

ПРОБЛЕМЫ ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ ПОДПИСИ НА ПРЕДПРИЯТИЯХ МАЛОГО БИЗНЕСА

Л.В. Астахова, В.С. Лужнов

Обоснован комплекс типовых программных решений для предприятий малого бизнеса, которые позволили бы им самостоятельно организовать защищенный электронный документооборот с минимальными экономическими затратами, адекватной сложностью разработки и сопровождения. С учетом нынешнего уровня развития информационных технологий, появления новых механизмов глобального взаимодействия большого числа разработчиков и ориентированности на минимизацию затрат в качестве основы для формирования набора решений было выбрано программное обеспечение с открытым исходным кодом.

Ключевые слова: электронный документооборот, защита информации, открытое программное обеспечение, электронная подпись, облачные технологии, малый бизнес.

Введение

Основой для ведения деятельности любой коммерческой организации является качественно организованный процесс движения документов между ее структурными подразделениями. По мере своего развития организация усложняет существующие и вводит новые бизнес-процессы, что неминуемо ведет к росту объемов ее документооборота.

С развитием информационных технологий проблема роста объемов бумажной документации получила решение в виде перехода к системам электронного документооборота (СЭД). Специфика такого перехода за последние 15 лет связана с тем, что до середины 2000-х годов на рынке информационных продуктов были представлены СЭД, ориентированные на предприятия крупного бизнеса. Это объясняется, в первую очередь, высокой стоимостью разработки систем, а, следовательно, нерентабельностью их для среднего и малого бизнеса; повышенной сложностью СЭД; отсутствием возможности создания универсальных решений, способных удовлетворить потребности широкого круга организаций.

На сегодняшний день рынок СЭД претерпел некоторые изменения[9]: значительно увеличилось количество доступных решений; у организаций сформировалось четкое понимание положительных и отрицательных эффектов от внедрения СЭД; разработчики, используя усовершенствованные технологии, смогли повысить степень универсальности своих продуктов и их доступности широкому кругу потребителей.

Тем не менее, многие из проблем продолжают оставаться актуальными, в особенности для предприятий малого бизнеса. В первую очередь, это рентабельность внедрения СЭД. Несмотря на широкий выбор продуктов, организация часто отказывается от их приобретения в силу высокой стоимости. Кроме того, сам процесс внедрения защищенной СЭД требует привлечения не просто квалифицированных специалистов по защите информации, а специалистов широкого профиля, что зачастую оказывается весьма сложной, а порой и невозможной задачей. Дело в том, что увеличение количества малых и средних инновационных компаний в современной высокотехнологичной российской экономике резко повысило требования к системной целостности, универсальности и широте подготовки специалиста по защите информации, который, как инженер в начале прошлого века, оказывается одновременно в роли ученого, технического эксперта и руководителя подразделения по защите информации [4]. Кроме того, в отличие, например, от специалиста по защите информации в банковской сфере [5], на малом предприятии такой специалист выполняет комплекс целей, связанных с пожарной, экономической, информационной, кадровой (информационно-психологической, социальной) безопасностью, что расширяет зону

его ответственности и требует от него не только системного видения защищаемых объектов [2, 3, 4], но и построения и эксплуатации самих этих объектов, к которым относятся СЭД.

И все же главная функция такого специалиста – это обеспечение безопасности документооборота. В частности, речь идет о защищенном канале передачи документов, а также о необходимости гарантированно подтверждать авторство и целостность электронной документации. Удовлетворение этих потребностей также ведет к усложнению СЭД, и, как следствие, к сужению круга продуктов, доступных для выбора, и их общему удорожанию.

Таким образом, можно утверждать о существовании противоречия: с одной стороны, малый бизнес в своем развитии пришел к необходимости организации качественного и защищенного документооборота; с другой стороны, рынок не готов удовлетворить потребности таких организаций – решения либо слишком упрощенные, либо их разработка не соответствует финансовым возможностям компаний.

