УДК 004.312

Афанасенков А.С., Кучинский П.В., Петрунин А.П.

ИСПОЛЬЗОВАНИЕ КАРТОЧНЫХ ТЕХНОЛОГИЙ ДЛЯ ЗАЩИТЫ ПЭВМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Разработан и изготовлен программно-аппаратный комплекс, позволяющий с использованием электронных пластиковых карт обеспечить защиту от несанкционированного доступа информации, обрабатываемой и хранимой на ПЭВМ. Комплекс реализует генерацию и защищенное хранение криптографических ключей, шифрование информации, электронную цифровую подпись, доступ к ПЭВМ авторизованных пользователей.

В настоящее время с учетом активного внедрения во все сферы жизни общества современных информационных технологий особую актуальность приобретают вопросы обеспечения защиты информации. При построении и использовании современных информационно-коммуникационных систем важно обеспечить конфиденциальность и целостность обрабатываемой информации, ее защиту от несанкционированного доступа, а также подтверждение авторства.

Задача защиты информации имеет комплексный характер. Ее решение в целях обеспечения требуемого уровня защиты от несанкционированного доступа (НСД) информации, обрабатываемой в персональных электронных вычислительных машинах (ПЭВМ) с операционными системами (ОС) семейств Windows и Linux, достигается путем применения комплекса программно-технических средств и организационных мероприятий.

Разработанный и изготовленный программно-аппаратный комплекс (ПАК) «Подпись» функционирует в ОС Windows 2000/XP и ОС Ubuntu Linux, использует технологии, базирующиеся на электронных пластиковых картах (ЭПК), и обеспечивает:
а) защиту обрабатываемой и хранимой в ПЭВМ информации с применением криптографических преобразований;
б) защиту от НСД к ПЭВМ неавторизованных пользователей;
в) защищенное хранение криптографических ключей, информации о пользователе и аутентификационных данных в USB-ключе;
г) создание криптографических ключей с использованием генератора случайной числовой последовательности (ГСЧП) ЭПК;
д) аутентификацию в сетях под управлением Active Directory (для серверов под управлением ОС Windows 2003 и рабочих станций под управлением ОС Windows 2000/XP).
В ПАК «Подпись» реализованы следующие криптографические функции:

- шифрование по ГОСТ 28147-89 (аппаратная и программная реализации);
- шифрование по СТБ П 34.101.31-2007 (программная реализация);
- вычисление и проверка ЭЦП по СТБ 1176.2-99, а также хэш-значения по СТБ 1176.1-99 и СТБ П 34.101.31-2007 (программная реализация).

ПАК «Подпись» представляет собой комплекс, который в аппаратной части взаимодействует с ПЭВМ посредством USB-интерфейса, а в программной части встраивается в подсистему безопасности ОС (рисунок 1).

Аппаратная часть ПАК «Подпись» состоит из USB-ключа, который содержит отчуждаемый портативный карт-ридер с USB интерфейсом и встроенную в него ЭПК доступа (ЭКД), представляющую собой ЭПК формата SIM-PLUGIN (рисунок 2). В качестве ЭПК в ПАК «Подпись» выбрана ЭПК с ОС «Магистра» на базе микроконтроллера ST19NR66 [1].

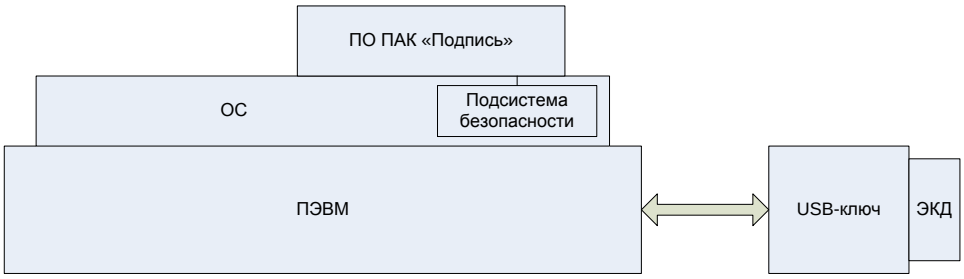

Рисунок 1 – Схема взаимодействия ПАК «Подпись» с ПЭВМ

Применение ЭПК с ОС «Магистра» на базе микроконтроллера ST19NR66 позволяет использовать аппаратное шифрование по алгоритму ГОСТ 28147 и реализовать разграничение доступа к криптографическим ключам, информации о пользователе и аутентификационным данным.

В ПАК «Подпись» также реализована возможность использования полноразмерной ЭПК и стационарного считывателя ЭПК вместо USB-ключа, что значительно уменьшает стоимость комплекса.

