

Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики

Факультет инфокоммуникационных технологий

Направление подготовки 11.03.02

Практическая работа №1

«Основы защиты информации»

Выполнил:

Швалов Даниил Андреевич

Группа: К34211

Проверил:

Назаров Михаил Сергеевич

Санкт-Петербург

2024

1. Цель работы

Изучить основные понятия защиты информации и уяснить связи между ними.

2. Порядок выполнения работы

- 1) Были организованы группы из числа студентов в составе не менее 12 студентов каждая.
- 2) Каждой из групп была назначена одна из следующих ролей:
 - «Источник информации»;
 - «Приемник информации»;
 - «Нарушители».
- 3) Группа «Источник информации», получив от преподавателя «Сообщение», должна была произвести его шифрование и подготовить шифротекст, которое должно было передаваться в общем канале связи с группами «Нарушителей» и «Приемников».
- 4) Обе подгруппы, получившие шифротекст, должны попытаться его расшифровать и получить исходное «Сообщение». Действовать они должны независимо и втайне друг от друга.
- 5) Группа «Источник информации» может оказывать содействие группе «Приемник информации» в процессе расшифровки, но их действия должны иметь открытый характер, позволяя студентам из группы «Нарушители» получать к ним доступ.
- 6) Запрещается в процессе передачи информации между подгруппами использовать технические средства, препятствовать студентам из подгруппы «Нарушители» получать доступ к передаваемой информации.

2. Ход работы

Первое сообщение


В качестве первого сообщения от преподавателя был получен текст «Тестим игру!».

Подгруппа «Источник информации» воспользовалась шифром Цезаря со сдвигом 31. Зашифрованное сообщение было передано через чат в Zoom.

Его содержание было следующим: «Фжуфко кетх!».

Подгруппа «Приемник информации» не смогла расшифровать сообщение до подгруппы «Нарушители».

Подгруппа «Нарушители» предположила, что в переданном сообщении используется шифр сдвига, скорее всего шифр Цезаря. С помощью онлайн-средств зашифрованное сообщение было расшифровано. Примерные действия нарушителей при расшифровке шифра Цезаря показаны на рисунках 1 и 2.

 Шифр Цезаря

Входной текст
Фжуфко кетх!

Алфавит
Русский

РАССЧИТАТЬ

Рисунок 1 — Онлайн-средство для расшифровки шифра Цезаря

ROT22	Йыйад аэзк!
ROT23	Кэйкбе быил!
ROT24	Люклвё вьйм!
ROT25	Мялмгж гэкн!
ROT26	Намндз дюло!
ROT27	Обноеи еямп!
ROT28	Пвопёй ёанр!
ROT29	Ргпржк жбос!
ROT30	Сдрсэл звпт!
ROT31	Тестим игру!
ROT32	Уётуйн йдсф!

Рисунок 2 — Выбор текста, похожего на реальное сообщение

Второе сообщение

В качестве второго сообщения от преподавателя был получен аудиофайл в формате MP3 с названием `unnamed.mp3`.

Подгруппа «Источник информации» несколько искажила файл, чтобы стандартные средства воспроизведения аудио не смогли проиграть его. После этого файл был передан с помощью чата в Zoom (рисунок 3).

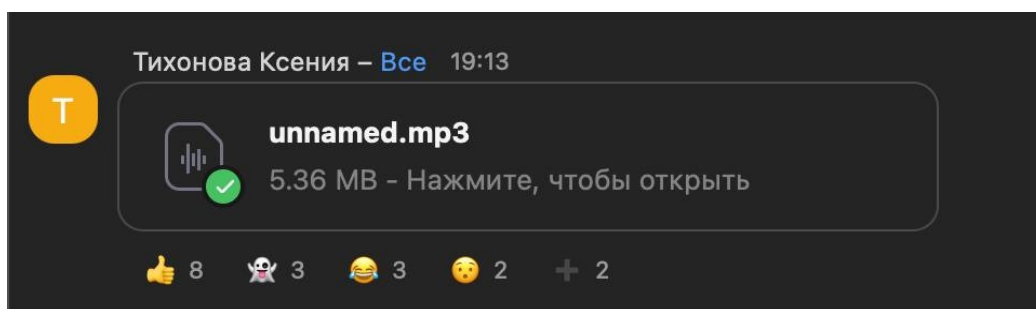


Рисунок 3 — Сообщение в формате MP3-файла

Подгруппа «Приёмник информации» попыталась расшифровать переданное сообщение с помощью автоматизированного распознавания текста из аудио. Также подгруппа попробовала восстановить файл с помощью онлайн средств. Однако данные попытки были безуспешными.

