

Навчально-науковий інститут інформаційних технологій
Харківський національний економічний університет
імені Семена Кузнеця

Звіт

З Виконання лабораторної роботи №2
за дисципліною: “ Організаційне забезпечення захисту інформації ”
на тему: “ Аналіз сертифікатів безпеки сайтів організацій ”
Варіант №10

Виконав: студент кафедри
Кібербезпеки та інформаційних
технологій

4 курсу, спец. Кібербезпека,
групи 6.04.125.010.21.2

Бойко Вадим Віталійович

Перевірив:
Андрейчиков Олександр Олегович

ХНЕУ ім. С. Кузнеця

2024

Мета: Для сайтів, обраних у лабораторній роботі №2, виконати аналіз наявних сертифікатів безпеки та описати їх. Провести порівняння сертифікатів безпеки сайтів та зробити обґрунтований висновок, щодо оптимальності вибору сертифікату.

Для аналізу сертифікатів рекомендується використати функції браузера, сервіси: <https://www.sslshopper.com/ssl-checker.html>, <https://regeery.ua/uk/security/ssl-tools/certificate-checker>, <https://www.websiteplanet.com/uk/webtools/ssl-checker/>, інформацію з сайтів реєстраторів та інших джерел.

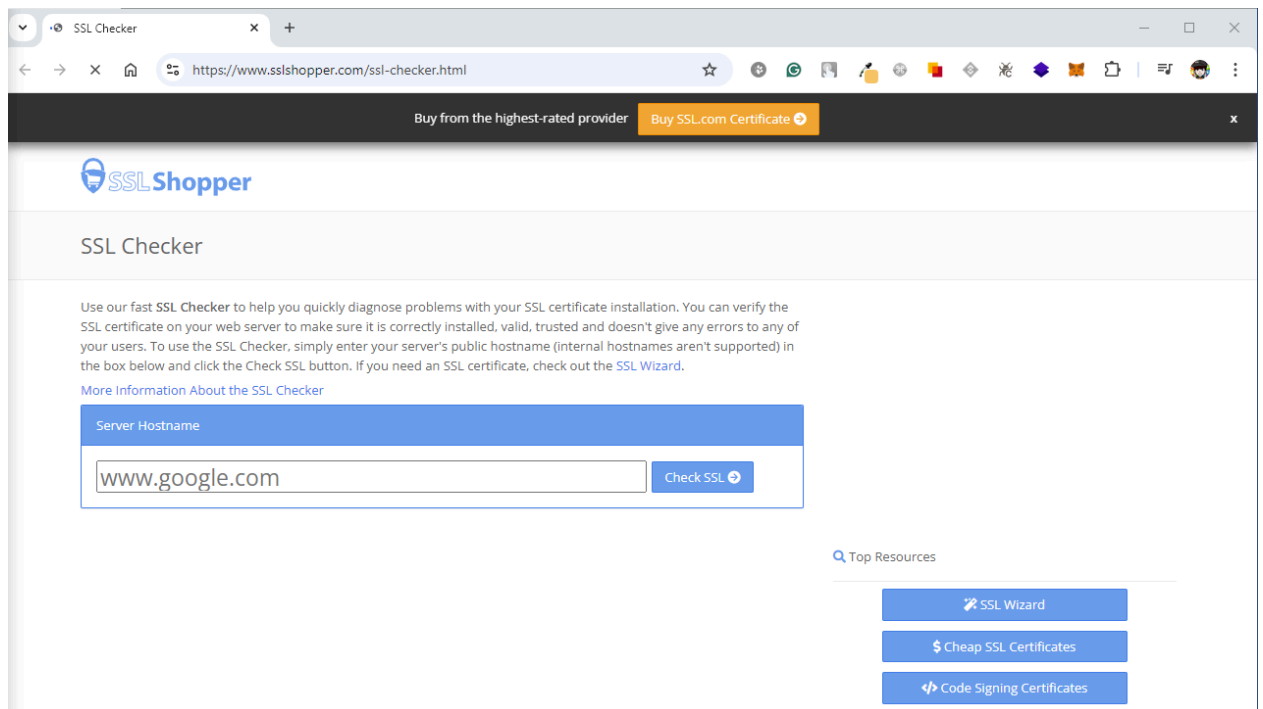
Сайти з попередньої лабораторної роботи:

