МЕТОДИКА ВСТРАИВАНИЯ ОТЕЧЕСТВЕННЫХ КРИПТОАЛГОРИТМОВ В *Microsoft Office*

Панасенко С.П., начальник отдела разработки программного обеспечения фирмы "АНКАД"

Одним из основных направлений научно-технического прогресса в настоящее время является компьютеризация и автоматизация различных этапов и направлений деятельности организаций. Характерным примером компьютеризации является неуклонный переход с бумажного документооборота на электронный. Развитие компьютерных и информационных технологий позволяет автоматизировать все этапы жизненного цикла документов: от его составления и редактирования до пересылки с помощью различных средств передачи информации и/или электронных сообщений по компьютерным сетям. Возможности современных средств создания и редактирования электронных документов (ЭД) позволяют как значительно ускорить данный процесс, так и достичь качественного улучшения характеристик ЭД по сравнению с печатным документом.

Пакет программ Microsoft Office

Одним из наиболее распространенных в настоящее время пакетов офисных программ является пакет программ Microsoft Office. Microsoft Office представляет собой набор программных средств, позволяющих, например, автоматизировать документооборот организаций. В различные варианты поставки Microsoft Office могут входить следующие компоненты:

- Текстовый процессор Microsoft Word.
- Программа обработки электронных таблиц Microsoft Excel.
- СУБД Microsoft Access.
- Диспетчер задач, контактов и почтовых сообщений Microsoft Outlook.
- Программа создания презентаций Microsoft PowerPoint.
- Графический редактор Microsoft PhotoDraw.
- Редактор HTML Microsoft FrontPage.

Рассмотрим, прежде всего, текстовый процессор Microsoft Word, являющийся ключевым элементом пакета Microsoft Office и получивший наибольшее распространение. По оценке, приведенной в [1], Microsoft Word занимает около 80% рынка текстовых процессоров в мире. Согласно [2] в мире продано более 120 миллионов экземпляров Microsoft Office.

Такой успех объясняется, прежде всего, огромной функциональностью Microsoft Word, обладающего целой гаммой встроенных средств обработки текстовой и графической информации в различных форматах. Кроме того, Microsoft Word содержит встроенный язык программирования VBA (Visual Basic for Applications), позволяющий исключительно гибко менять как собственную функциональность, так и пользовательский интерфейс. Огромные возможности VBA позволяют строить целые системы масштаба предприятия, базирующиеся на использовании Microsoft Word и других программ комплекса Microsoft Office [1, 3, 4, 5].

Однако, у данного программного продукта есть и недостатки (присущие и другим программам пакета). Один из них - недостаточная защита содержимого ЭД от просмотра и модификации. Рассмотрим систему защиты документов Microsoft Word версий 97 и 2000 (Здесь и далее будут иметься в виду только данные версии Microsoft Word, поскольку только они являются актуальными на данный момент).

Microsoft Word дает возможность пользователю установить две степени защиты редактируемого ЭД:

- защита документа от прочтения,
- защита документа от модификации.

Установить защиту текущего (т.е. открытого в данный момент времени для просмотра и/или редактирования) ЭД можно с помощью меню Microsoft Word "Сервис/Параметры", после выбора которого на экран выводится диалоговое окно, содержащее параметры текущего ЭД. В данном окне присутствует вкладка "Сохранение", содержащая, помимо прочих параметров сохранения документа, две опции, с помощью которых можно установить защиту ЭД:

- "Пароль для открытия файла".
- "Пароль разрешения записи".

