Студенческий Вестник
Электронный научно-технический журнал Октябрь 2005
http://www.bru.mogilev.by

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ШИФРОВАНИЯ ДЛЯ ПЕРЕДАЧИ ДАННЫХ ПРИ НАПОЛНЕНИИ БАЗ ДАННЫХ РЕГИОНАЛЬНЫХ ОРГАНИЗАЦИЙ

Е.С. Козлова, **В.М. Прудников**

Автоматизированная система шифрования для передачи данных при наполнении баз данных региональных организаций выполнена с целью реализации защищенного взаимодействия через Интернет между органами государственной власти и региональными организациями Могилевской области в рамках Интернет-портала.

Ключевые слова: шифрование, электронная подпись, защищенный документооборот

1. Введение

Проблема защиты информации в информационных системах в настоящее время особенно актуальна, тем более что существует тенденция перехода с бумажного документооборота на электронный.

Одним из решений данной проблемы может служить использование ассиметричного алгоритма шифрования, электронной подписи и протокола защищенной передачи данных в общей автоматизированной системе для передачи данных.

2. Компоненты системы для передачи данных через Интернет

Для защищенной передачи данных через Интернет предложено использование 3-х компонентов, функционирующих в рамках единой автоматизированной системы. Эти компоненты следующие:

- асимметричный алгоритм шифрования;
- электронно-цифровая подпись (ЭЦП);
- протокол защищенной передачи данных.

2.1 Асимметричный алгоритм шифрования

Алгоритм шифрования используется для непосредственного кодирования передаваемых данных.

Суть ассиметричного алгоритма состоит в том, что каждым адресатом сети генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сообщение возможно только с использованием закрытого ключа, который известен только самому адресату [1, 2]. Такой вид шифрования очень удобен для передачи разных сообщений, поскольку дает возможность распространять открытые ключи «на лету» – прямо перед обменом зашифрованной информацией.

2.2 Электронно-цифровая подпись

ЭЦП используется для установления подлинности и авторства безбумажной документации, а также защищает от следующих нарушений и действий при передаче данных между пользователем А и Б [3, 4]:

- отказ (ренегатство): А заявляет, что он не посылал сообщение Б, хотя на самом деле он все-таки посылал;
- модификация (переделка): Б изменяет сообщение и утверждает, что данное (измененное) сообщение послал ему А;

- подделка: Б формирует сообщение и утверждает, что данное (измененное) сообщение послал ему А;
- активный перехват: Х перехватывает сообщения между А и Б с целью их скрытой модификации;
- маскировка (имитация): Х посылает Б сообщение от имени А;
- повтор: Х повторяет ранее переданное сообщение, которое А посылал ранее Б.

Невозможность подделки ЭЦП опирается на очень большой объем необходимых математических вычислений.

Каждый абонент, обладающий правом подписи, самостоятельно на автономной ПЭВМ формирует два ключа подписи: секретный и открытый. Секретный ключ используется для выработки подписи. Открытый ключ вычисляется как значение некоторой функции от секретного, но знание открытого ключа не дает возможности определить секретный ключ. Понятие ЭЦП тесно связано с понятием дайджеста.

Алгоритмы-дайджесты в некотором роде похожи на алгоритмы шифрования тем, что тоже получают на входе обыкновенное «читаемое» сообщение и на выходе дают некоторый «нечитаемый» набор байтов. Эти дайджесты необратимы, то есть процедуру их дешифрования произвести нельзя.

Для получения цифровой подписи используется следующий механизм:

- получают дайджест исходного сообщения;
- зашифровывают дайджест с помощью секретного ключа отправителя («подписывают дайджест»);
- посылают «подписанный дайджест» (ЭЦП) и исходное сообщение получателю.

Для проверки цифровой подписи необходимо предпринять следующие действия:

- дешифровать «подписанный дайджест» с помощью публичного (открытого) ключа отправителя;
- получить дайджест полученного сообщения;
- сравнить эти два дайджеста.

Совпадение означает, что исходное сообщение не изменено и получено именно от того лица, чей публичный ключ использовался для дешифрования, тем самым подтверждая подлинность отправителя информации.