Сайти
https://it.hneu.edu.ua/
https://iszzi.kpi.ua/
https://khtu.edu.ua/

Хід роботи:

1. Перейду на перший сайт, який було запропоновано у лабораторній роботі

<https://www.sslshopper.com/ssl-checker.html>



можна побачити, що інтерфейс досить зручний, оскільки є одна строка для вводу посилання на сайт та кнопка для перевірки сертифікату, тож перший сайт протестую завдяки цій утиліті



SSL Checker

Use our fast SSL Checker to help you quickly diagnose problems with your SSL certificate installation. You can verify the SSL certificate on your web server to make sure it is correctly installed, valid, trusted and doesn't give any errors to any of your users. To use the SSL Checker, simply enter your server's public hostname (internal hostnames aren't supported) in the box below and click the Check SSL button. If you need an SSL certificate, check out the [SSL Wizard](#).

[More Information About the SSL Checker](#)

Server Hostname

Check SSL



it.hneu.edu.ua resolves to 212.111.204.241

[Top](#)



Server Type: nginx



The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).



The certificate will expire in 41 days.

[Remind me](#)



The hostname (it.hneu.edu.ua) is correctly listed in the certificate.



Common name: it.hneu.edu.ua
SANs: it.hneu.edu.ua, www.it.hneu.edu.ua
Valid from September 1, 2024 to November 30, 2024
Serial Number: 040f0c7da8f3d176b9c72e0413bda618b3e1
Signature Algorithm: sha256WithRSAEncryption
Issuer: R10



Common name: R10
Organization: Let's Encrypt
Location: US
Valid from March 12, 2024 to March 12, 2027
Serial Number: 4ba85293f79a2fa273064ba8048d75d0
Signature Algorithm: sha256WithRSAEncryption
Issuer: ISRG Root X1

В результаті перевірки можемо дізнатись наступну інформацію:

IP адреса: 212.111.204.241

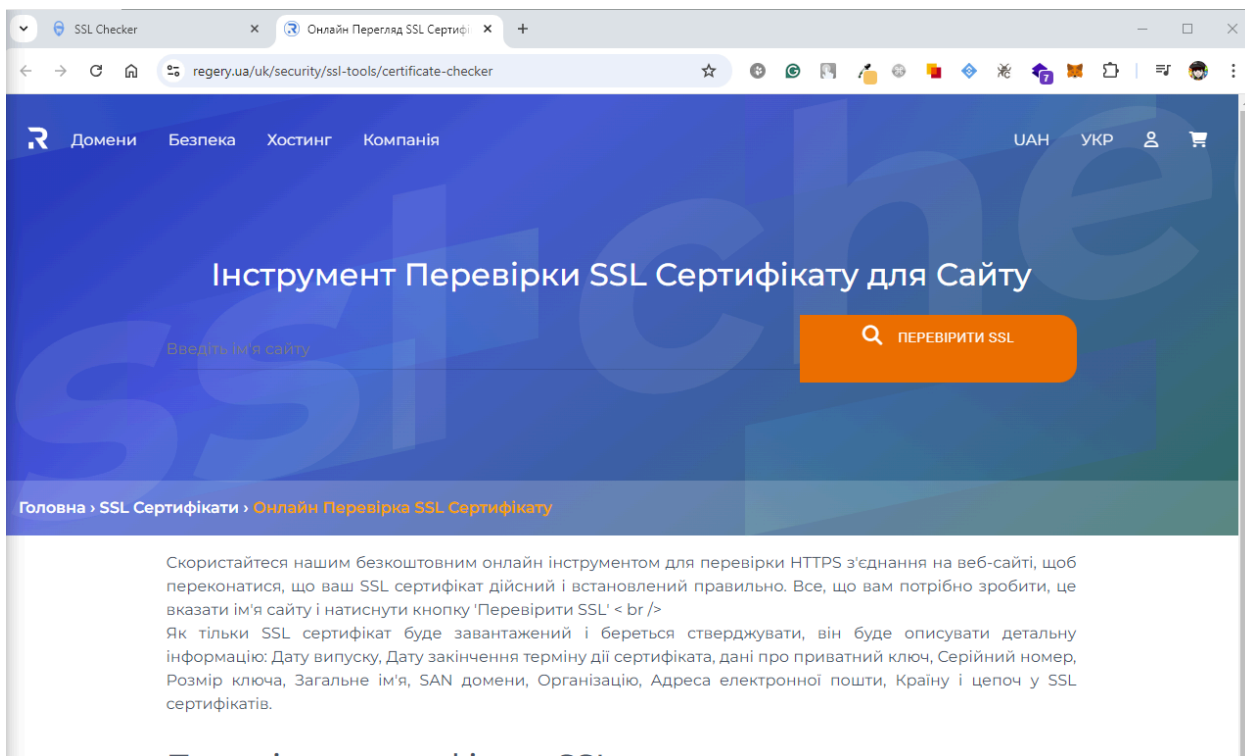
Що сервер функціонує на системі nginx

Що більша частина веб браузерів сприймають цей сертифікат як довірений

Що сертифікат буде валідний ще 41 день

Та що сервер коректно використовує сертифікат

2. Наступний сайт перевірю за допомогою іншої утиліти, для цього спочатку перейду на сайт



тут такий самий інтерфейс, як і в попередньому сайті, тому ввожу наступний URL та натисну на перевірку

Інструмент Перевірки SSL Сертифікату для Сайту

Введіть ім'я сайту
https:iszzi.kpi.ua

ПЕРЕВІРИТИ SSL

Сертифікати > Онлайн Перевірка SSL Сертифікату

Скористайтеся нашим безкоштовним онлайн інструментом для перевірки HTTPS з'єднання на веб-сайті, щоб переконатися, що ваш SSL сертифікат дійсний і встановлений правильно. Все, що вам потрібно зробити, це вказати ім'я сайту і натиснути кнопку 'Перевірити SSL' < br />

Як тільки SSL сертифікат буде завантажений і береться стверджувати, він буде описувати детальну інформацію: Дату випуску, Дату закінчення терміну дії сертифіката, дані про приватний ключ, Серійний номер, Розмір ключа, Загальне ім'я, SAN домени, Організацію, Адреса електронної пошти, Країну і цепоч у SSL сертифікатів.

Перевірка сертифіката SSL

Що таке SSL? Під цією аббревіатурою прийнято розуміти спеціальний протокол шифрування даних, які передбачені між сервером, на якому розміщуються ресурси і клієнтом. Даний протокол є найбільш поширений спосіб захисту даних в мережевому просторі. Для того щоб сайт залишався безпечним для відвідувачів, потрібна періодична перевірка сертифіката SSL, яка передбачає аналіз даних по протоколу. Перш ніж описати яким чином здійснюється перевірка, вкажемо, що представляє собою сам протокол.

Дані про SSL

Свого часу, дана міра безпеки була розроблена безпосередньо компанією Netscape. Безпечний обмін забезпечується за допомогою унікального механізму шифрування, а також подальшої аутентифікації виданого цифрового сертифікату. Являє собою **HTTPS сертифікат безпеки** - своєрідний файл, який в подальшому ідентифікується серверами. Підпис такого сертифіката здійснюється спеціалізованими центрами, вони ж і запевняють даний електронний протокол. Такі сервіси прийнято називати центрами, що засвідчують SSL або ж центр сертифікації.

Більш простими словами можна сказати, що такий протокол являє собою своєрідну цифровий підпис сайту, що дозволить підтвердити його справжність. Таким чином, клієнти, які вирішили підключити і перевірити SSL сертифікат забезпечують безпечне використання своїх ресурсів.

Практичне застосування протоколів дозволить забезпечити, як повноцінний захист ресурсу, так і клієнтів, які прийняли рішення відвідувати сайти і взаємодіяти з ними. Сертифікат дозволяє без проблем застосувати до власного сайту спеціальну методику шифрування.