Путем ввода соответствующих паролей (или одного из них) в указанные поля, пользователь может указать текстовому процессору, что текущий ЭД необходимо зашифровать с использованием введенных паролей в качестве исходных данных для формирования ключа шифрования. Это сохранит конфиденциальность ЭД. Целостность ЭД обеспечивается применением пароля на запись. Однако, несмотря на всю полноту механизма защиты документов Microsoft Word 97 (аналогичный механизм присутствует в Microsoft Word 2000), ему присущ ряд недостатков, делающих бесполезным его применение [3, 6, 7, 8]:

1. В отличие от криптографического ключа, сформированного с помощью датчика случайных чисел (ДСЧ), пароли пользователей очень легко подобрать из-за небрежного отношения боль-

шинства пользователей к выбору пароля. Часто встречаются случаи выбора легко предугадываемых паролей, например:

- пароль эквивалентен имени пользователя (или имени пользователя в обратном порядке, или производной от имени пользователя);
- паролем является слово или фраза; такие пароли подбираются за ограниченное время путем атаки по словарю, содержащему все слова используемого языка (или нескольких) и общеупотребительные фразы, с помощью соответствующей утилиты подбора;
- достаточно часто пользователи применяют короткие пароли, которые взламываются методом "грубой силы" (brute-force attack), то есть простым перебором; стоит отметить, что Microsoft Word ограничивает длину вводимых паролей 15 символами, что несколько упрощает задачу прямого перебора паролей.

2. Существуют и свободно доступны множество утилит подбора паролей, в том числе, специализированных для конкретных программных средств. Например, в [3] описана утилита подбора пароля для ЭД Microsoft Word 2000, предназначенная для восстановления доступа к документу, если его владелец забыл пароль. Несмотря на данное полезное назначение, ничто не мешает использовать эту и подобные ей утилиты для взлома чужих паролей.

3. В связи с существовавшими экспортными ограничениями США, все программные продукты, поставляемые в другие страны, не должны были содержать сильную криптографию. При использовании сильных криптографических алгоритмов слабость криптографии в экспортных версиях достигалась урезанием длины используемых криптографических ключей, что делало такую защиту неэффективной, поскольку короткие ключи позволяли использовать метод "грубой силы". Однако, проблема экспортных версий не имеет прямого отношения к Microsoft Word, поскольку ограничение длины пароля позволяет успешно атаковать путем перебора паролей независимо от длины ключа шифрования.

Из всего сказанного выше следует, что Microsoft Word и другие программы пакета Microsoft Office, в случае их использования для обработки конфиденциальной информации, нуждаются в дополнительном использовании средства криптографической защиты информации (СКЗИ). Рассмотрим методику разработки и встраивания СКЗИ в программы пакета Microsoft Office.

Методика встраивания СКЗИ

Прежде всего, уточним задачу:

1. СКЗИ должна быть максимально близкой к пользователю, т.е. иметь интерфейс, встроенный непосредственно в программы пакета. Это необходимо именно в связи с огромной распространенностью Microsoft Office, что означает широкий круг пользователей различной квалификации. Встроенность интерфейса СКЗИ в знакомый пользователю Microsoft Word позволит существенно упростить процесс обучения работе с СКЗИ даже для низкоквалифицированных, но имеющих опыт работы с Microsoft Word, пользователей.

2. В основе СКЗИ должны лежать именно отечественные криптоалгоритмы, что позволит не ограничивать потенциальный рынок СКЗИ только коммерческими организациями. Отсутствие сертификата ФАПСИ на СКЗИ не дает возможность использования СКЗИ в Государственных органах и организациях РФ, организациях, выполняю-

