ISNN 3030-3907

2026
JUNE
ISSUE - 6
VOLUME -3

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

IYUN 2026
Issue - 6, VOLUME – 3

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ И АНАЛИЗ УЯЗВИМОСТЕЙ МЕТОДОВ ТЕКСТОВОЙ СТЕГАНОГРАФИИ В СРЕДЕ UNICODE

Хусанова Мохирахон Курбоналиевна
Ферганский государственный технический университет
Старший преподаватель кафедры "Программный инжиниринг и кибербезопасность".
Фергана, Узбекистан
E-mail: mokhira.khusanova@gmail.com
Мирзаев Жамшид Боймуродович
Ферганский государственный технический университет
Старший преподаватель кафедры "Программный инжиниринг и кибербезопасность".
Фергана, Узбекистан
E-mail: j.b.mirzayev@gmail.com

Аннотация. В статье исследуются механизмы скрытой передачи данных в текстовых средах с использованием спецификаций стандарта Unicode. Рассматриваются два наиболее распространенных подхода: инжекция скрытых битовых потоков с помощью символов нулевой ширины и подмена визуально идентичных графем из разных алфавитных пространств. Была разработана программная модель на языке Python, реализующая алгоритмы побитового внедрения (*embed*) и извлечения (*extract*) секретных сообщений. Проведен комплексный анализ безопасности и деструктивного контроля стегоконтейнеров. Выявлены ключевые маркеры детекции скрытых каналов, такие как аномальное расширение размера файлов и появление характерных байтовых последовательностей в HEX-структуре документа. Определены границы применимости Unicode-стеганографии, включая ее высокую уязвимость к процедурам транскодирования.

Ключевые слова: текстовая стеганография, Unicode, символы нулевой ширины, омоглифы, информационная безопасность, Python, HEX-анализ, уязвимости стегосистем, фишинг.

Abstract. The paper investigates the mechanisms of covert data transmission in text environments using the Unicode standard specifications. Two of the most common approaches are examined: the injection of hidden bitstreams using zero-width characters and the substitution of visually identical graphemes from different alphabetic spaces. A software model was developed in Python, implementing algorithms for bitwise embedding (embed) and extraction (extract) of secret messages. A comprehensive security and destructive control analysis of stego-containers was conducted. Key markers for detecting hidden channels were identified, such as anomalous file size expansion and the occurrence of

ISSN 3030-3907

characteristic byte sequences in the document's HEX structure. The boundaries of applicability for Unicode steganography were determined, including its high vulnerability to transcoding procedures.

Keywords: text steganography, Unicode, zero-width characters, homoglyphs, information security, Python, HEX analysis, stegosystem vulnerabilities, phishing.

Annotatsiya. Maqolada Unicode standarti spetsifikatsiyalaridan foydalangan holda matnli muhitlarda ma’lumotlarni yashirin uzatish mexanizmlari tadqiq etilgan. Eng ko‘p tarqalgan ikkita yondashuv, nol kenglikdagi belgilar yordamida yashirin bitli oqimlarni kiritish (injeksiya) va turli alifbo hududlaridan olingan, vizual jihatdan bir xil bo‘lgan grafemalarni almashtirish ko‘rib chiqilgan. Python tilida maxfiy xabarlarni bitlar darajasida joylashtirish (embed) va ajratib olish (extract) algoritmlarini amalga oshiruvchi dasturiy model ishlab chiqilgan. Stegokonteynerlarning xavfsizligi va destruktiv nazoratining kompleks tahlili o‘tkazilgan. Yashirin kanallarni aniqlashning asosiy markerlari, masalan, fayl hajmining anomal kengayishi va hujjatning HEX-tuzilmasida xarakterli baytlar ketma-ketligining paydo bo‘lishi aniqlangan. Unicode-steganografiyasini qo‘llash chegaralari, shu jumladan uning transkodlash (kodlashni o‘zgartirish) jarayonlariga yuqori darajada zaifligi belgilab berilgan.

Kalit so‘zlar: matnli steganografiya, Unicode, nol kenglikdagi belgilar, omogliflar, axborot xavfsizligi, Python, HEX-tahlil, stegotizimlar zaifliklari, fishing.

ВВЕДЕНИЕ.

