифікації, накладеними багатьма банківськими веб-сайтами.

Онлайн менеджер паролів - веб-сайт, який надійно зберігає дані логіна. Таким чином це мережева версія звичайного десктоп-менеджера паролів. Переваги онлайн менеджерів паролів над десктоп-версіями - це мобільність (вони можуть використовуватися на будь-якому комп'ютері з web-браузером і інтернет-з'єднанням, без необхідності встановлювати програмне забезпечення) і менший ризик втрати паролів через злодійство або пошкодження PC. Ризик пошкодження може бути в значній мірі знижений, якщо заздалегідь будуть створені резервні копії.

Головний недолік онлайн менеджерів паролів - необхідна довіра хостингу сайту. Неодноразові зломи і втрати централізовано збереженої інформації на сервері не вселяють довіри.

Існують змішані рішення. Ряд ресурсів, таких як FortNotes або МоіПаролі, що надають послуги онлайн-зберігання паролів та інших секретних даних, поширюють вихідні коди цих систем. Можливість провести аудит коду та встановити таку систему на захищений фаєрволом сервер або на сервер, що не має прямий вихід в Інтернет, дозволяє вирішити проблему з можливою компрометацією даних.

Використання мережевого менеджера паролів - альтернатива технології єдиного входу (Single Sign On), такий як OpenID або Microsoft's Windows Live ID, і може використовуватися як тимчасова міра, поки не буде прийнятий кращий метод.

Приклад програмного коду генератора паролів на мові програмування C++

#include <iostream>

#include <algorithm>

#include <time.h>

#include <stdlib.h>

#include <fstream>

using std::cout;

using std::cin;

using std::endl;

class PassGen {

public:

void displayMessage()

{

int passLenght;

int numOfPasswords;

char\* filename = new char;

cout << "Enter the password length to generate: ";

cin >> passLenght;

cout << "Enter the number of passwords to generate: ";

cin >> numOfPasswords;

cout << "Passwords will be generated: " << numOfPasswords << "." << endl;

cout << endl;

cout << "Enter the file name to record: ";

cin >> filename;

std::ofstream outFile(filename);

for (int k = 0; k < numOfPasswords; k++) {

for (int i = 0; i < passLenght; ++i) {

numOfChars(passLenght);

passGenerator(passLenght);

outFile << password[i];

}

outFile << endl;

}

outFile.close();

cout << "Passwords have been successfully generated and written to a file " << filename << "" << endl;

}

void passGenerator(int passLenght)

{

password = new char[passLenght];

for (int i = 0; i < numOfNumbers; ++i) {

password[i] = char(rand() % 10 + 48);

}

for (int i = numOfNumbers; i < numOfNumbers + numOfBigChars; ++i) {

password[i] = char(rand() % 26 + 65);

}

for (int i = numOfNumbers + numOfBigChars; i < passLenght; ++i) {

password[i] = char(rand() % 26 + 97);

}

std::random\_shuffle(password, password + passLenght);

}

void numOfChars(int passLenght)

{

numOfSmallChars = rand() % passLenght;

int charRandEnd = passLenght - numOfSmallChars;

numOfBigChars = rand() % charRandEnd;

numOfNumbers = passLenght - numOfSmallChars - numOfBigChars;

}

private:

int numOfSmallChars;

int numOfBigChars;

int numOfNumbers;

char\* password;

};

int main()

{

setlocale(0, "");

srand(time(NULL));