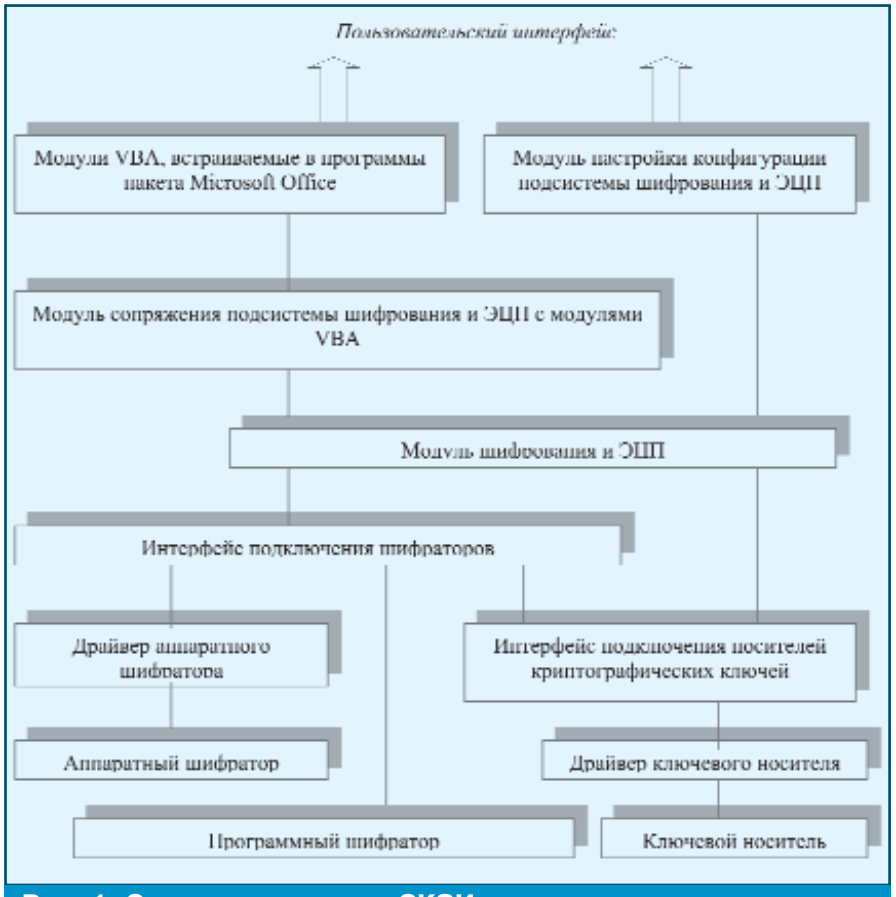

Рис. 1. Структурная схема СКЗИ

щих оборонные заказы РФ, и организациях или частных лицах, обменивающихся конфиденциальной информацией с Государственными органами и организациями РФ, а также организациями, выполняющими оборонные заказы РФ [9]. А Положение ФАПСИ о системе сертификации СКЗИ [10] устанавливает следующее требование к используемым в сертифицируемых СКЗИ криптоалгоритмам: "Заявки на проведение сертификации шифровальных средств принимаются при условии, что в указанных средствах реализованы криптографические алгоритмы, объявленные государственными или отраслевыми стандартами Российской Федерации, иными нормативными документами, утвержденными Советом Министров - Правительством Российской Федерации или ФАПСИ".

3. Необходима модульная структура СКЗИ, что позволит легко распространять использование СКЗИ на различные программные продукты (прежде всего, входящие в состав пакета Microsoft Office). Кроме того, на нижнем уровне модульность СКЗИ позволит использовать различные шифраторы (как программные, так и аппаратные) при условии унифицированности их интерфейса.

4. Помимо шифрования для защиты конфиденциальности ЭД, СКЗИ должна обеспечивать и их целостность с помощью электронной цифровой подписи (ЭЦП).

Рассмотрим модульную структуру СКЗИ. В качестве отправной точки для собственной разработки СКЗИ автором данной статьи была разработана и принята методика встраивания СКЗИ, опирающаяся на структуру СКЗИ, представленную на рис. 1. Назначение модулей структуры:

1. Модули VBA. Предназначены для обработки действий пользователя, относящихся к интерфейсу СКЗИ. Следует учесть, что могут быть две принципиально различных методики активизации СКЗИ: по требованию пользователя (отработка действий пользователя с элементами управления собственного интерфейса СКЗИ) и событийная (перехват и обработка стандартных действий пользователя, например, открытия файла встроенными средствами Microsoft Word). Выбор методики активизации зависит, прежде всего, от возможностей конкретной реализации языка VBA в конкретной программе пакета Microsoft Office.