Подгруппа «Нарушители» смогла открыть переданный файл в текстовом редакторе (рисунок 4). Подгруппе удалось распознать изначальное название аудиофайла, а также загрузить похожий аудиофайл в качестве ответа. Однако восстановить исходный файл не удалось.

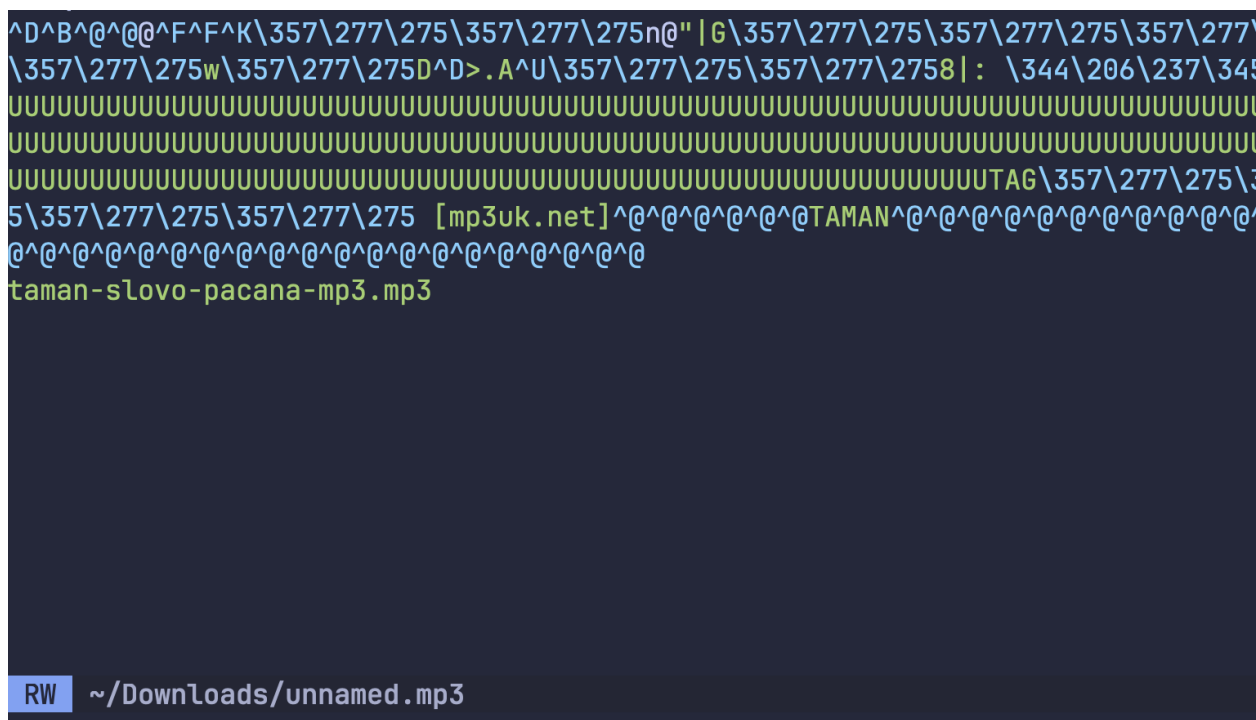


Рисунок 4 — Содержимое MP3-файла в текстовом представлении

Третье сообщение

В качестве третьего сообщения от преподавателя была получена фотография разводных мостов Санкт-Петербурга (рисунок 5).



Рисунок 5 — Третье сообщение в виде фотографии

Подгруппа «Источник информации» сделали ZIP-архив, в который добавили фотографию, а также лишние файлы. Для введения нарушителей в заблуждение расширение архива было изменено с ZIP на DOCX (рисунок 6). Данный архив был передан с помощью чата в Zoom.

