**Лабораторная работа №2**

**Изучение аппаратных методов защиты информации   
с помощью смарт-карт e-Token PRO**

**Цель работы.** Изучение основных возможностей защиты информации с помощью смарт-карт; применение методов криптографической защиты информации на примере смарт-карт e-Token PRO на практике; изучение области применяемости смарт-карт в России и в международной практике, оценке стойкости различных типов смарт-карт, возможных способах атак на контактные и бесконтактные смарт-карты.

**Подготовительный этап.** На данном этапе необходимо:

Изучить основные функции аутентификации и шифрования при помощи смарт-карт, ознакомиться со способами интеграции защитных функций смарт-карт   
e-Token PRO в разрабатываемые приложения.

**Порядок выполнения работы.**

Написать программу, которая работает со смарт картой e-Token PRO. Необходимо в программе выполнить как минимум следующие действия:

1. Получить список доступных функций (GetFunctionList).

2. Выполнить инициализацию PKCS # 11 библиотеки (C\_Initialize).

3. Получить список имеющихся слотов (C\_GetSlotList).

4. Получить информацию о слоте (C\_GetSlotInfo).

5. Получите информацию о токене (C\_GetTokenInfo()).

6. Отобразить информацию о токене (см. определение CK\_TOKEN\_INFO для получения дополнительных сведений).

7. Открыть сессию работы с токеном (C\_OpenSession)

8. Произвести авторизацию с пользовательским уровнем доступа (C\_Login, PIN 1234567890).

9. Инициализировать параметры шифрования и генерации ключа.

10.Сгенерировать ключ шифрования (C\_GenerateKey).

11. Инициализировать процедуру шифрования (C\_EncryptInit) и зашифровать произвольный буфер с информацией (какой-либо строкой) с помощью функций e-Token PRO (C\_Encrypt).

12. Проверить корректность выполненного шифрования (расшифровать данные) (C\_DecryptInit, C\_Decrypt).

13. Разлогиниться и закрыть сессию (C\_Logout, C\_CloseSession).

**Содержание отчета**

1. Описание используемых в лабораторной работе функций eToken Pro.
2. Листинг кода.

**Контрольные вопросы:**

1. Опишите назначение старт-карт.
2. Опишите основные виды смарт-карт.
3. Опишите архитектуру смарт-карт.
4. Какие стандарты безопасности смарт-карт Вы знаете?
5. Какие методы атак на смарт-карты Вам известны?
6. Какие модели смарт-карт eToken Вы знаете?
7. Опишите основные области памяти смарт-карт eToken Pro.
8. Опишите основные уровни доступа к информации на смарт-карте.
9. Раскройте основные элементы архитектуры программного обеспечения смарт-карт.
10. Опишите основные функции интерфейса PKCS#11.
11. Какие группы функций PKCS#11 Вам известны?
12. Опишите назначение и функции программы eToken Properties.