УДК 004.942

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ РАБОТЫ С ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСЬЮ И ОБЕСПЕЧЕНИЯ ШИФРОВАНИЯ ДАННЫХ

Зелинский И.П.,
научный руководитель доц. Лапина Л.А., ст. преподаватель Лапина Е.В.
Сибирский федеральный университет

Информация в современном обществе приобрела коммерческую ценность и стала широко распространенным, почти обычным товаром. Её производят, хранят, транспортируют, покупают и продают и, как следствие, воруют и подделывают. В связи с этим встала проблема защиты обмениваемой и хранимой информации. Современное общество все в большей степени становится информационно-обусловленным, успех любого вида деятельности все сильней зависит от обладания определенными сведениями и от отсутствия их у конкурентов. И чем сильней проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере, и тем больше потребность в защите информации.

Среди всего спектра методов защиты данных от несанкционированного доступа особое место занимают криптографические методы. В отличие от других методов, они опираются лишь на свойства самой информации и не используют свойства ее материальных носителей, особенности узлов ее обработки, передачи и хранения.

На сегодняшний день существует огромное количество программных продуктов криптографической защиты информации, но многие из них, за явным исключением, обладают рядом минусов, одним их которых является отсутствие обучающего модуля для обычных пользователей. Пользователь обычно не имеет ни малейшего представления о методах шифрования данных и о том, как правильно использовать тот или иной метод. В связи с этой проблемой было решено разработать такой программный продукт, который не просто может быть использован в качестве криптографической защиты информации, но и сможет обучить пользователей основам защиты данных, а так же наглядно показать работу основных методов защиты, что называется, изнутри.

Таким образом, разработанный программный продукт представляет собой программу для реализации в прикладном программном обеспечении функций криптографической защиты информации - применения электронной цифровой подписи (ЭЦП) и шифрования с, так называемым, HELP-приложением. Такой программный продукт может применяться практически в любых системах различного уровня и назначения, нуждающихся в использовании средств ЭЦП и шифрования, кроме того, может использоваться и непосредственно пользователем MS Windows для подписи и шифрования файлов в проводнике MS Windows. Программа написана на высокоуровневом языке программирования C++ с использованием интерфейса MicrosoftCryptoAPI, который является основой средств защиты MicrosoftInternetSecurityFramework. Он позволяет создавать приложения, использующие криптографические методы и обеспечивает базовые функции защиты для безопасных каналов и подписи кода.

Программа работает в трех режимах:

1. обучение основам криптографической защиты информации с возможностью наглядного представления в виде схем, изображений и обучающих FLASH-роликов;

2. пошаговый режим работы с краткими объяснениями на каждом шаге работы с возможностью видеть, что происходит на каждом этапе шифрования или использования ЭЦП;

3. обычный режим (режим профи), используемый непосредственно для применения ЭЦП и шифрования в форсированном режиме.

Основные функции, реализованные в программе:

- формирование и проверка корректности ЭЦП;
- подпись и шифрование;
- расшифрование и проверка корректности ЭЦП;
- управление сертификатами и ключами пользователя;
- управлениекриптопровайдерами.

Программа обеспечивает возможность использования криптопровайдеров, входящих в состав Windows:

- Microsoft Base Cryptographic Provider;
- Microsoft Strong Cryptographic Provider;
- Microsoft Enhanced Cryptographic Provider;
- Microsoft AES Cryptographic Provider;
- Microsoft DSS Cryptographic Provider;
- MicrosoftBase DSS andDiffie-HellmanCryptographicProvider;
- Microsoft DSS andDiffie-Hellman/SchannelCryptographicProvider;
- Microsoft RSA/SchannelCryptographicProvider.

Все они отличаются друг от друга своими типами, которые определяются набором параметров, включающим:

- алгоритм обмена сессионным (симметричным) ключом;
- алгоритмвычислениецифровойподписи;
- форматцифровойподписи;
- схема генерирования сессионного ключа по хешу;
- длинаключа.

В зависимости от выбора криптопровайдера, пользователю предоставляется выбор алгоритмов шифрования и хэширования. Алгоритмы шифрования и хэшированияот выбора типа криптопровайдера приведены в таблице 1.

Таблица 1 – Использование алгоритмов криптопровайдерами

Тип криптопровайдера	**Алгоритмы ключевого обмена**	**Алгоритмы цифровой подписи**	**Алгоритмы шифрования**	**Алгоритмы хеширования**
PROV_RSA_FULL	RSA	RSA	RC2,RC4	MD5,SHA
PROV_RSA_AES	RSA	RSA	RC2,RC4,AES	MD5,SHA
PROV_RSA_SIG	-	RSA	-	MD5,SHA
PROV_RSA_SCHANNEL	RSA	RSA	RC4,DES,3DES	MD5,SHA
PROV_DSS	-	DSS	-	MD5,SHA
PROV_DH_SCHANNEL	DH	DSS	DES,3DES	MD5,SHA
PROV_MS_EXCHANGE	RSA	RSA	CAST	MD5,SHA
PROV_SSL	RSA	RSA	РАЗЛИЧНЫЕ	РАЗЛИЧНЫЕ
PROV_GOST_2001_DH	ГОСТ Р 34.10-2001	ГОСТ Р 34.10-2001	ГОСТ 28147-89	ГОСТ 28147-89

Обучающий модуль разработан в виде HELP-приложения, с помощью языка разметки гипертекста HTML и языка программирования JavaScript. Особое внимание в обучающем модуле уделяется проблеме использования ЭЦП в системах электронного документооборота и юридически значимого электронного документооборота, в прикладных системах персонального использования. В HELP-приложении для изучения и ознакомления с ЭЦП вынесены следующие разделы:

- Общиеположения;
- Историясоздания;
- Сферыприменения;
- Функционирование ЭЦП;
- Виды ЭЦП;
- Средстваработы с ЭЦП;
- Атакина ЭЦП.

В разделе «Общие положения» включены законодательные аспекты обеспечения правовых условий использования электронной цифровой подписи в электронных документах, описаны действующие федеральные законы об использовании ЭЦП, рассмотрены основные понятия и определения. В разделе «Функционирование ЭЦП» представлены FLASH-ролики и схемы функционирования ЭЦП, ее создания и проверки.

Разработанный программный комплекс предназначен в первую очередь для студентов специальности «Информационные системы и технологии», изучающих дисциплину «Информационная безопасность и защита информации». Так же программный продукт будет полезен специалистам, работающим с электронным документооборотом, и всем желающим получить, обновить или восполнить знания в направлении криптографической защиты информации, ЭЦП, шифрования. В программе реализованы функции управления сертификатами, криптопровайдерами, реализована работа с ЭЦП и шифрованием, а значит программа будет полезна всем пользователям, которые хотят защитить личные файлы в проводнике MS Windows.