Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Студентка: Чепелева Е.Г.

ФИТ 2 курс 4 группа

Минск 2022

**Практическое занятие №14**

**Контрольные вопросы:**

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

AES, RC5, IDEA, Blowfish, RC4, SEAL, WAKE

1. **Какие ассиметричные алгоритмы шифрования Вы знаете?**

RSA, Эль-Гамаля, Деффи-Хеллмана, DSA, ECDSA

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

Предоставляет криптографические услуги, включая кодирование и декодированние данных, а также множество других операций, таких как хэширование, генерация случайных чисел и аутентификация сообщений.

1. **Влияет ли размер ключа на криптостойкость алгоритма?**

Да, так как чем больше ключ, тем больше времени требуется на реконструкцию такого ключа. Сильным называют шифрование с длиной ключа в 128 бит. Реконструкция такого ключа занимает времени больше, чем возраст Вселенной в миллионы раз. Это технически невозможно, если не известны какие-либо ещё данные для расшифровки ключа.

1. **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) |