Целью данной работы является формирование комплекса типовых решений для предприятий малого бизнеса, которые позволили бы им самостоятельно организовать защищенный электронный документооборот с минимальными экономическими затратами, адекватной сложностью разработки и сопровождения.

Пути решения проблемы

Анализ публикаций о СЭД [12], о критериях выбора оптимальной СЭД в соответствии с требованиями заказчика и алгоритмах выбора [13] привел нас к выводу о том, что при подборе решений для организации СЭД на малом предприятии необходимо руководствоваться потребностями бизнеса. В общем виде это: минимальная стоимость; простота разработки, внедрения и сопровождения; безопасность; гибкость; прозрачность и контролируемость документооборота; упрощение управленческих процессов.

При этом важно понимать, что специфичным для малого бизнеса является ориентированность на простоту применяемых решений. В частности, это значит, что бизнес готов отказаться от многих функций, предусмотренных в существующих СЭД, в силу отсутствия необходимости в них. Поэтому подход, применяемый в данной работе, базируется на следующих основных положениях:

- для обеспечения гибкости и удовлетворения максимально широкого круга потребностей итоговый набор решений должен обладать модульностью, т. е. независимостью каждого компонента набора и возможностью комбинировать компоненты в любых вариациях;
- минимальные затраты являются главным критерием формирования набора решений;
- безопасность и защищенность всех процессов является обязательным условием;
- степень сложности решений должна быть такой, чтобы с сопровождением системы мог справиться специалист средней квалификации, не обладающий специальными навыками.

С учетом нынешнего уровня развития информационных технологий, появления новых механизмов глобального взаимодействия большого числа разработчиков и ориентированности на минимизацию затрат в качестве основы для формирования набора решений было выбрано программное обеспечение с открытым исходным кодом.

Положительные стороны такого подхода выражаются в следующем:

- бесплатность программного обеспечения;
- открытый исходный код, исключающий недеklarированные возможности;
- неограниченные возможности по расширению функционала собственными силами;
- регулярная поддержка и обновление;
- подробная, регулярно обновляемая документация.

Необходимо также отметить мнение экспертов в области информационной безопасности по данному вопросу, поскольку существует стереотип об уязвимости указанного программного обеспечения именно из-за его открытости. Консультант по безопасности компании Cisco, авторитетный эксперт по вопросам информационной безопасности А.В. Лукацкий в своем личном блоге неоднократно [7, 8] обозначал свою позицию по вопросу безопасности ПО с открытым исходным кодом: не существует сколь бы то ни было весомой корреляции между безопасностью программы и степенью открытости ее исходного кода, с учетом чего нет никаких ограничений по использованию таких программ. Крупнейшая корпорация в мире по разработке программного обеспе-

чения, Microsoft, открыто заявила [5], что пересмотрит свою политику в сторону интеграции программ с открытым исходным кодом в свои продукты.

Можно добавить кроме этого, что Правительство РФ своим Распоряжением от 17 декабря 2010 г. №2299-р «О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения (2011–2015 годы)» [10] законодательно одобрило использование подобных программ на всех уровнях государственного управления.

Документооборот. Для организации движения документов внутри организации предлагается использовать:

- Системы управления версиями (VCS, Version Control System);
- Системы управления заданиями (TMS, Task Management System).

Рассмотрим каждый вариант в отдельности.

Системы управления версиями представляют собой программное обеспечение, позволяющее осуществить полный контроль над всеми версиями документа в системе (включая обеспечение доступа к каждой из версий после любых изменений), дистанционный обмен документами между пользователями внутри локальной сети, учет вносимых изменений, подсистему разграничения прав доступа отдельных пользователей.

Различают два вида реализации таких систем: клиент-серверные (требующие существования в локальной сети центрального сервера-хранилища, через который происходит обмен данными между всеми пользователями) и распределенные (на каждом рабочем месте хранится история обо всех изменениях документов другими пользователями, история синхронизируется по локальной сети между каждым клиентом, не требуя наличия сервера).