2. Модуль шифрования и ЭЦП. Библиотека динамической компоновки (DLL - Dynamic Linked Library), экспортирующая стандартный набор функций шифрования и ЭЦП по отечественным алгоритмам ГОСТ 28147-89, ГОСТ Р 34.10-94 и ГОСТ Р 34.11-94 на уровне файлов: зашифрование/расшифрование файла, расчет и проверка ЭЦП файла. Опционально может содержать функции генерации ключей шифрования и ЭЦП в требуемых данной DLL форматах, а также встроенное протоколирование всех выполняемых операций.

3. Модуль сопряжения подсистемы шифрования и ЭЦП с модулями VBA. Предназначен выполнять две задачи: во-первых, должен компенсировать недостаточные возможности языка VBA, что позволит упростить встраивание библиотеки шифрования и ЭЦП (вместо реализации дополнительных интерфейсов и функциональности на VBA существенно проще использовать, например, более гибкий язык С++); во-вторых, существенно облегчает код VBA-модулей, что позволяет не обеспечивать блокировку их просмотра пользователем ввиду отсутствия элементов ноу-хау.

4. Модуль настройки конфигурации библиотеки шифрования и ЭЦП. Функциям шифрования и ЭЦП необходим большой набор параметров, которые должны быть легко доступны для изменения в процессе работы, прежде всего, указание конкретных криптографических ключей, с помощью которых выполняется шифрование и ЭЦП, или места их расположения.

5. Интерфейс подключения шифраторов. Должен предоставлять программам верхнего уровня стандартные функции шифрования блоков памяти и выработки имитоприставок для данных по алгоритму ГОСТ 28147-89 (опционально - функции ДСЧ для генерации криптографических ключей). Снизу должен иметь возможность подключения драйверов устройств шифрования, обладающих унифицированным интерфейсом, или программного шифратора, выполненного в виде драйвера с тем же интерфейсом.

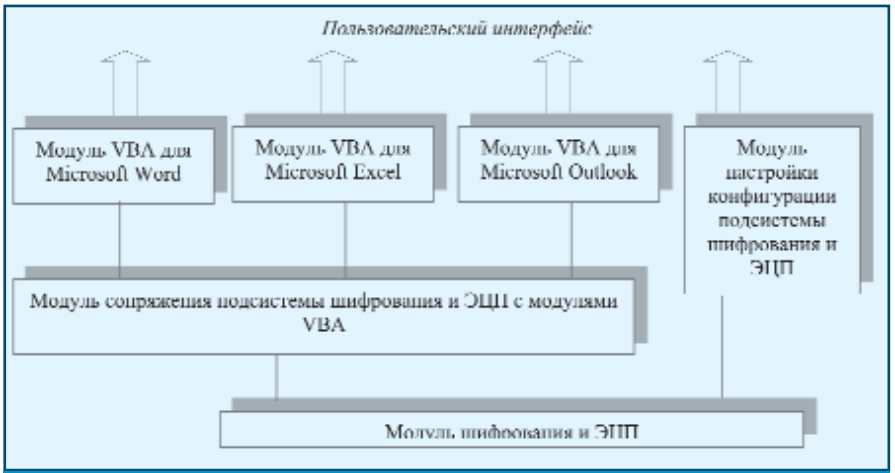

Рис. 2. Интерфейсная часть СКЗИ для Microsoft Word, Excel и Outlook

6. Интерфейс подключения ключевых носителей. Аналогично предыдущему, должен предоставлять программам верхнего уровня стандартные функции чтения ключевых файлов с носителей, подключаемых через драйверы с унифицированным интерфейсом. Если в качестве ключевых носителей планируется использование только стандартных устройств (прежде всего, дискет), то в данном модуле нет необходимости.