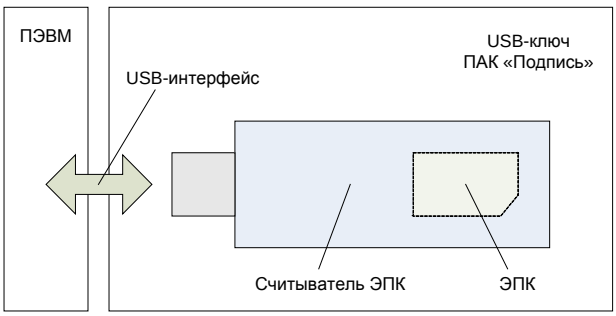

Рисунок 2 – Функциональная схема USB-ключа

Программная часть ПАК «Подпись» включает следующее программное обеспечение (ПО): модуль администрирования, модуль конфигурирования, модуль тестирования, модуль управления подсистемой защиты данных, модуль управления подсистемой контроля доступа, защищённый журнал аудита, криптографический сервер, модуль аутентификации, модуль работы с USB-ключами.

ПАК «Подпись» обеспечивает защиту ПЭВМ от НСД со стороны неавторизированных пользователей посредством двухфакторной аутентификации. В ПАК «Подпись» используются два элемента аутентификации: персональный идентификационный объект и персональный пароль пользователя, что предотвращает НСД к ПЭВМ при хищении одного из них.

В качестве персонального идентификационного объекта в ПАК «Подпись» используется USB-ключ, а в качестве персонального пароля пользователя – короткий ПИН-код, который хранится пользователем в тайне. Защищённость от атаки перебором поддерживается за счёт ограничения числа попыток ввода ПИН-кода, после чего ЭКД переходит в фазу блокирования, выход из которой возможен только по предъявлению пользователем персонального разблокировочного кода (ПРК-кода), также хранимого пользователем в тайне. Количество попыток ввода ПРК-кода ограничено, после чего наступает необратимое блокирование ЭКД.

Ключевая информация в ПАК «Подпись» создается на основе случайной числовой последовательности, полученной с ГСЧП ЭПК, и хранится в защищенной от НСД области ЭПК, что снижает риски компрометации зашифрованной информации.

ПО ПАК «Подпись» встраивается в ОС и внедряется в её политику разграничения доступа. Для разграничения доступа к объектам на этапе активации создаются две группы операторов ПАК «Подпись»: администраторы, обладающие полномочиями по управлению подсистемой контроля доступа, настройками безопасности и аудита; пользователи, которым доступны только криптографические функции.

Информация, занесенная в USB-ключ администратором на конкретной ПЭВМ с установленным ПО ПАК «Подпись», привязывает USB-ключ к определённой учётной записи ОС данной ПЭВМ. Имеется также возможность многопользовательской привязки для использования администратором одного USB-ключа на разных ПЭВМ.

Разработанный ПАК «Подпись» не имеет полных аналогов в Республике Беларусь. К его достоинствам относятся:

– встраиваемость в ОС семейства Windows и Linux, что позволяет в полной мере использовать их политику безопасности;

– двухфакторная аутентификация оператора, что позволяет освободить пользователя от необходимости запоминания различных имен и паролей – достаточно знать только свой ПИН-код;

– реализация национальных стандартов криптопреобразований;

– генерация и защищенное хранение ключевой информации в ЭПК USB-ключа.

ПАК «Подпись», являясь современным техническим средством защиты информации, имеет потенциал для дальнейшего развития в следующих направлениях:

– создание вместо стандартного считывателя ЭПК собственной высокопроизводительной аппаратной платформы, реализующей национальные алгоритмы криптографических преобразований;

– встраивание и/или подключение к аппаратному устройству флэш-памяти для организации защищенного хранения пользовательских данных (создание открытого и закрытого для доступа извне разделов);

– загрузка ОС в режиме «только чтение» с аппаратного устройства для работы с защищаемыми данными закрытого раздела (шифрование, подпись) с возможностью их выгрузки на открытый раздел устройства;

– создание криптопровайдера для ОС Windows и использование возможностей аппаратного устройства в протоколе SSL.

Список литературы

1. ООО «ПрограмПарк», [Электронный ресурс]/ Сайт ООО «ПрограмПарк», http://programpark.ru/smart/.

We designed and manufactured a smart card system for protecting information processed and stored on a PC from an unauthorized access. The system integrates hardware and software components to generate and securely store cryptographic keys, encrypt information, provide digital signing capabilities, and control computer logon and access.

Афанасенков А.С., с.н.с. НИИПФП им. А.Н.Севченко БГУ, Минск, Беларусь, e-mail: afanasenkov.andrey@gmail.com