При этом положительными сторонами использования такого ПО являются:

- Простота установки и использования;
- В качестве сервера может выступать любой персональный компьютер в локальной сети;
- При использовании распределенной версии системы сервер как таковой в принципе не требуется – система будет активна до тех пор, пока в ней функционирует хотя бы одна рабочая станция;
- Выход из строя оборудования любого участника обмена (будь то клиент или сервер) никак не влияет на целостность документов;
- Осуществляется полный учет изменений документа с возможностью вернуться к любой предыдущей его версии;
- Система разграничения прав позволяет организовывать маршруты обмена любой сложности, включая обмен конфиденциальной информацией только между заинтересованными лицами.

На сегодняшний день существует множество бесплатных систем управления версиями с открытым исходным кодом, крупнейшими из которых являются системы SubVersion (SVN) и Git. Установка этих систем не требует от администратора каких-либо специальных навыков и полностью сопровождается подробной документацией.

Традиционно системы управления версиями применяются разработчиками программного обеспечения для контроля за ходом процесса разработки; системы дают возможность привлекать к одному проекту нескольких программистов и обеспечивают качественный менеджмент программного кода. Использование VCS в качестве систем документооборота – пока что довольно редкое явление в практике, однако положительные стороны такого подхода и рост популярности открытого ПО постепенно формируют представление, как можно организовать управление потоком документации на основе контроля версий.

На сегодняшний день вопросами практического использования VCS в контексте документооборота занимается Региональный Финансово-Экономический Институт [11]. В существующей при институте школе бизнес-информатики читается курс «Контроль версий с использованием Git» [6], который, помимо прочего, оговаривает аспекты внедрения VCS как системы управления документацией.

Системы управления заданиями представляют собой программное обеспечение для распределения задач между пользователями, контроля над их исполнением и отчетности по результатам.

Применимость таких систем в контексте организации документооборота выражается в возможности сопровождать каждую задачу документацией различного рода, что обеспечивает дви-

жение документов между структурными подразделениями и отдельными сотрудниками организации.

Данные системы существуют в виде специализированного программного обеспечения либо в виде веб-приложения, устанавливаемого на локальный сервер. Независимо от типа исполнения ПО предусматривает контроль за движением документации, учет вносимых изменений и отчетность по каждому сотруднику, вовлеченному в документооборот.

С технической точки зрения данные системы могут устанавливаться как отдельная программа на каждое рабочее место (децентрализованный вариант коммуникации «клиент – клиент») либо как приложение на сервер с возможностью подключения через веб-интерфейс. Последний вариант требует наличия в локальной сети организации сервера с дополнительной установкой программных модулей, обеспечивающих работу веб-приложения (веб-сервер (Apache, Nginx) и интерпретатор языка программирования, на котором написано приложение (PHP, Ruby, Perl)). Самыми известными на сегодняшний день системами управления заданиями являются системы Redmine, JIRA, TeamLab, Google Calendar.

Электронная подпись и шифрование. Центральным элементом электронного документооборота является обеспечение гарантии авторства документа и его целостности при передаче внутри сети, а также исключение несанкционированного доступа. Первая задача решается путем использования электронной подписи, вторая – путем применения криптографических методов защиты.

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» [14] допускает применение внутри корпоративной локальной сети электронной подписи, реализованной на базе любого криптографического алгоритма, гарантированно обеспечивающего подтверждение авторства и целостности документа. При этом, несмотря на расхожее заблуждение, не требуется прибегать к услугам лицензированных удостоверяющих центров или получать какие-либо разрешающие документы.

Основопологающим требованием для организации обмена документами, подписанными электронной подписью, является наличие единого «удостоверяющего центра» – т. е., в контексте данной работы все подписи, выдаваемые сотрудникам организации, должны быть выданы одним и тем же центром (например, ПО, установленным на рабочем месте руководителя).