Как видно из структуры, на верхнем уровне может быть модуль, встроенный в любую программу пакета Microsoft Office, а также в любой другой программный продукт, имеющий встроенный язык высокого уровня, аналогичный VBA, или позволяющий получить доступ к функциональности с помощью OLE Automation (технология передачи данных и взаимодействия различных программ) или аналогичной технологии.

Дополнительным плюсом такой системы была бы возможность подключения криптографических ключей различных форматов, что позволило бы использовать СКЗИ, в частности, в инфраструктуре открытых ключей (PKI - Public Key Infrastructure). Конечно, это при условии открытого распределения ключей СКЗИ, что реально сделать и для симметричного алгоритма ГОСТ 28147-89, если применить алгоритм Диффи-Хеллмана для динамического вычисления ключей парной связи из пары "свой секретный ключ + чужой открытый ключ". Дополнительным плюсом такой схемы является унификация ключей ЭЦП и ключей, на основе которых вычисляются ключи парной связи [11, 12].

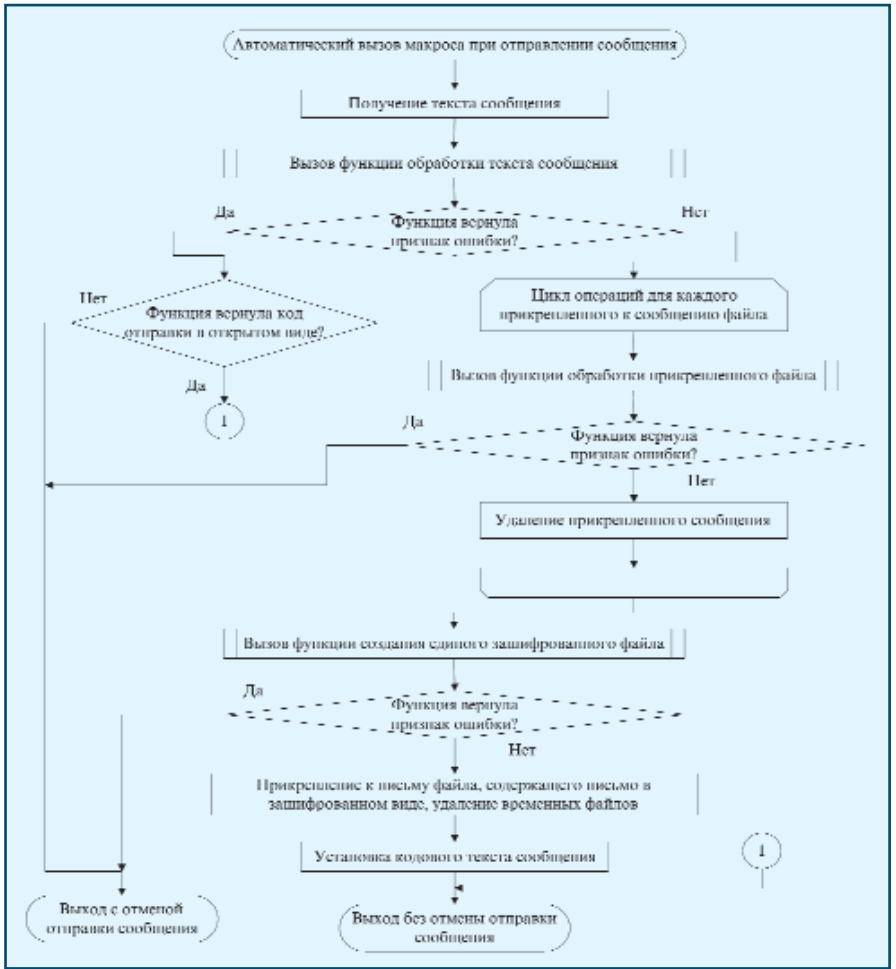

Рис. 3. Алгоритм защиты сообщения электронной почты

Реализация

Для защиты автором выбраны три, на его взгляд, наиболее популярных программных продукта пакета Microsoft Office:

- Текстовый процессор Microsoft Word.
- Программа обработки электронных таблиц Microsoft Excel.
- Диспетчер задач, контактов и почтовых сообщений Microsoft Outlook.