Умо файли cookie для включення основних послуг на нашому сайті і збору даних про те, як відвідувачі нашім сайтом, продуктами і послугами. **Натискаючи Прийняти або продовжити** ви погоджуєтесь з тим, що ми використовуємо ці інструменти для реклами і аналітиці. **Адресу не знайдено**

Прийняти Відхилити

в результаті отримаю повідомлення, що адресу не знайдено, хоча сайт функціонує та браузер бачит, що з'єднання безпечне

SSL Checker | Онлайн Перегляд SSL Сертифі | ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИ

iszzki.kpi.ua

Безопасность iszzki.kpi.ua

Подключение защищено
Информация, которую вы сообщаете этому сайту (например, пароли и номера

ЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИ
Т СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХ
льного технічного університету У

Для того, щоб бути впевненим, що утиліта працює перевірю перший сайт

Інструмент Перевірки SSL Сертифікату для Сайту

Введіть ім'я сайту

<https://it.hneu.edu.ua>

🔍 ПЕРЕВІРИТИ SSL

Сертифікати > **Онлайн Перевірка SSL Сертифікату**

Скористайтеся нашим безкоштовним онлайн інструментом для перевірки HTTPS з'єднання на веб-сайті, щоб переконатися, що ваш SSL сертифікат дійсний і встановлений правильно. Все, що вам потрібно зробити, це вказати ім'я сайту і натиснути кнопку 'Перевірити SSL' < br />

Як тільки SSL сертифікат буде завантажений і береться стверджувати, він буде описувати детальну інформацію: Дату випуску, Дату закінчення терміну дії сертифіката, дані про приватний ключ, Серійний номер, Розмір ключа, Загальне ім'я, SAN домени, Організацію, Адреса електронної пошти, Країну і цепоч у SSL сертифікатів.

Перевірка сертифіката SSL

Що таке SSL? Під цією аббревіатурою прийнято розуміти спеціальний протокол шифрування даних, які передбачені між сервером, на якому розміщуються ресурси і клієнтом. Даний протокол є найбільш поширений спосіб захисту даних в мережевому просторі. Для того щоб сайт залишався безпечним для відвідувачів, потрібна періодична перевірка сертифіката SSL, яка передбачає аналіз даних по протоколу. Перш ніж описати яким чином здійснюється перевірка, вкажемо, що представляє собою сам протокол.

Дані про SSL

Свого часу, дана міра безпеки була розроблена безпосередньо компанією Netscape. Безпечний обмін забезпечується за допомогою унікального механізму шифрування, а також подальшої аутентифікації виданого цифрового сертифікату. Являє собою [HTTPS сертифікат безпеки](#) - своєрідний файл, який в подальшому ідентифікується серверами. Підпис такого сертифіката здійснюється спеціалізованими центрами, вони ж і запевняють даний електронний протокол. Такі сервіси прийнято називати центрами, що засвідчують SSL або ж центр сертифікації.

Більш простими словами можна сказати, що такий протокол являє собою своєрідну цифровий підпис сайту, що дозволить підтвердити його справжність. Таким чином, клієнти, які вирішили підключити і перевірити SSL сертифікат забезпечують безпечне використання своїх ресурсів.

Практичне застосування протоколів дозволить забезпечити, як повноцінний захист ресурсу, так і клієнтів, які прийняли рішення відвідувати сайти і взаємодіяти з ними. Сертифікат дозволяє без проблем застосувати до власного сайту спеціальну методику шифрування.

ми файли cookie для включення основних послуг на нашому сайті і збору даних про те, як відвідувачі використовують наш сайт, продуктами і послугами. Натискаючи **Прийняти** або **продовжити** ви згодні з тим, що ми використовуємо ці інструменти для реклами і аналітики.

Прийняти Відхилити

Адресу не знайдено

Бачу таке саме повідомлення, отже утиліта виглядає як не робоча, хоча якщо трохи змінити адресу сайту, та прибрати тип з'єднання, тоді утиліта працює

Результати перевірки сайту iszzi.kpi.ua

SSL сертифікат встановлений правильно.