Самым известным на сегодняшний день открытым программным обеспечением, реализующим, помимо прочего, механизм работы с электронными подписями, является программа GnuPG. Основными преимуществами ее использования являются:

- Наличие понятного графического интерфейса, позволяющего быстро подписать документ;
- Реализация функций выдачи, проверки и отзыва электронных подписей (при наличии рабочего места, выступающего «центром»);
- Реализация большого набора алгоритмов шифрования документов, позволяющих обеспечить конфиденциальность передаваемой информации (поддержка симметричных и асимметричных шифров по стандартам IEEE P1363, ГОСТ Р 34.10-2012, Kerberos и другим).

При использовании систем управления заданиями в виде веб-приложений для обеспечения защищенного обмена может применяться протокол SSL. Протокол использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности и коды аутентификации сообщений для целостности сообщений. Данный протокол поддерживается всеми современными веб-обозревателями. Для его реализации необходимо осуществить выпуск SSL-сертификата и его установку на сервер, который обеспечивает работу веб-приложения. Выпуск сертификата обеспечивается функциями большинства современных операционных систем (Microsoft Windows, UNIX-based системы).

Облачные решения. Кроме оговоренных решений для организации документооборота в локальной сети предприятия, необходимо отдельно отметить возможность использования очень популярных сегодня технологий облачного хранения данных (облачных вычислений).

Кроме исполнения в виде «частного облака» (на ресурсах организации) существует огромное количество предложений от различных провайдеров по предоставлению доступа к облачной инфраструктуре посредством сети Интернет.

В контексте организации документооборота существует несколько крупных облачных решений. Положительными сторонами их использования является низкая стоимость, отсутствие необ-

ходимости в каком-либо стороннем программном обеспечении, высокая степень дружелюбности к пользователям с любым уровнем квалификации.

Корпорации Google и Microsoft предлагают собственные системы по контролю за оборотом и хранением документов – Google Drive (в прошлом – Google Docs) и Microsoft SkyDrive (с дополнительным инструментарием WebOffice).

Оба указанных решения обеспечивают хранение любых объемов документации, гибкое управление политикой доступа пользователей к ресурсам, оперативную маршрутизацию документационных потоков. Кроме этого, для непосредственной работы с документами нет необходимости устанавливать какое-либо ПО, кроме веб-обозревателя – весь стандартный инструментарий так называемых «офисных пакетов» доступен конечному пользователю.

Нельзя не сказать о недостатках облачных решений. Самый главный из них – особенно в контексте информационной безопасности – это тот факт, что вся документация организации находится под контролем сторонней компании. Использование облачных решений для работы с конфиденциальными сведениями, несмотря на гарантии об обеспечении безопасности данных от разработчиков систем, является очень рискованным, так как создает предпосылки для утечки и несанкционированного доступа информации.

Кроме вопросов безопасности существует «проблема регулярной связи»: так как доступ к «облаку» осуществляется посредством сети Интернет, любой выход из строя коммутационного оборудования или неполадки в линии связи могут привести к полной остановке документооборота в компании. Да и обучение пользователей в виртуальных образовательных средах представляет собой непростую задачу [1]. Обращение к облачным технологиям оправдано, если финансовый эффект от их применения значительно превышает объем рисков от такого применения.

Заключение

Таким образом, обоснованный в статье набор решений позволяет оперативно и с минимальными затратами внедрить в организации систему электронного документооборота, оптимальную как для сопровождения, так и для дальнейшего расширения. Использование программного обеспечения с открытым исходным кодом дает возможность при необходимости адаптировать систему под индивидуальные нужды организации силами штатного разработчика. На сегодняшний день отсутствуют аналоги применения обоснованного в статье набора решений для организации защищенного документооборота, что и обуславливает научную новизну и практическую значимость результатов представленной работы.