Объекты защиты: ЭД Microsoft Excel и Microsoft Word, а также сообщения электронной почты и их вложения, отправляемые с помощью Microsoft Outlook.

В соответствии с принципом повторного использования кода [1], в целях обеспечения совместимости с уже существующими программными продуктами, выполняющими шифрование и ЭЦП по упомянутым выше алгоритмам, и в целях уменьшения времени разработки использованы следующие программные продукты (производства фирмы "АНКАД"), отвечающие изложенным выше требованиям:

- Библиотека Crypton ArcMail для Windows - в качестве модуля шифрования и ЭЦП, а также несколько модифицированная программа ее конфигурирования.
- Программное обеспечение Crypton API, содержащее универсальный интерфейс подключения шифраторов, а также интерфейс подключения ключевых носителей.

Таким образом, задача разработки СКЗИ практически свелась к следующим пунктам:

1. Модули VBA для Microsoft Word, Excel и Outlook.
2. Модуль сопряжения.
3. Программы инсталляции и деинсталляции СКЗИ.

А верхняя часть структурной схемы, представленной на рис. 1, модифицировалась в соответствии с задачей, как показано на рис. 2.

Согласно принципу приближения интерфейса СКЗИ к работающему в Microsoft Word пользователю, интерфейс СКЗИ встраивается в основной шаблон Microsoft Word Normal.dot в виде дополнительной панели инструментов, содержащей 4 кнопки для выполнения различных действий с СКЗИ:

- "Подписать и зашифровать". Предназначена для защиты текущего документа (создания защищенного документа) Microsoft Word.
- "Открыть защищенный документ". Предназначена для открытия подписанного и зашифрованного ранее документа.
- "Настройка". Предназначена для вызова программы настройки конфигурации модуля шифрования и ЭЦП СКЗИ. Конфигурация модуля шифрования и ЭЦП является одинаковой для всех трех программ Microsoft Office, независимо от того, из какой программы (или из Главного меню Windows) была вызвана программа настройки.
- "Справка". Предназначена для вызова эксплуатационной документации СКЗИ. Документация загружается в качестве текущего документа Microsoft Word.

В тот же основной шаблон Normal.dot на этапе инсталляции СКЗИ встраиваются макросы VBA-модуля, обеспечивающие обработку нажатий кнопок панели инструментов СКЗИ.

Совершенно аналогично выглядит интерфейс СКЗИ в Microsoft Excel. Вместо шаблона Normal.dot для хранения макросов используется xls-файл, копируемый на этапе инсталляции СКЗИ в каталог библиотек Microsoft Office (подкаталог Library каталога установки Microsoft Office).

Для Microsoft Outlook была выбрана событийная схема активизации, поскольку активизацию СКЗИ для защиты почтовых сообщений логично привязать к моменту наступления одного из двух событий, которые предусмотрены в реализации VBA в Microsoft Outlook:

- Отправление сообщения электронной почты.
- Получение нового сообщения электронной почты.

При отправлении нового сообщения производятся следующие действия (см. рис. 3):

- Выделяется текстовая часть сообщения, вычисляется ее ЭЦП и производится зашифрование.
- Если сообщение содержит прикрепленные файлы, для каждого из них производится вычисление ЭЦП, файл зашифровывается и удаляется из сообщения.
- Вся зашифрованная информация собирается в один файл, который прикрепляется к сообщению.
- Текстовая часть сообщения заменяется на идентификатор зашифрованного сообщения.

