Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студентка: Сятковская Е.Д.

ФИТ 2 курс 4 группа

Минск 2022

**Практическое занятие №14**

**Тема «Изучение стандартных средств для реализации приложений, использующих симметричное и ассиметричное шифрование с использованием библиотеки [System.Security.Cryptography](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography)»**

## *1. Какие симметричные алгоритмы шифрования Вы знаете?*

– Простая перестановка

– Одиночная перестановка по ключу

– Двойная перестановка

– Перестановка «Магический квадрат»

## 2. *Какие ассиметричные алгоритмы шифрования Вы знаете?*

– [RSA](https://encyclopedia.kaspersky.ru/glossary/rsa/)

– Схема Эль–Гамаля

– Алгоритм Диффи–Хеллмана

## 3. *Основное назначение библиотеки System.Security.Cryptography?*

Пространство имен System. Security. Cryptography открывает программный доступ к самым разнообразным криптографическим сервисам, с помощью которых приложения могут шифровать и дешифровать данные, обеспечивать их целостность, а также обрабатывать цифровые подписи и сертификаты.

## *4. Влияет ли размер ключа на криптостойкость алгоритма?*

Да

## *5. Назовите основные классы библиотеки System.Security.Cryptography?*

|  |
| --- |
| – [CryptoStream](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography.cryptostream?view=netstandard-2.1) |
| – [CspParameters](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography.cspparameters?view=netstandard-2.1) |
| – [RijndaelManaged](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography.rijndaelmanaged?view=netstandard-2.1) |
| –[RSACryptoServiceProvider](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography.rsacryptoserviceprovider?view=netstandard-2.1) |