Литература

1. Астахова, Л.В. *Виртуальная образовательная среда: сущность понятия* / Л.В. Астахова, Н.С. Запускалова // *Сибирский педагогический журнал*. – 2011. – № 12. – С. 63–68.
2. Астахова, Л.В. *Герменевтический психологический метод исследования в деятельности по обеспечению информационной безопасности: педагогический аспект* / Л.В. Астахова, Т.В. Харлампьева // *Вестник Челяб. гос. пед. ун-та*. – 2010. – № 4. – С. 5–11.
3. Астахова, Л.В. *Информационно-психологическая безопасность в регионе: культурологический аспект* / Л.В. Астахова // *Вестник УрФО. Безопасность в информационной сфере*. – 2011. – № 2. – С. 40–47.
4. Астахова, Л.В. *Развитие управленческой компетенции будущего специалиста по защите информации в вузе* / Л.В. Астахова // *Современные проблемы науки и образования*. – 2012. – № 6. – С. 330.
5. Астахова, Л.В. *Совершенствование подготовки кадров как важнейшее условие предупреждения операционных рисков в банковской деятельности* / Л.В. Астахова // *Финансы и кредит*. – 2009. – № 45. – С. 34–36.
6. *Контроль версий с использованием Git*. – М.: Региональный Финансово-Экономический Институт: Бизнес-Школа информационных технологий. – <http://it.rfei.ru/~13>
7. Лукацкий, А.В. *Анализ качества кода* / А.В. Лукацкий. – М.: Официальный сайт Лукацкого А.В., 2013. – http://lukatsky.blogspot.ru/2013/03/blog-post_5.html
8. Лукацкий, А.В. *Открытый исходный код* / А.В. Лукацкий. – М.: Официальный сайт Лукацкого А.В., 2012. – http://lukatsky.blogspot.ru/2010/12/blog-post_13.html

9. *Позиция Microsoft в отношении Open Source.* – М.: Портал свободного программного обеспечения OpenNet, 2008. – <http://www.opennet.ru/opennews/art.shtml?num=17672>

10. *Правительство РФ. Распоряжение от 17 декабря 2010 г. №2299-р «О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения (2011–2015 годы)» // Собрание законодательства Российской Федерации от 27 декабря 2010 г. N 52 (часть I), ст. 7181.*

11. *Региональный Финансово-Экономический Институт.* – М.: Официальный сайт. – <http://rfei.ru/>

12. *Сабаева, А.А. Алгоритм и модель выбора системы электронного документооборота для коммерческой компании / А.А. Сабаева, М.А. Семенов, В.В. Скоморохов // Вестник Иркут_ гос_ техн_ ун_та.* – 2012. – № 11. – С. 263–270.

13. *СЭД (Рынок России).* – М.: Аналитическое агентство TAdviser, 2012. – <http://www.tadviser.ru/index.php>

14. *Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи».* – <http://base.garant.ru/12184522>

Астахова Людмила Викторовна, д-р пед. наук, профессор, профессор кафедры безопасности информационных систем, Южно-Уральский государственный университет (г. Челябинск); lvastachova@mail.ru.

Лужнов Василий Сергеевич, студент кафедры безопасности информационных систем, Южно-Уральский государственный университет (г. Челябинск); ua9stz@gmail.com.

Bulletin of the South Ural State University
Series “Computer Technologies, Automatic Control, Radio Electronics”
2013, vol. 13, no. 3, pp. 54–60

PROBLEMS OF ORGANIZATION OF PROTECTED ELECTRONIC DOCUMENT CIRCULATION USING ELECTRONIC DIGITAL SIGNATURE AT THE SMALL BUSINESS ENTERPRISES

L.V. Astakhova, South Ural State University, Chelyabinsk, Russian Federation,
lvastachova@mail.ru,

V.S. Luzhnov, South Ural State University, Chelyabinsk, Russian Federation,
ua9stz@gmail.com

The article grounds of the complex model of software solutions for small business enterprises, which would enable them to independently organize protected electronic document circulation with minimum economic cost and with adequate complexity of software development and support. Taking into account the current level of development of information technologies, the emergence of new mechanisms of global interactions of a large number of developers and the orientation on the minimization cost, software with open source code was selected as the basis for creating a set of decisions.

Keywords: electronic document management, information security, open source software, electronic signature, cloud-based technology, small business.