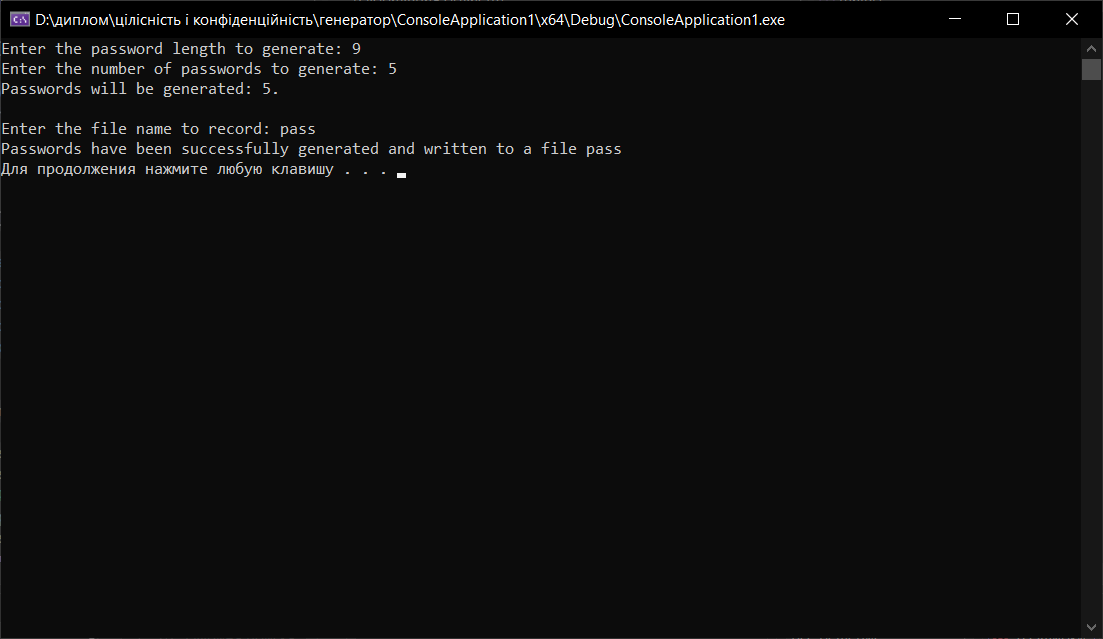
PassGen\* pass = new PassGen;