В сфере защиты информации стеганография занимает уникальную нишу, решая задачу скрытия самого факта осуществления коммуникации. В отличие от криптографии, которая трансформирует текст в нечитаемый вид и тем самым детерминированно привлекает внимание систем мониторинга трафика (DLP, DPI), стеганография маскирует конфиденциальный объект внутри легитимного массива данных.

В качестве стегоконтейнеров традиционно выступают мультимедийные файлы. Однако их регулярная циркуляция в строго контролируемых корпоративных сетях может вызывать подозрения. Напротив, текстовые документы такие как, договоры, электронные письма, системные логи составляют основу повседневного трафика любой организации, что делает текстовую стеганографию крайне перспективным инструментом для построения скрытых каналов.

Главным препятствием для развития текстовой стеганографии исторически являлась низкая информационная избыточность текста. Изменение межзнаковых интервалов, манипуляции со шрифтами или

ISSN 3030-3907

знаками препинания легко разрушаются при копировании или изменении форматирования. Ситуация изменилась с повсеместным внедрением стандарта Unicode, предоставляющего обширное пространство управляющих кодов и мультиязычных символов.

Настоящая работа посвящена программной реализации стегосистемы на языке Python, использующей скрытые возможности стандарта Unicode, а также детальному исследованию уязвимостей и методов обнаружения созданных скрытых каналов.

Современное адресное пространство Unicode включает в себя специализированные символы, разработанные для нужд типографики и лингвистического форматирования, но не имеющие физической ширины при визуальном рендеринге на экране. Такие объекты называют символами нулевой ширины (*Zero-Width Characters*, ZWC). К их числу относятся:

- **U+200B** (Zero-Width Space) — пробел нулевой ширины, используемый для указания потенциального переноса слова;
- **U+200C** (Zero-Width Non-Joiner) — разделитель нулевой ширины, запрещающий слияние соседних глифов в лигатуру.

Поскольку данные знаки не отображаются текстовыми редакторами, они идеально подходят для побитового кодирования информации. В рамках бинарного представления каждый бит секретного сообщения может быть сопоставлен с конкретным ZWC-символом (например, ***0*** → ***U+200B***, ***1*** → ***U+200C***). Цепочка таких символов интегрируется внутрь легитимного текста-контейнера, не нарушая его визуального восприятия.

Вторым направлением является использование омоглифов — символов, имеющих идентичное или крайне похожее начертание, но принадлежащих к разным кодовым таблицам. Классическим примером служат строчные буквы русской кириллицы и латиницы: например, русская «а» (***U+0430***) и английская «а» (***U+0061***). Модуляция контейнера в данном случае происходит за счет управляемой замены букв: если символ заменен на латинский аналог — передается логический ноль, если оставлен кириллический — логическая единица.

Для проведения вычислительных экспериментов на языке Python был разработан программный комплекс, состоящий из модулей инжекции (*embed*) и экстракции (*extract*).

Алгоритм внедрения данных (Embed)

Процедура внедрения переводит строковое секретное сообщение в массив бит. Каждый бит заменяется на соответствующий шестнадцатеричный управляющий код Unicode. Сгенерированная скрытая последовательность встраивается в тело текста-контейнера

ISSN 3030-3907

непосредственно после первого символа, что позволяет сохранить целостность структуры при чтении потока. Скрипт переводит секретное сообщение в двоичный формат, затем заменяет биты на символы нулевой ширины: U+200B = бит 0, U+200C = бит 1. Невидимые символы вставляются внутрь текста-контейнера после первого символа.

Ниже представлена программная реализация функции внедрения:

```
def embed_zwc_message(container_text, secret_message): ZERO_CHAR =
    '\u200B' # Код для бита 0
    ONE_CHAR  = '\u200C'  # Код для бита 1
    # Перевод секретного сообщения в двоичный формат (8 бит на
    символ) binary_secret = ''.join(format(ord(c), '08b') for c in
    secret_message)
    # Формирование скрытого стего-тега
    zwc_payload = ''.join(ONE_CHAR if bit == '1' else ZERO_CHAR for bit
in binary_secret)
    # Внедрение скрытого тега внутрь контейнера после первого символа
    stego_text = container_text[0] + zwc_payload + container_text[1:] return
    stego_text
```

Алгоритм извлечения данных (Extract)

На приемной стороне получатель, обладающий информацией о правилах кодирования, сканирует текст на наличие скрытых Unicode-маркеров, восстанавливает исходную битовую последовательность и выполняет обратное декодирование в символы ASCII/UTF-8. Скрипт сканирует каждый символ текста, находит U+200B и U+200C, собирает двоичную строку и преобразует каждые 8 бит обратно в символ ASCII.