При получении новых сообщений для каждого непрочитанного сообщения, содержащего идентификатор зашифрованного сообщения, выполняется обратное преобразование.

Процедуры обработки событий на этапе инсталляции встраиваются в макросы Application_ItemSend и Application_NewMail стандартного модуля Microsoft Outlook ThisOutlookSession, загружающегося автоматически при запуске Microsoft Outlook.

Стоит сказать и о том, что разработка инсталлятора СКЗИ сама по себе является достаточно трудоемкой задачей. Инсталлятор должен выполнить следующие действия:

1. Скопировать на диск компьютера файлы программных модулей СКЗИ (включая программный шифратор, если не используется аппаратный).
2. Скопировать на диск компьютера тестовые криптографические ключи (можно давать в дистрибутиве СКЗИ и "боевые" ключи, если существует процедура генерации уникальных ключей при создании дистрибутивов СКЗИ и если фирма-производитель предоставляет надежные гарантии неиспользования и нераспространения ключей).
3. Записать все необходимые настройки в системный реестр Windows.
4. Инсталлировать VBA-модули СКЗИ.

Первые три из перечисленных действий являются тривиальными, чего нельзя сказать об инсталляции VBA-модулей. Для инсталляции VBA-модулей в Microsoft Word и Microsoft Excel автором был использован механизм OLE Automation, позволяющий получить доступ к объектам данных программ и выполнить необходимые действия с ними: создать панель инструментов с требуемыми кнопками, скопировать макросы в шаблон, ассоциировать макросы с кнопками. Инсталляция VBA-модуля Microsoft Outlook производится простым копированием модуля вместо стандартного модуля ThisOutlook Session, который после инсталляции Microsoft Office не содержит макросов.

Для примера приведена блок-схема работы инсталлятора части СКЗИ, предназначенной для Microsoft Word (см. рис. 4).

Заключение

Приведенную в данной статье методику встраивания, в принципе, можно распространить на любую функциональность (не только на защиту информации). В качестве примера можно привести автоматическую архивацию ЭД при их сохранении на жесткий диск или автоматическую отправку сохраненных ЭД указанным адресатам по электронной почте. Богатейшие возможности программ пакета Microsoft Office, усиленные поддержкой механизма OLE Automation и встроенным языком программирования VBA, позволяют практически неограниченно наращивать функциональность программ пакета и тонко настраивать их под конкретные выполняемые задачи.

Литература

1. Харт-Девис Г. Word 2000: Руководство разработчика. // Пер. с англ.: Киев: БХВ, 2000 - 944 с.
2. MS Office: новая версия, старые проблемы. // Compute Review. - 2001 - № 11 - с. 19.
3. Гарнаев А., Матросов А., Новиков Ф., Усаров Г., Харитонова И. Microsoft Office 2000: разработка приложений. // Санкт-Петербург: БХВ, 2000 - 656 с.
4. MSDN Library Office 2000 Developer.
5. Microsoft Office 2000 Object Model Guide. - 1999 - 52 с.
6. Леонтьев Б. Хакинг без секретов. // Москва: Познавательная книга плюс, 2000 - 607 с.
7. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. // Москва: ДМК, 2000 - 336 с.
8. Филягин Г. Программы для восстановления паролей к архивам и документам. // Компьютер Пресс. - 2000 - № 7 - с. 87.
9. Приказ ФАПСИ №158. Об утверждении положения о порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. // Российская газета. - 2000 - № 18.
10. Положение ФАПСИ. Система сертификации средств криптографической защиты информации. Октябрь, 1993. // www.ancud.ru.
11. Панасенко С.П., Петренко С.А. Криптографические методы защиты информации для российских корпоративных систем. // Защита информации. Конфидент. - 2001 - № 5.
12. Панасенко С. Защита электронных документов: целостность и конфиденциальность. // Банки и технологии. - 2000 - № 4 - с. 82-87.