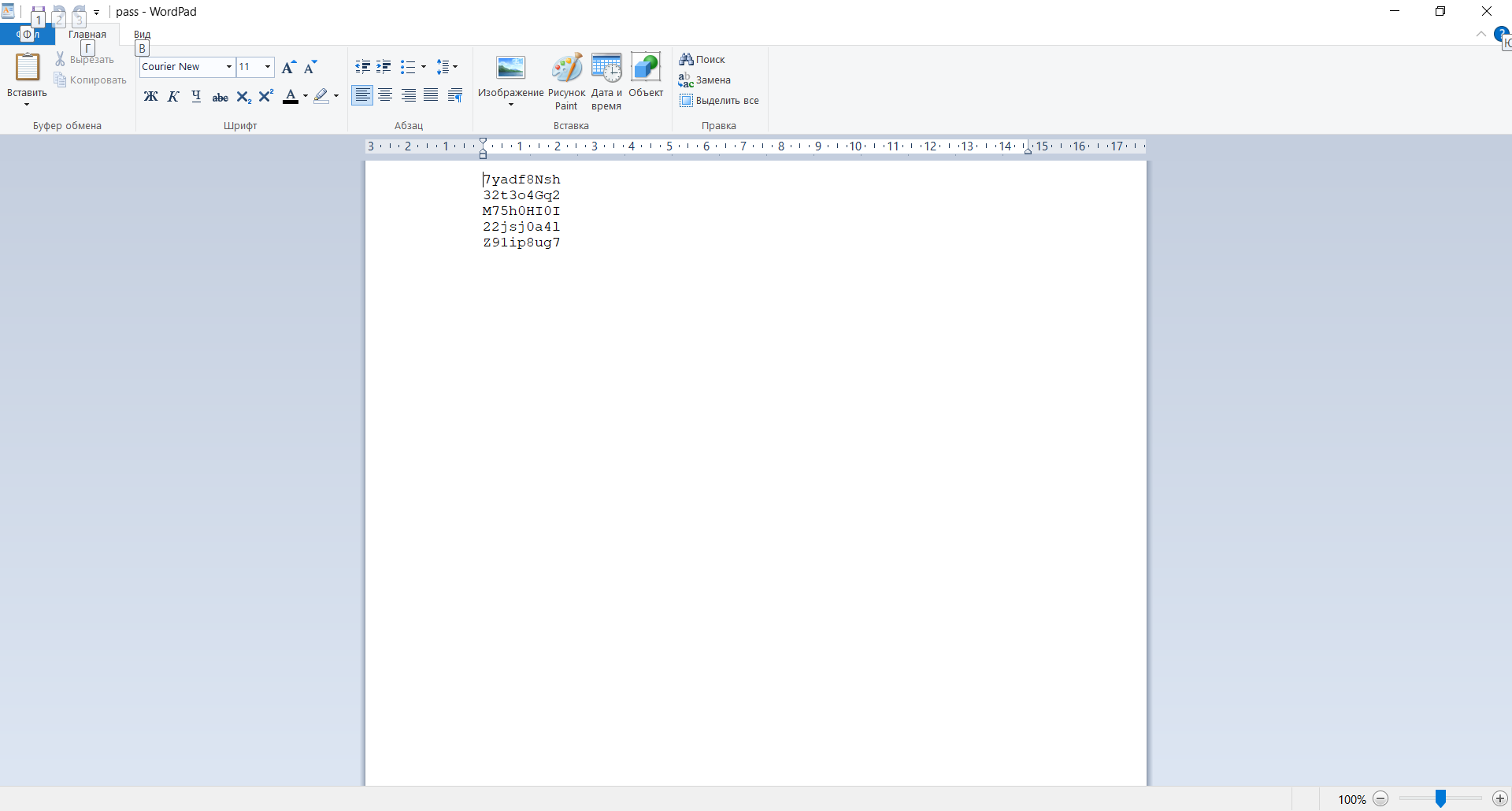
pass->displayMessage();