Программный код функции извлечения:

```
def extract_zwc_message(stego_text): ZERO_CHAR = '\u200B'
    ONE_CHAR  = '\u200C'
    binary_bits = []
    # Сбор скрытых символов нулевой ширины из текста for char in
    stego_text:
        if char == ZERO_CHAR: binary_bits.append('0')
        elif char == ONE_CHAR: binary_bits.append('1')
    if not binary_bits:
        return "Скрытое сообщение не обнаружено."
    binary_str = ''.join(binary_bits) secret_message = ""
    # Побайтовое декодирование (блоки по 8 бит) for i in range(0,
    len(binary_str), 8):
        byte_chunk = binary_str[i:i+8] if len(byte_chunk) == 8:
```


ISSN 3030-3907

```
        secret_message += chr(int(byte_chunk, 2))
    return secret_message
```

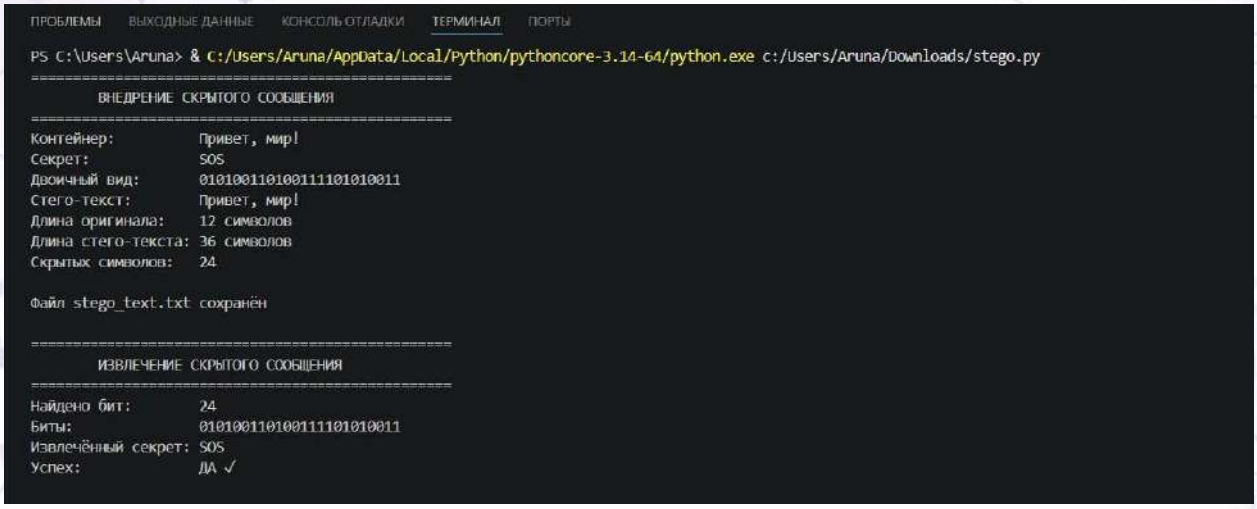


Рисунок 1 — Внедрение и извлечение сообщения "SOS" в консоли VS Code

На скриншоте показан результат запуска скрипта stego.py: контейнер «Привет, мир!», секретное сообщение «SOS», его двоичное представление, длина оригинального и стего-текста, а также успешное извлечение секрета.

Несмотря на абсолютную визуальную незаметность (критерий стеганографической неотличимости полностью выполняется), разработанный метод обладает рядом критических уязвимостей, которые необходимо учитывать при проектировании защищенных систем.