Загальна інформація про сертифікат

Створено:	17 Oct 2023
Закінчиться:	16 Nov 2024 (залишилося днів: 27)
Довжина відкритого ключа:	2048 біт
Приватний Ключ:	Ні
Серійний номер:	05654025FA71332CBF6C876C682B0E78
Серійний номер (16x):	0x05654025FA71332CBF6C876C682B0E78

Інформація про сертифікат

Загальна ім'я:	*.kpi.ua
Доп. Домени (SAN):	kpi.ua, *.kpi.ua
Організація:	Igor Sikorsky Kyiv Politechnic Institute
Країна:	Україна
Місто:	Kyiv



Інформація про емітента

Загальна ім'я:	GeoTrust TLS RSA CA G1
Організація:	DigiCert Inc
Тип сертифіката:	www.digicert.com
Країна:	Сполучені Штати

Можна дізнатись, що сертифікат буде валідним ще 27 днів, що довжина відкритого ключа 2048 біт, чого більше ніж достатньо для публічного сайту, також можна побачити серійний номер сертифікату, та інформацію, яку було отримано в попередній лабораторній роботі, єдине з нової інформації можна побачити хто видав сертифікат, це “GeoTrust TLS RSA CA G1” та що країна, яка видала сертифікат - США,

Також можна подивитись на ланцюг SSL

Інформація про ланцюжку SSL сертифікатів

Головний Сертифікат	Загальна ім'я: Організація: Створено: Закінчиться: Емітент:	*.kpi.ua Igor Sikorsky Kyiv Politechnic Institute 17 Oct 2023 17 Nov 2024 (залишилося днів: 27) GeoTrust TLS RSA CA G1
		
Проміжний Сертифікат	Загальна ім'я: Організація: Тип сертифіката: Створено: Закінчиться: Емітент:	GeoTrust TLS RSA CA G1 DigiCert Inc www.digicert.com 02 Nov 2017 02 Nov 2027 (залишилося днів: 1107) DigiCert Global Root G2
		
Кореневий Сертифікат	Загальна ім'я: Організація: Тип сертифіката: Створено: Закінчиться: Емітент:	DigiCert Global Root G2 DigiCert Inc www.digicert.com 01 Aug 2013 15 Jan 2038 (залишилося днів: 4834) DigiCert Global Root G2

Та з цієї інформації можна зрозуміти, що сайт використовує одну й ту саму організацію для отримання сертифікатів.

3. Тепер передо до третьої утиліти

The screenshot shows a web browser window with three tabs: 'SSL Checker', 'Онлайн Перегляд SSL Сертифі...', and 'Перевірка SSL - Онлайн-переві...'. The address bar shows the URL 'websiteplanet.com/uk/webtools/ssl-checker/'. Below the browser window, there is a disclaimer in Ukrainian: 'Наші оцінки постачальників послуг засновані на результатах ретельних тестувань та досліджень, але ми беремо до уваги також і ваші відгуки та комерційні угоди, укладені з окремими постачальниками послуг. Ця сторінка містить партнерські посилання. Розкриття інформації про рекламодавців'. The main navigation bar includes the 'WEBSITE PLANET' logo, links to 'Огляди', 'Купони' (with a '99+' badge), 'Інструменти', and 'Блог', a search bar with the text 'Шукати...', and language/region selectors for 'UAH' and 'Українська'. The main content area has a purple header with a shield icon and the text 'Перевірка SSL – Онлайн-перевірка сертифікатів безкоштовно'. Below this, it says 'Перевірте, чи ваш SSL-сертифікат було встановлено належним чином і чи довіряють йому веб-браузери'. There is a text input field for 'URL-адреса вашого веб-сайту' with a placeholder example 'www.websiteplanet.com' and a yellow 'Перевірити' button. At the bottom, there is a section titled 'Найчастіші питання'.

SSL Checker Онлайн Перегляд SSL Сертифі... Перевірка SSL - Онлайн-переві...

websiteplanet.com/uk/webtools/ssl-checker/

Наші оцінки постачальників послуг засновані на результатах ретельних тестувань та досліджень, але ми беремо до уваги також і ваші відгуки та комерційні угоди, укладені з окремими постачальниками послуг. Ця сторінка містить партнерські посилання. Розкриття інформації про рекламодавців

WEBSITE PLANET Огляди Купони 99+ Інструменти Блог Шукати... UAH Українська

Перевірка SSL – Онлайн-перевірка сертифікатів безкоштовно

Перевірте, чи ваш SSL-сертифікат було встановлено належним чином і чи довіряють йому веб-браузери

URL-адреса вашого веб-сайту Перевірити

Приклад: www.websiteplanet.com

Найчастіші питання

Тут такий самий інтерфейс, тому вводжу останній сайт та натисну на кнопку для перевірки



ВАШ СЕРТИФІКАТ ВСТАНОВЛЕНО ВІРНО!