system("pause");

return 0;

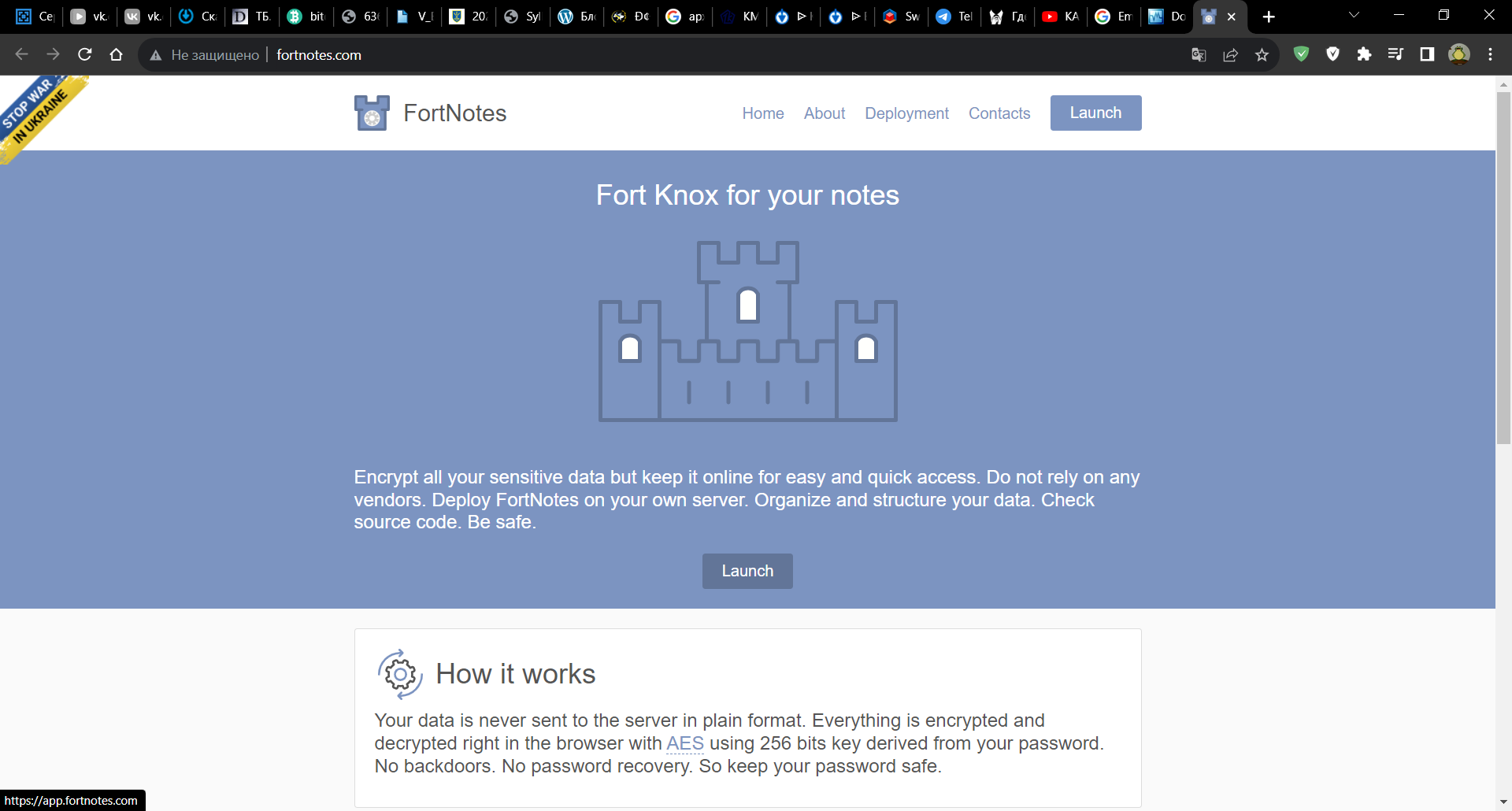
}



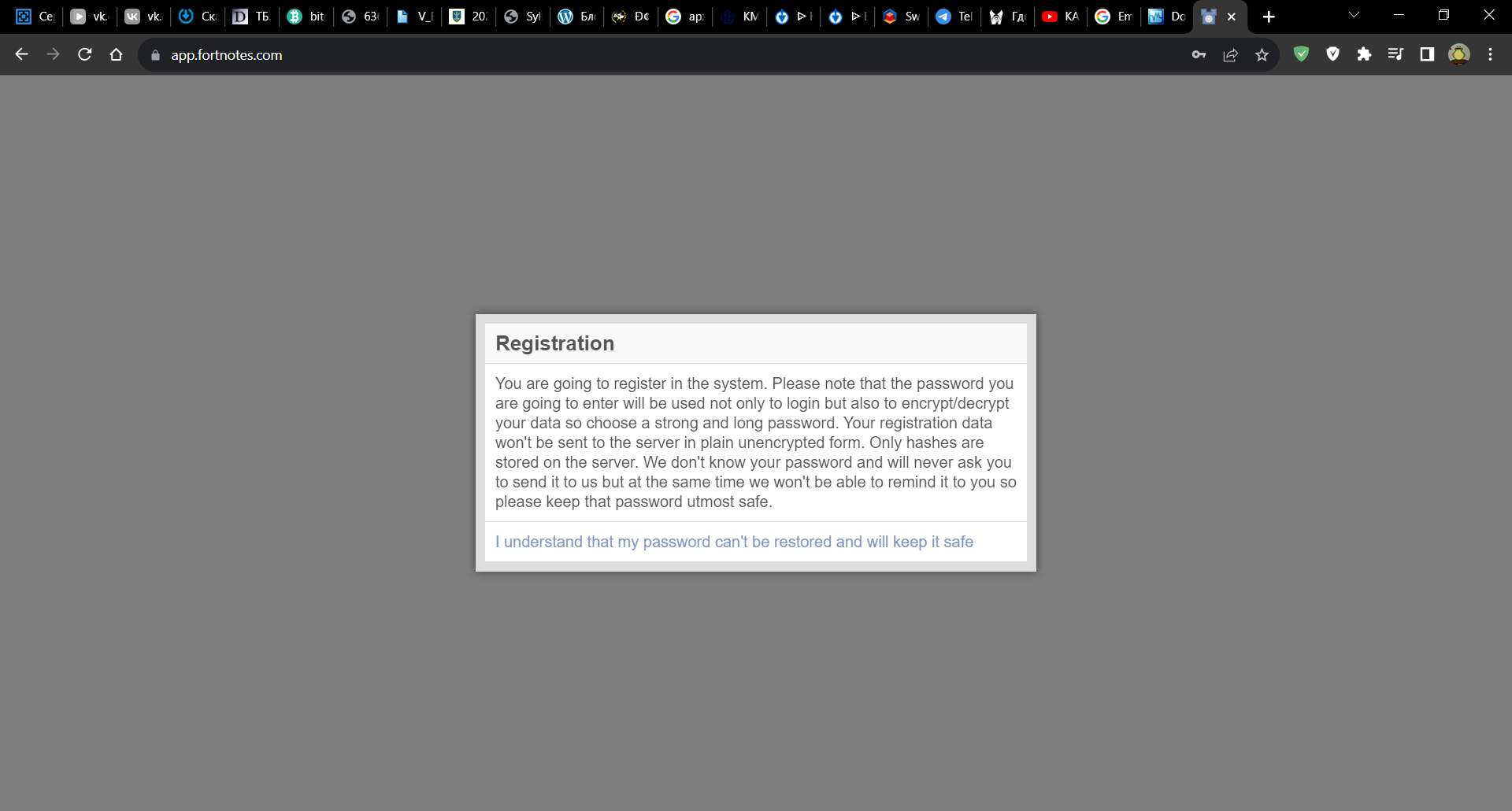


