МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Задание по практике

Методы обеспечения целостности информации

(наименование дисциплины (модуля) в соответствии с учебным планом)

Уровень	бакалавриат
	(бакалавриат, магистратура, специалитет)
Форма обучения	очная
	(очная, очно-заочная, заочная)
Направление подготовки	09.03.02 «Информационные системы и технологии»
	(код(-ы) и наименование(-я))
Институт	кибербезопасности и цифровых технологий
	(полное и краткое наименование)
Кафедра	«Разработка программных решений и системное программирование»
	(полное и краткое наименование кафедры, реализующей дисциплину (модуль))
Лектор	К.т.н. Ермакова Алла Юрьевна
	(сокращенно – ученая степень, ученое звание; полностью – ФИО)

Используются в данной редакции с учебного года 2023/24

(учебный год цифрами)

Проверено и согласовано «____» _____2023_г. _____ _____

(подпись директора Института/Филиала с расшифровкой)

Москва 2023 г.

ПРАКТИЧЕСКАЯ РАБОТА № 2. АЛГОРИТМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Цель: научиться работать с алгоритмами электронной цифровой подписи (ЭЦП) и правовыми документами по защите информации регламентирующие требования по созданию ЭЦП.

Теоретические вопросы

1. Предмет и задачи электронной цифровой подписи.
2. Основные понятия электронной цифровой подписи.
3. Классификация алгоритмов и протоколов электронной цифровой подписи.
4. Стандарты электронной цифровой подписи и функции хеширования.

Задание 1. Выписать государственные стандарты электронной цифровой подписи. Указать дату принятия стандарта и даты, вносимых в него поправок и изменений, с кратким пояснением сути поправок.

Задание 2. Выписать ФЗ электронной цифровой подписи. Указать дату принятия стандарта и даты, вносимых в него поправок и изменений, с кратким пояснением сути поправок.

Задание 3. Изучить группу стандартов регламентирующих требования по разработке электронной цифровой подписи.

Задание 4. Изучить алгоритм ЭЦП RSA. Рассмотреть пример на своих числах. (смотри таблицу вариантов)

Задание 5. Изучить ЭЦП стандарт DSS. Рассмотреть пример на своих числах. (смотри таблицу вариантов)

Задание 6. Оформить отчет.

Таблица вариантов

Вариант №	p	q
1	23	353
2	29	349
3	31	347
4	37	337
5	41	331
6	43	317
7	47	313
8	53	311
9	59	307
10	61	293
11	67	283
12	71	281
13	73	277
14	79	271
15	83	268
16	89	263
17	97	257
18	101	251
19	103	241
20	107	239
21	109	233
22	113	229
23	127	227
24	131	223
25	137	211