Видано: khtu.edu.ua
Видав: WE1
Довірений: Так
Відповідність імені: SSL відповідає імені домену
Дійсний: 24 Вересня 2024 - 23 Грудня 2024 (термін дії спливає через 63 днів)

Додати нагадування до календарю

Інформація про сертифікат

Спільне ім'я: khtu.edu.ua
Малі локальні мережі: khtu.edu.ua, *.khtu.edu.ua
Розмір ключа: 256 bits
Алгоритм формування електронного підпису: ecdsa-with-SHA256
Слабкий ключ шифрування: Ні
Тип сертифікату SSL: Domain Validated
Алгоритм шифрування відкритим кодом: ecdsa
Відбиток 0335d9be22eb45cebdc83590c7e80986ad36f47d
Серійний номер: 0x97153E5FBA9339760D2B681600BC4C35
Бренд видавника: Google Trust Services
Видавець (Центр сертифікації): WE1

Інформація про сервер

Тип серверу: cloudflare
IP-адреса: 172.67.193.48
Порт: 443
Ім'я хосту: khtu.edu.ua

Мережа сертифікатів



Сертифікат серверу

Спільне ім'я:
khtu.edu.ua

Більше інформації ▾



Проміжний сертифікат

Спільне ім'я:
WE1

Більше інформації ▾



Кореневий сертифікат

Спільне ім'я:
GlobalSign Root CA

Більше інформації ▾

Різнноманітний

Дата звіту: 20 Жовтня 2024
Тривалість звіту: 27 ms

Завантажити в PDF

Скопіювати посилання на звіт

Тут можна побачити, що сертифікат ще буде валідним 63 дні, розмір ключа 256, що є стандартною й мінімальною довжиною для публічного ключа для публічного сайту, також, що сертифікат виданий брендом “Google Trust Services”, також сайт використовує “cloudflare” для більшого захисту, але це означає, що доступ до всього трафіку має ще одна організація, також можна побачити IP адресу 172.67.193.48 та що є мережа сертифікатів, для спільного ім’я - один сертифікат, та проміжний сертифікат.

Оскільки остання утиліта має майже ту саму інформацію, що й попередня утиліта, тому перевірю перший сайт завдяки цій утиліті

https://it.hneu.edu.ua/



Перевірити

Приклад: www.websiteplanet.com



ВАШ СЕРТИФІКАТ ВСТАНОВЛЕНО ВІРНО!

Видано:	it.hneu.edu.ua
Видав:	R10
Довірений:	Так
Відповідність імені:	SSL відповідає імені домену
Дійсний:	2 Вересня 2024 - 1 Грудня 2024 (термін дії спливає через 41 днів)

Додати нагадування до календарю

Інформація про сертифікат

Спільне ім'я:	it.hneu.edu.ua
Малі локальні мережі:	it.hneu.edu.ua, www.it.hneu.edu.ua
Розмір ключа:	4096 bits
Алгоритм формування електронного підпису:	RSA-SHA256
Слабкий ключ шифрування:	Hi
Тип сертифікату SSL :	Domain Validated
Алгоритм шифрування відкритим кодом:	RSA
Відбиток	10066d7fe866300a756c80c35f0832c9f0c9ada0
Серійний номер:	0x040F0C7DA8F3D176B9C72E0413BDA618B3E1
Бренд видавника:	Let's Encrypt
Видавець (Центр сертифікації) :	R10

Із додаткової інформації можна побачити, що використовується ключ шифрування розміром 4096 біт, чого буде достатньо ще на декілька років так точно, оскільки це публічний сайт, бренд, який видав сертифікат “Let's Encrypt”

Інформація про сервер така сама, як і з першої утиліти, й також використовується мережа сертифікатів окремо для серверу й окремо проміжний сертифікат.

Висновок: я проаналізував декілька сертифікатів, які належать певним сайтам завдяки утилітам, які були представлені у лабораторній роботі, й можу сказати, що всі сайти використовують мінімальну або стандартну довжину ключа, також один сайт має захист завдяки сервісу “cloudflare” що гарно й погано одночасно, гарно, що є додатковий захист, й погано оскільки є організація, яка має доступ до всього трафіку у нешифрованому вигляді