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

ОТЧЕТ №2
ПО ВНЕАУДИТОРНОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЕ НА ТЕМУ

«Механизмы контроля целостности данных»

ОП.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. _____14.10.2020_____ _____
дата подпись

Проверил
преподаватель _____ _____
Горницкая И.И. дата подпись

Новоуральск 2020

Цель: исследование порядка вычисления и проверки ЭЦП (электронной цифровой подписи)
Задание вариант 2

p	q	e	d	M
17	11	7	23	8866

Отправитель	Получатель
Сообщение:8866 Шаг 1: находим N = p*q=17*11=187 Шаг 2 Найдите два числа e и d которые относительно просты для N и для которого e*d = 1 mod r: N = 187 r = (p-1)*(q-1)=(17-1)*(11-1)=160 Шаг 3 Шифровка по формуле (M)^e mod N Поскольку у нас 8866 надо воспользоваться системой ASCII По которой 8866 = 56,56,54,54 И шифруем каждую цифру по формуле (M)^e mod N, получаем: 56^7 mod 187 =78 78,78,164,164 Шаг 5 отправляем сообщение получателю	Шаг 1 Получаем сообщение 78,78,164,164 Шаг 2 Дешифровка по формуле (M)^d mod N 78^23 mod 187 =56 56,56,54,54 Шаг 3 Используя систему ASCII переводим в 8866 Ответ 8866

Вывод: в ходе работы было выведено способ шифрации и дешифрации данных, а также был изучен порядка вычисления и проверки ЭЦП