2.3 Протокол защищенной передачи данных

Протокол SSL (Secure Sockets Layer protocol) спроектирован для обеспечения конфиденциальности обмена между двумя прикладными процессами клиента и сервера. Преимуществом SSL является то, что он независим от прикладного протокола. Протоколы приложения, такие как HTTP, FTP, TELNET и т.д. могут работать поверх протокола SSL совершенно прозрачно. SSL позволяет делать выбор алгоритмов с учетом требуемой надежности, соответствия принятому законодательству и прочих факторов [5].

3. Особенности построения автоматизированной системы

Разработанная автоматизированная система шифрования для передачи данных при наполнении баз данных региональных организаций является частью общей системы наполнения баз данных региональных организаций, алгоритм функционирования которой представлен на *рисунке* 1.

Рассматриваемая подсистема представляет собой альтернативный способ передачи данных. Штрих-код на бумажной копии нужен для обеспечения целостности данных, в то время как рассматриваемая подсистема (блоки 3, 4, 5, 8, 9) обладает механизмами, обеспечивающими не только проверку целостности данных, но и аутентификацию отправителя, а также защиту данных при передаче.

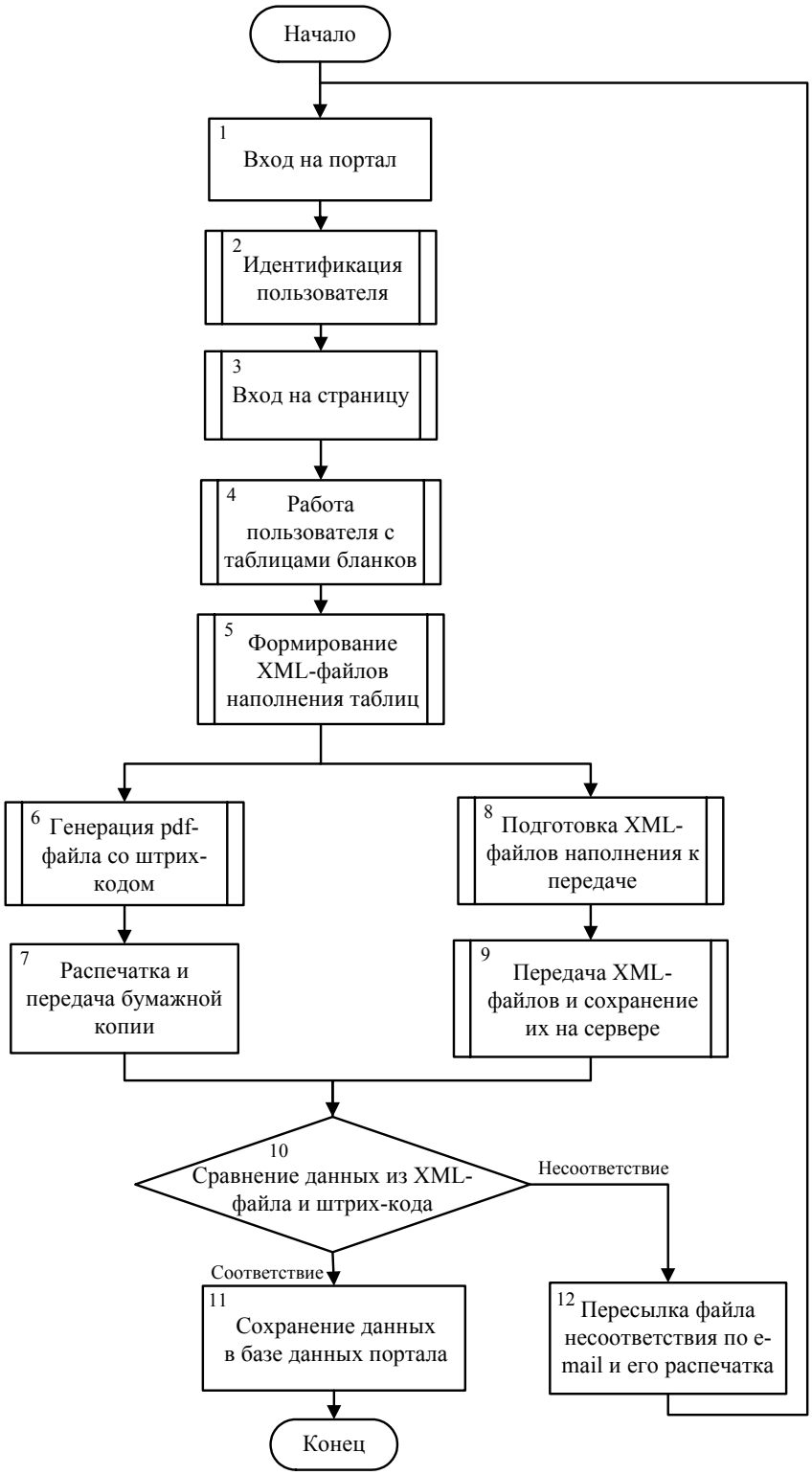

Рис. 1. Общий алгоритм работы системы

Следует также обратить внимание, что пользователь работает не с электронной формой бланка, а с таблицей бланка. Это значит, что таблица имеет те же поля для заполнения, что и бланк, соответствующий государственным стандартам. Такой подход упрощает работу по заполнению бланков отчетности. Наполнение таблицы подставляется в соответствующий бланк при генерации pdf-файла, что показано в блоке 6 рисунка 1.

Когда проверяющая сторона получает данные обоих видов, производится сравнение. Непосредственно перед операцией сравнения штрих-код сканируется, данные из XML-файла извлекаются. Сравнение производится, чтобы определить были ли утеряны данные.

Сохранение бумажной копии в организации необходимо, т.к. не все государственные учреждения используют электронный документооборот, и для отчетности перед ними нужна именно бумажная копия.

В автоматизированной системе передаваемые данные представляются в виде шаблона для заполнения и непосредственно самих вносимых данных, то есть это электронная форма бланка и его наполнение соответственно. Для обеспечения гибкости представления данных и уменьшения их объема, предназначенного для передачи, передаются лишь полезные данные, т.е. наполнение бланков.

Этот механизм реализован средствами языка XML.