В ходе эксперимента в текст-контейнер объемом 84 символа внедрялось секретное сообщение длиной 29 символов. Поскольку каждый символ секретного текста кодируется 8 битами, общий объем скрытого блока составил:

$$29 \times 8 = 232 \text{ бит (символов нулевой ширины)}$$

Результирующий размер файла увеличился со 84 символов до 316 символов. На малых объемах текста такое соотношение (***len(stego)*** $\gg$ ***len(original)***) порождает явную структурную аномалию. Физический размер текстового файла на диске возрастает пропорционально объему вложения, что мгновенно регистрируется автоматизированными DLP-системами на основе сигнатурного анализа размеров документов.

Уязвимость к HEX-анализу структуры

Символы ***U+200B*** и ***U+200C*** не отображаются в графическом интерфейсе стандартных редакторов (Блокнот, MS Word), однако они чётко фиксируются при низкоуровневом анализе. В кодировке UTF-8 указанные символы преобразуются в строго определенные трехбайтовые последовательности:

ISSN 3030-3907

- ***U+200B → E2 80 8B***
- ***U+200C → E2 80 8C***

После выполнения скрипта был проведён анализ байтового содержимого файла stego_text.txt. Первые два байта D0 9F соответствуют букве "П" в кодировке UTF-8. Далее следуют цепочки байт E2 80 8B (U+200B, бит 0) и E2 80 8C (U+200C, бит 1) — это и есть внедрённые невидимые символы, содержащие закодированное сообщение "SOS".

При открытии стегоконтейнера в любом HEX-редакторе исследователь обнаруживает плотный массив повторяющихся байт ***E2 80 8B*** и ***E2 80 8C***. Это делает метод полностью беззащитным перед простейшими сигнатурными стеганоанализаторами.

ISSN 3030-3907

```
==================================================
        HEX-АНАЛИЗ ФАЙЛА
==================================================
Размер файла: 93 байт
HEX-дамп (первые 80 байт):
  D0        = обычный байт
  9F        = обычный байт
  [E2 80 8B] = U+200B = бит 0 (ZWS)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  [E2 80 8B] = U+200B = бит 0 (ZWS)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  [E2 80 8B] = U+200B = бит 0 (ZWS)
  [E2 80 8B] = U+200B = бит 0 (ZWS)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  [E2 80 8B] = U+200B = бит 0 (ZWS)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  [E2 80 8B] = U+200B = бит 0 (ZWS)
  [E2 80 8B] = U+200B = бит 0 (ZWS)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  [E2 80 8B] = U+200B = бит 0 (ZWS)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  [E2 80 8B] = U+200B = бит 0 (ZWS)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  [E2 80 8B] = U+200B = бит 0 (ZWS)
  [E2 80 8B] = U+200B = бит 0 (ZWS)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  [E2 80 8C] = U+200C = бит 1 (ZWNJ)
  D1        = обычный байт
  80        = обычный байт
  D0        = обычный байт
  B8        = обычный байт
  D0        = обычный байт
  B2        = обычный байт
```

Рисунок 2 — HEX-дамп файла stego_text.txt: байты E2 80 8B и E2 80 8C соответствуют скрытым битам

Файл stego_text.txt при открытии в текстовом редакторе выглядит как обычный текст "Привет, мир!" — невидимые символы не отображаются визуально:

ISSN 3030-3907

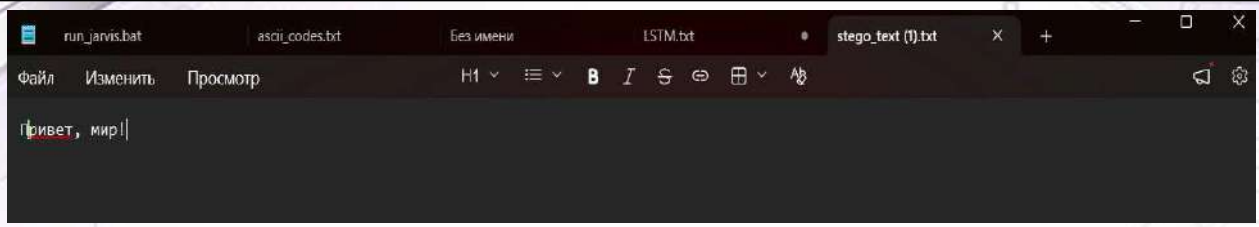


Рисунок 3 — Файл stego_text.txt в текстовом редакторе: визуально неотличим от обычного текста

Стего-текст был скопирован из файла stego_text.txt и отправлен через мессенджер Telegram (функция «Избранное»). При отправке Telegram отобразил сообщение как «Привет, мир!» — невидимые символы были удалены платформой.