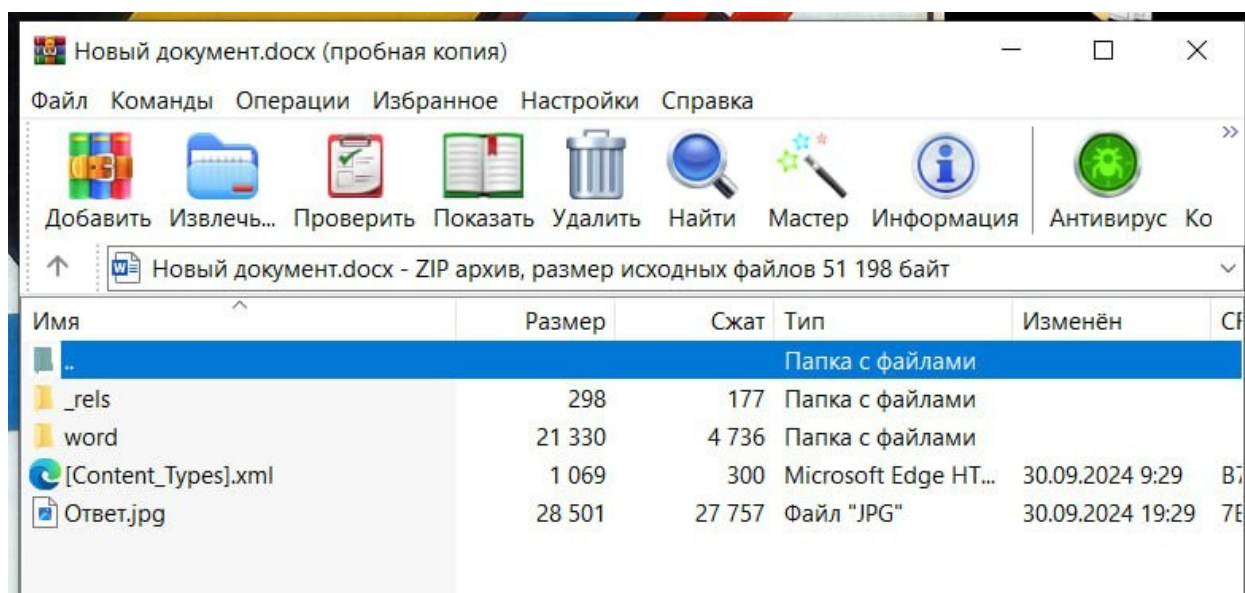


Рисунок 6 — Третье сообщение, архивированное в ZIP

Подгруппа «Приёмник информации» получила архив и смогла понять, что перед ними архив, а не Word-документ. С помощью разархиватора ZIP подгруппа смогла получить доступ к картинке.

Подгруппа «Нарушители» получили архив, но не успели понять, что это не Word-документ до момента дешифровки командой «Приёмник информации».

Четвертое сообщение

В качестве четвёртого сообщения от преподавателя был получен текст «Ничего не понятно, дайте подсказку!!!».

Подгруппа «Источник информации» использовала ночную фотографию Москва-Сити. На фоне неба поверх картинки был написан текст таким образом, чтобы он не выделялся и был практически нечитаемым невооружённым взглядом (рисунок 7). Также к тексту были добавлены лишние слова, чтобы ввести нарушителей в заблуждение. Данная фотография была передана через чат в Zoom.



Рисунок 7 — Фотография, внутри которой закодировано сообщение

Подгруппа «Приёмник информации» смогла обнаружить текст на фотографии. После этого с помощью приближения и изменения контрастности сообщение было расшифровано.

Подгруппа «Нарушители» также обнаружила текст и смогла его расшифровать теми же средствами. Однако это было сделано немного позже подгруппы «Источник информации».

Вывод

В ходе выполнения данной практической работы были изучены основные способы для защиты и передачи информации в зашифрованном виде. В практической работе также были рассмотрены основные принципы защиты информации.