**Завдання**

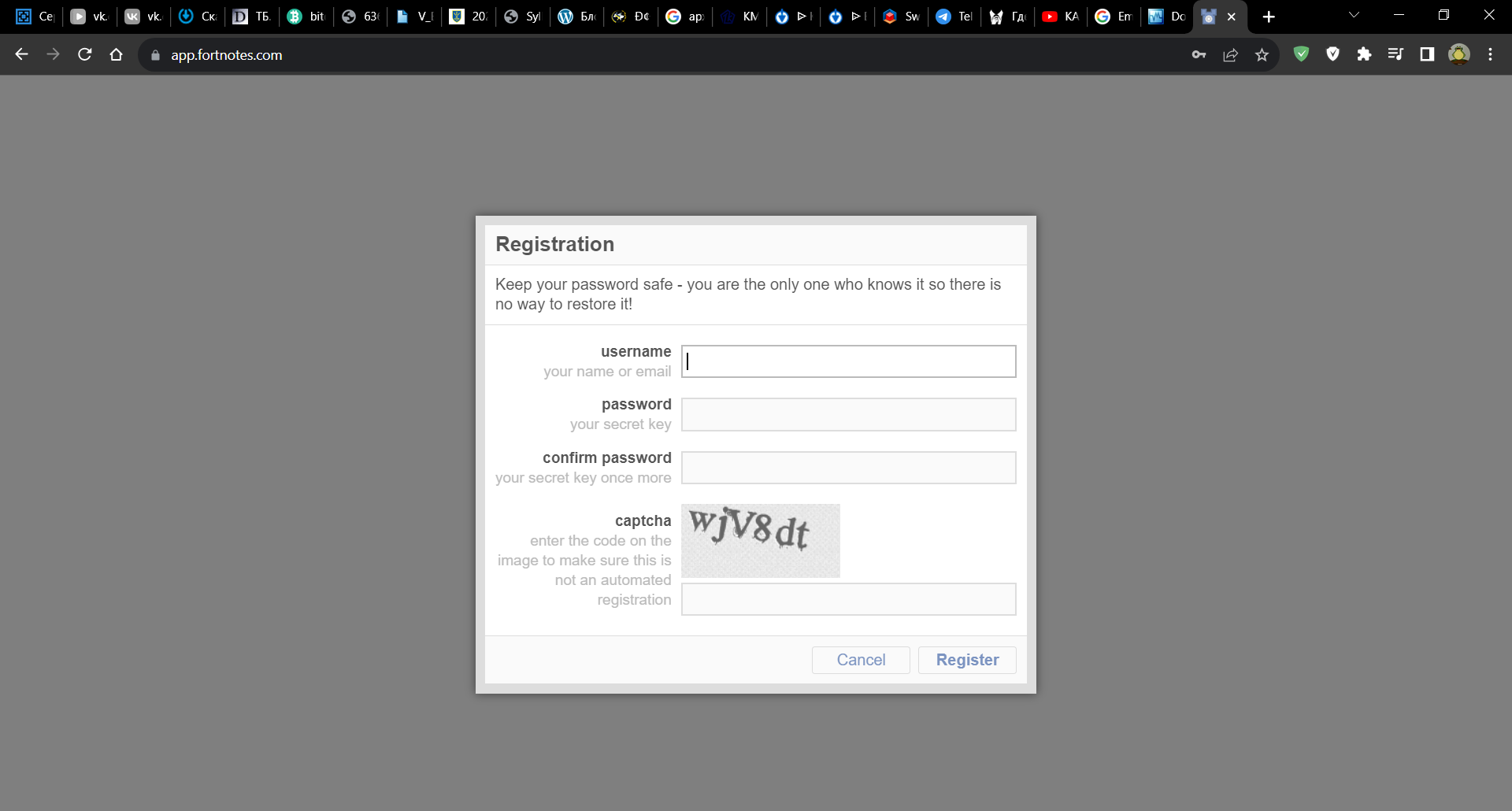
1. Запустіть встановлений на вашому комп’ютері браузер.
2. Перейдіть по посиланню <http://fortnotes.com/>
3. Створіть свій особистий аккаунт (Для цього потрібно натиснути кнопку Launch