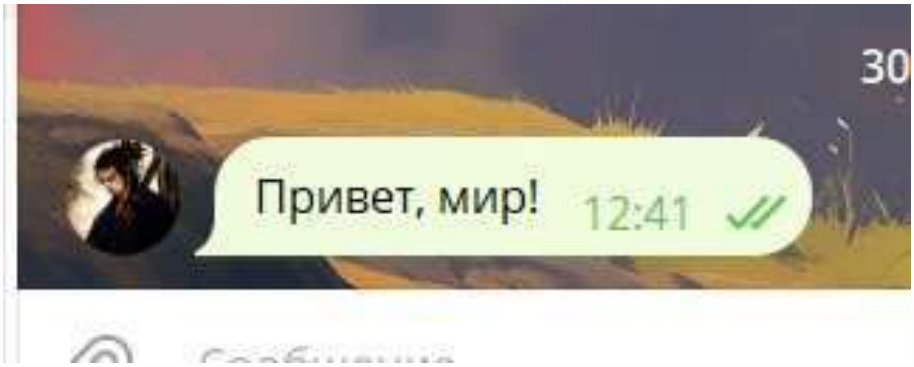


Рисунок 4 — Сообщение в Telegram: ZWC-символы удалены, стего-текст потерян

После копирования текста обратно из Telegram и попытки извлечения скрытого сообщения скрипт нашёл 0 бит — секрет не восстановился. Вывод: Telegram фильтрует символы нулевой ширины при передаче сообщений.

Файл stego_text.txt был пересохранён в кодировке ASCII. Поскольку символы U+200B и U+200C выходят за пределы ASCII (код > 127), они были полностью удалены. После смены кодировки в файле осталось только ", !" (кириллические буквы также не поддерживаются ASCII). Скрытое сообщение было уничтожено.

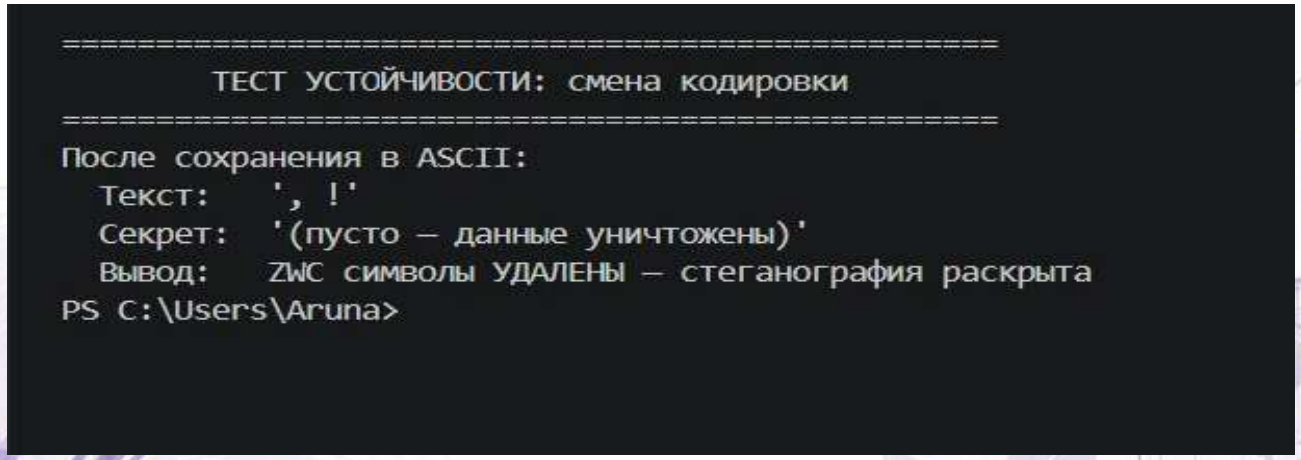


Рисунок 5 — Результат теста: после сохранения в ASCII секрет уничтожен

Спецификация Unicode-стеганографии критически зависит от используемой среды передачи. Символы ***U+200B*** и ***U+200C*** имеют кодовые позиции выше 127. Если стегоконтейнер подвергается процедуре транскодирования или очистки (например, принудительная конвертация из UTF-8 в стандартный 7-битный ASCII или отправка через устаревшие почтовые шлюзы), все символы с кодами выше 127 либо безвозвратно удаляются, либо заменяются на маркеры ошибки (например, знак вопроса «?»). Как результат, скрытая информация полностью уничтожается, что свидетельствует о нулевой робастности (живучести) метода против активного перекодирования.

