МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Новоуральский технологический институт –
филиал федерального государственного автономного образовательного учреждения
высшего образования «Национальный исследовательский ядерный университет «МИФИ»
(НТИ НИЯУ МИФИ)
Колледж НТИ

Цикловая методическая комиссия информационных технологий

ДОКЛАД
ПО ВНЕАУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЕ НА ТЕМУ

«ШИФР ГРОНСФЕЛЬДА»

ПМ.05 «Разработка программного обеспечения компьютерных сетей»
МДК.05.01 «Защита информации в КС»

Специальность СПО 09.02.03
«Программирование в компьютерных системах»

очная форма обучения
на базе основного общего образования

Выполнил
студент группы КПР–47 Д
Егорушкин И.А. 3.12.2020 
дата подпись

Проверил
преподаватель
Горницкая И.И.
дата подпись

Новоуральск 2020

В современном мире цифровая безопасность является очень важной частью общества. Из-за этого появились разные методы шифрования, одним из них является шифр Гронсфельда. При помощи шифр Гронсфельда можно понять базу шифрования.

Шифр Гронсфельда представляет собой модификацию шифра Цезаря числовым ключом. Для этого под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно, как в шифре Цезаря, но отсчитывают по алфавиту не третью букву, а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа.

Шифр Гронсфельда имеет следующий способ шифрования. Допустим, мы хотим зашифровать слово «ТАЙНЫ», используя ключ «103». Записываем циклически под словом ТАЙНЫ наш ключ, после чего сдвигаем по алфавиту каждую букву на столько букв вперед, сколько указано ниже, получим таблицу 1:

Таблица 1 — Шифр Гронсфельда

Т	А	Й	Н	А
1	0	3	1	0
У	А	М	О	А

Соответственно для дешифровки, сдвиг по алфавиту происходит в обратную сторону.

Теперь ещё пример по шифру Гронсфельда. Есть английские символы + ещё пробел, зашифруем SOURCE CODE (перевод — «исходный код»). Первые 6 символов шифрованного текста по-прежнему будут TSWTDI, как в примере со слово SOURCE и алфавитом без пробела. При этом мы применили один раз все цифры ключа 1422, также пришлось второй раз задействовать 1 и 4.

Далее по алгоритму шифра Гронсфельда задействуем двойку. На очереди пробел, он 26-ой, если A — символ номер 0. (26 + 2) mod 27 = 1, то есть вместо пробела ставим B. Теперь C и вторая двойка в ключе. Если A — номер 0, то C — номер 2. (2 + 2) mod 27 = 4, то есть это E. Далее шифруем O,

все цифры ключа использованы, опять начинаем со старшей (самой левой) цифры, то есть нужен сдвиг на 1, вместо О будет Р. И так далее…

Итог такого будет таблица 2:

Таблица 2 — Шифр Гронсфельда

Алфавит: ABCDE…XYZ_											
Открытый текст	S	O	U	R	C	E	_	C	O	D	E
Применение ключа	1	4	2	2	1	4	2	2	1	4	2
Шифрованный текст	T	S	W	T	D	I	B	E	P	H	G

Шифрация данных очень востребовательна поскольку мы можем зашифровать сообщение так, чтобы только наш оппонент мог их расшифровать.