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?***

Потоковые:

· с одноразовым или бесконечным ключом (infinite-key cipher);

· с конечным ключом;

· на основе генератора псевдослучайных чисел

Шифры перестановки (permutation, P-блоки);

Шифры замены (substitution, S-блоки):

· моноалфавитные;

· полиалфавитные;

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

Диффи-Хеллман DH (Diffie, Hellman);

Райвест-Шамир-Адлeман RSA (Rivest, Shamir, Adleman);

Эль-Гамаль (ElGamal).

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

В .NET классы в [System.Security.Cryptography](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography) пространстве имен управляют множеством сведений о криптографии

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

Да

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

* CSPParameters
* RSACryptoServiceProvder
* CryptoStream
* RijndaelManaged