С помощью XML описывается структурированный текст любого вида, в том числе другие языки разметки. Существует свыше десятка языков разметки, основанных на XML. С их помощью описывается все – от графики до математических уравнений. В отличие от HTML, имена тегов XML могут быть почти произвольными. Эта особенность и использована для представления XML-документа в требуемой форме.

Для построения автоматизированной системы был использован пакет OpenSSL 0.9.7f. На данный момент он является единственной свободной некоммерческой реализацией средств протокола SSL, предназначенной для построения систем шифрования и электронно-цифровой подписи.

При разработке системы также были использованы два языка программирования: JavaScript 1.3 – для работы с XML-документами, PHP 5.0.2 – для работы с OpenSSL.

4. Заключение

В результате проведенного исследования разработан программный комплекс, обеспечивающий надежную и эффективную защиту при передаче данных через Интернет. Программный комплекс представляет собой автоматизированную систему, написанную на языках HTML, XML, JavaScript и PHP. Система может быть реализована на операционных системах Windows98/Me/2000/NT/XP при условии наличия браузера Internet Explorer 6.0.

Представленные возможности автоматизированной системы шифрования для передачи данных при наполнении баз данных региональных организаций использованы для реализации защищенного взаимодействия через Интернет между органами государственной власти и региональными организациями Могилевской области в рамках разрабатываемого Интернет-портала.

Литература

1. *Наумов А.* Новости законодательства: ЭЦП в действии // Сети [Электрон. ресурс]. – 29 января 2002. — Режим доступа: http://www.osp.ru/nets/2002/01-02/014.
2. *Саломаа А*. Криптография с открытым ключом. – М.: Мир, 1995. – 318 с.: ил.
3. *Баричев С.* Современные криптографические методы защиты информации. – М.: Олма-Пресс, 2002. – 125 с.
4. *Бречко Р.* Цифровая подпись // Internet Zone [Электрон. ресурс]. – Режим доступа: http://www.zeiss.net.ru/docs/izone/izone343/pub/izone13.htm.
5. *Семенов Ю. А.* Протокол SSL. Безопасный уровень соединителей // Телекоммуникационные технологии [Электрон. ресурс]. – 12 января 2004. – Режим доступа: http://book.itep.ru/6/ssl_65.htm.

Козлова Екатерина Святославовна
Студентка электротехнического факультета
Белорусско-Российский университет, г. Могилев
Тел.: +375(222) 47-32-59
Прудников Василий Михайлович
Старший преподаватель кафедры АСУ
Белорусско-Российский университет, г. Могилев
Тел.: +375(222) 22-24-47