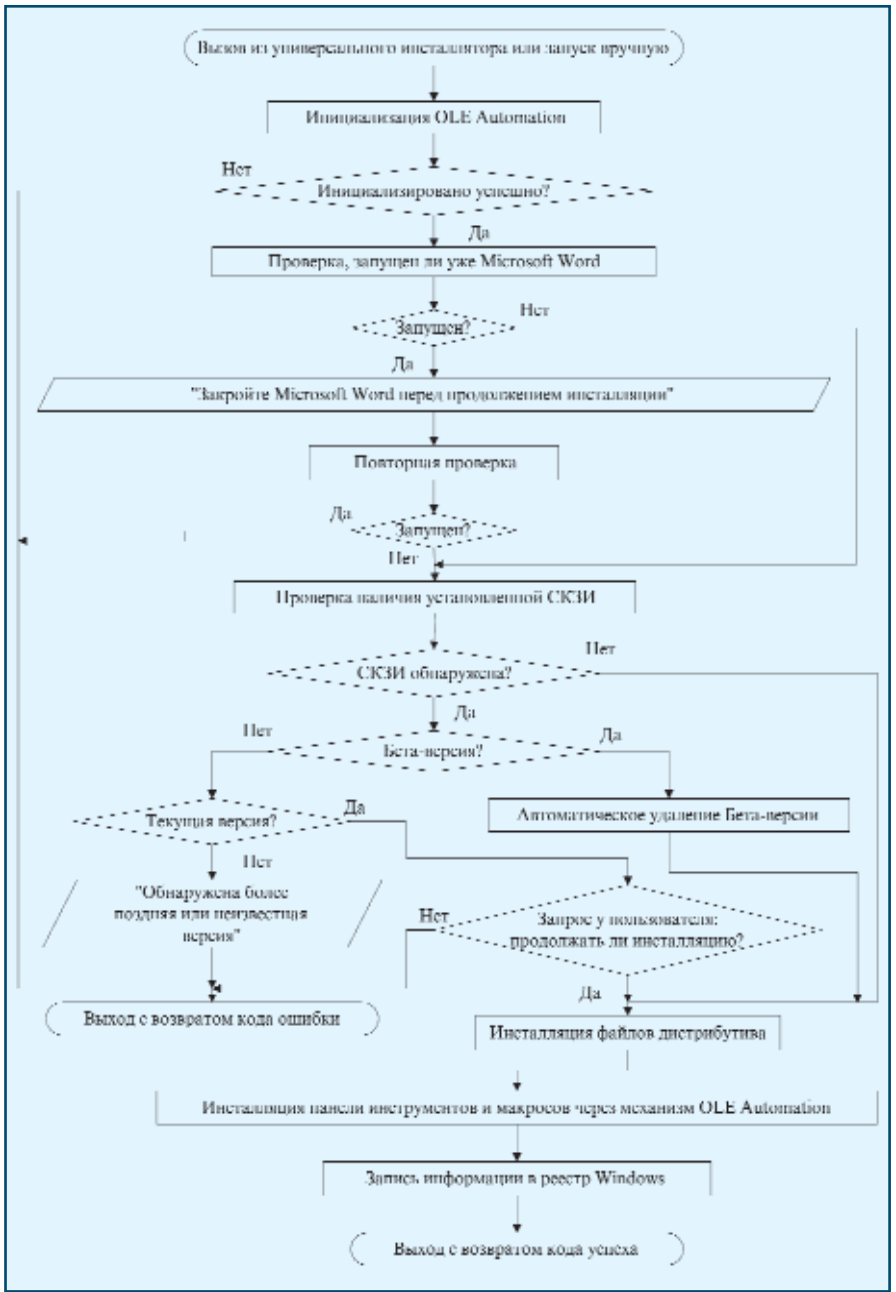

Рис.4. Алгоритм инсталляции части СКЗИ для Microsoft Word