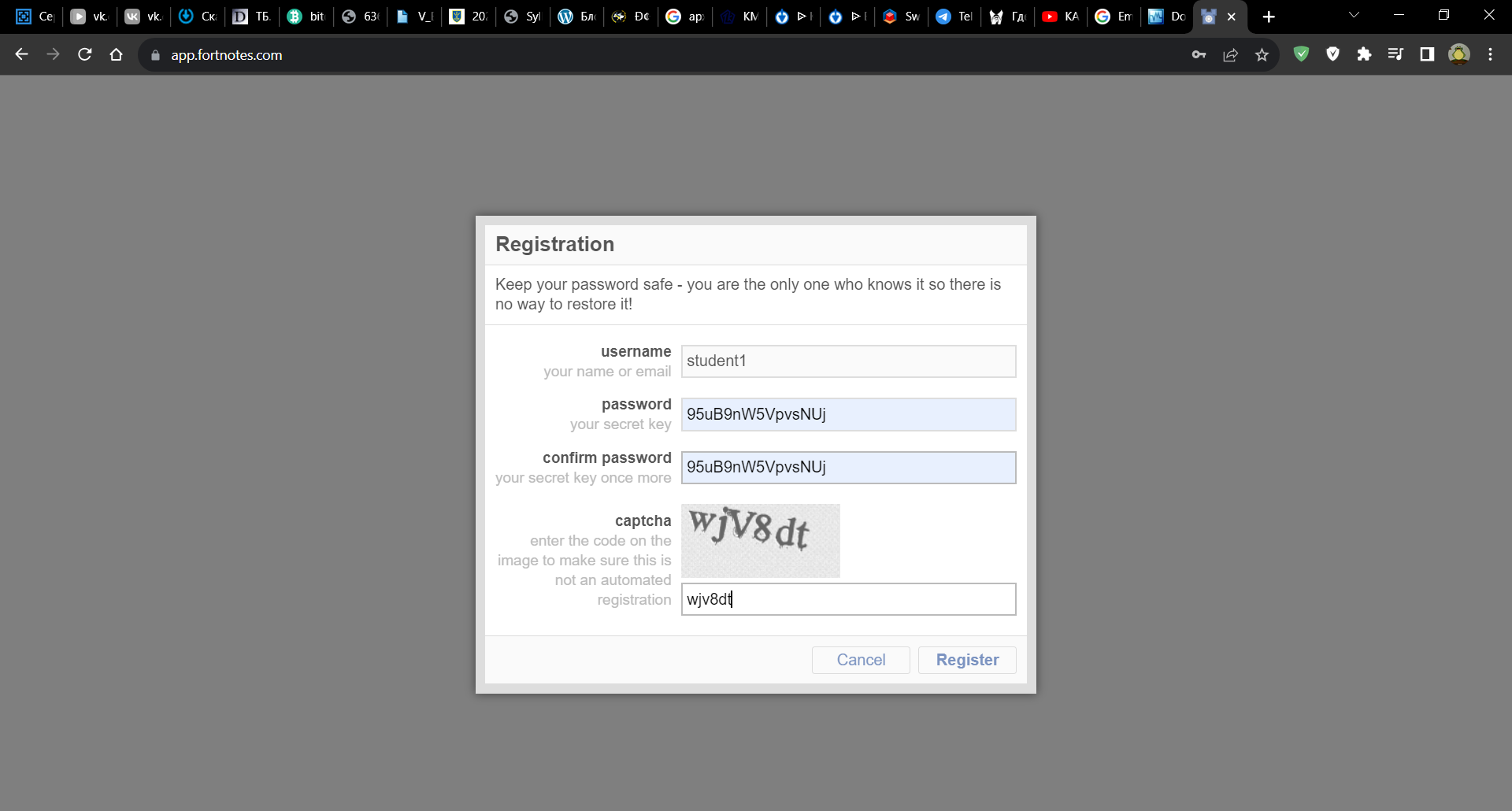


1. На наступній вкладці погоджуємось з умовами

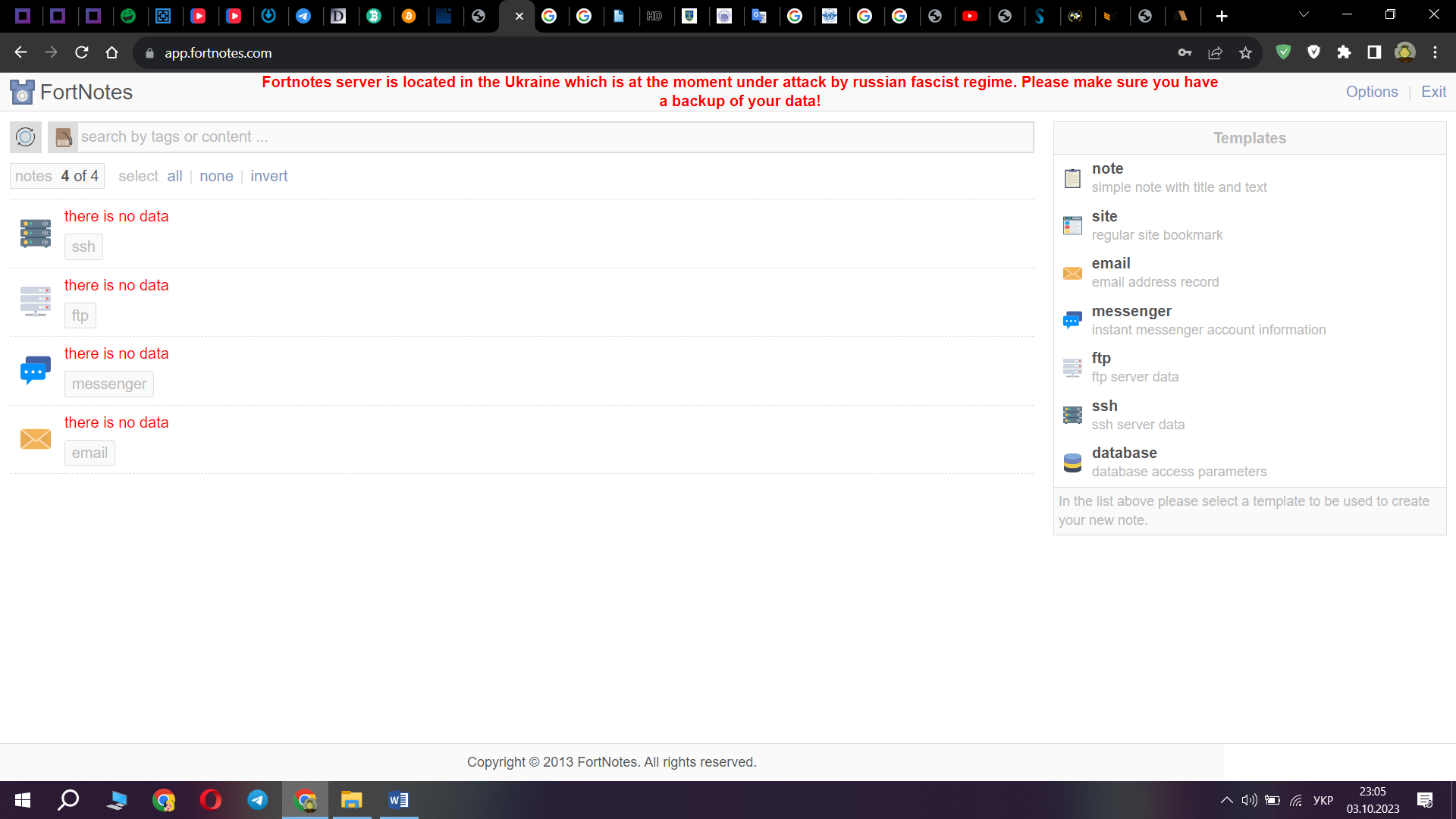


1. На відкритій далі вкладці заповнюємо поля





1. Проаналізуйте можливості даної служби
2. Створіть паролі для для всіх пунктів розділів Templates



1. Перегляньте створені вами записи.
2. Отримані результати у вигляді скріншотів занести до звіту.
3. Далі перейдіть за посиланням <http://websecurity.com.ua/password/>
4. Проаналізуйте можливості цього ресурсу.
5. Перевірте 5 своїх особистих паролів на рівень їх надійності, отримані результати занесіть до звіту.
6. Створіть 10 паролів різного рівня надійності не користуючись цим сервісом. Отримані результати занесіть до звіту. Перевірте надійність створених вами паролів використовуючи цей сайт. Отримані дані занесіть до таблиці
7. Користуючись цим сервісом створіть 10 паролів різної довжини. Перевірте надійність створених паролів за допомогою цього сайту. Отримані дані занесіть до таблиці
8. Порівняйте створені особисто вами паролі з паролями які були створені за допомогою цього сервісу, отримані результати занесіть до звіту.
9. Розробіть генератор паролів на зручній для вас мові програмування. Код програмної реалізації та скріншоти роботи програми занесіть до звіту. Код розробленої вами програми має відрізнятись від коду який представлено в прикладі.
10. Створіть 10 паролів за допомогою вашого генератора паролів.
11. Протестуйте створені паролі через вашу програму генерації паролів на цьому сайті <http://websecurity.com.ua/password/> , отримані результати занесіть до звіту.
12. Зробіть висновки та занесіть їх до звіту.

**Контрольні питання**

1. Що таке пароль?
2. Що таке менеджер паролів?
3. На які категорії поділяються менеджери паролів?
4. В чому недоліки менеджера паролів?
5. Яким чином потрібно створювати пароль, щоб його було тяжко вгадати або підібрати?