В ходе анализа уязвимостей кодового пространства Unicode необходимо выделить сопутствующую угрозу безопасности — омоглифические атаки. Поскольку символы разных алфавитов (например, латинская «о» и кириллическая «о») визуально неотличимы, злоумышленники активно используют этот фактор для создания поддельных доменных имен.

Например, в фишинговой строке вида ***google.com*** легитимные латинские символы ***U+006F*** могут быть заменены на кириллические ***U+043E***. Браузер обработает эту строку как совершенно иной сетевой адрес, в то время как пользователь будет уверен, что находится на доверенном ресурсе. Защита от таких атак на современном этапе требует обязательного внедрения систем конвертации доменов в формат Punycode (отображение вида ***xn--...***).

ЗАКЛЮЧЕНИЕ. Разработанный программный комплекс на языке Python подтвердил техническую осуществимость построения скрытых каналов передачи данных внутри стандартных Unicode-текстов с обеспечением абсолютной визуальной незаметности. Метод ZWC позволяет скрывать произвольные текстовые данные внутри обычного текста без каких-либо видимых изменений. Стего-текст визуально идентичен оригиналу, однако на байтовом уровне содержит дополнительные символы U+200B и U+200C, кодирующие биты скрытого сообщения. Обнаружить скрытые данные можно по аномальной длине строки, по наличию байт E2 80 8B / E2 80 8C в HEX-редакторе, а также с помощью специализированного ПО.

Тест устойчивости показал, что Telegram удаляет ZWC-символы при передаче сообщений, что делает данный метод ненадёжным для этой платформы. Смена кодировки файла с UTF-8 на ASCII полностью уничтожает скрытую информацию.

Метод применим для цифровых водяных знаков и маркировки

ISSN 3030-3907

документов, однако уязвим к фильтрации на уровне платформ и смене кодировки. Для надёжной передачи данных через мессенджеры необходимо использовать более устойчивые методы стеганографии.

Текстовая стеганография на основе невидимых управляющих символов Unicode может эффективно применяться только в изолированных средах передачи данных, исключающих автоматизированный HEX-мониторинг трафика и принудительное перекодирование документов.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. – М.: СОЛОН-Пресс, 2017. – 272 с.
2. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография: теория и практика. – К.: МК-Пресс, 2016. – 288 с.
3. Por L. Y., Wong K., Chee B. Information Hiding in Text Document Using Zero-Width Characters // Journal of Computer Science. – 2021. – Vol. 17, No. 3. – P. 244-253.
4. Qurbonaliyevna, X. M. (2025). Korxona va tashkilotlarning axborot-kommunikatsiya tizimlarida vpn tarmoq qurishning zamonaviy yechimlari. Al-Farg‘oniy avlodlari, 1(2), 122-125.
5. Al-Ahmar M. A. High Capacity Text Steganography Using Part of Speech Tagging // International Journal of Computer Science and Security. – 2012. – Vol. 6, No. 1. – P. 44-51.
6. Sotvoldiyeva, D. B., & Husanova, M. K. (2021). Analysis of discrete convolution in the matlab program. In Современные тенденции развития фундаментальных и прикладных наук (pp. 187-191).
7. Gutub A. A. Pixel Indicator Technique for RGB Image Steganography // International Journal of Computer and Information Science. – 2015. – Vol. 4, No. 1. – P. 17-24.
8. M.K.Khusanova (2022). Network security and monitoring. Research Focus, 1 (4), 177-183.
9. Din R. et al. A Review on Text Steganography Techniques, Imaging, and Detection // IEEE Access. – 2022. – Vol. 10. – P. 34512-34528.

ISSN 3030-3907