References

1. Astakhova L.V., Zapuskalova N.S. Virtual educational environment: the essence of the concept [Virtual'naja obrazovatel'naja sreda: sushhnost' ponjatija]. *Sibirskij pedagogicheskij zhurnal [Siberian pedagogical magazine]*, 2011, no. 12, pp. 63–68.

2. Astakhova L.V., Harlamp'eva T.V. Hermeneutic psychological method of research in information security activities: pedagogical aspect [Germenevticheskij psihologicheskij metod issledovaniya v dejatel'nosti po obespecheniju informacionnoj bezopasnosti: pedagogicheskij aspect]. *Vestnik Cheljabinskogo*

go gosudarstvennogo pedagogicheskogo universiteta [*Bulletin of the Chelyabinsk state pedagogical University*], 2010, no. 4, pp. 5–11.

3. Astakhova L.V. Information-psychological security in the region: the culturological aspect [Informacionno-psihologicheskaja bezopasnost' v regione: kul'turologicheskij aspekt] *Vestnik The Ural Federal district. Security in the information sphere* [*Vestnik UrFO. Bezopasnost' v informacionnoj sfere*], 2011, no. 2, pp. 40–47.

4. Astakhova, L.V. The Development of Managerial Competence of Future Specialist for the Protection of the Information in the University [Razvitie upravlencheskoj kompetencii budushhego specialista po zashhite informacii v vuze]. *Sovremennye problemy nauki i obrazovanija* [*Modern Problems of Science and Education*], 2012, no. 6, p. 330.

5. Astakhova L.V. Improving the training as an important condition for prevention of operational risks in the banking [Sovershenstvovanie podgotovki kadrov kak vazhnejshee uslovie preduprezhdenija operacionnyh riskov v bankovskoj dejatel'nosti]. *Finance and credit* [*Finansy i kredit*], 2009, no. 45, pp. 34–36.

6. *Kontrol' Versij s Ispol'zovaniem Git* [Version Control Using Git]. Available at: <http://it.rfei.ru/~13> (accessed 11 May 2013).

7. Lukatsky, A.V. *Analiz Kachestva Koda* [The Analysis of the Quality of the Code]. Available at: http://lukatsky.blogspot.ru/2013/03/blog-post_5.html (accessed 11 May 2013).

8. Lukatsky, A.V. *Otkrytyj Ishodnyj Kod* [An Open Source Code]. Available at: http://lukatsky.blogspot.ru/2010/12/blog-post_13.html (accessed 11 May 2013).

9. *Pozicija Microsoft v Otnoshenii Open Source* [The Position of Microsoft in Respect of Open Source]. Available at: <http://www.opennet.ru/opennews/art.shtml?num=17672> (accessed 11 May 2013).

10. *The Government of the Russian Federation. The Ordinance of 17 December 2010. №2299-R "On the Transfer of Federal Bodies of Executive Authority and the Federal Budgetary Institutions on the Use of Free Software (2011–2015)"* [Pravitel'stvo RF. Rasporjazhenie ot 17 dekabrja 2010 g. №2299-r "O plane perehoda federal'nyh organov ispolnitel'noj vlasti i federal'nyh bjudzhetnyh uchrezhdenij na ispol'zovanie svobodnogo programmnoho obespechenija (2011–2015 gody)"]. Collected legislation of the Russian Federation [Sobranie zakonodatel'stva Rossijskoj Federacii], 2010, December 27, no. 52 (part I), art. 7181.

11. *Regional'nyj Finansovo-Jekonomicheskij Institut* [Regional Financial And Economic Institute]. Available at: <http://rfei.ru> (accessed 11 May 2013).

12. Sabaeva A.A., Semenov M.A., Skomorokhov V.V. The Algorithm and the Model of Choice of the System of Electronic Document Circulation for a Commercial Company [Algoritm i model' vybora sistemy jelektronnogo dokumentooborota dlja kommercheskoj kompanii]. *Vestnik Irkutskogo gosudarstvennogo tehničeskogo universiteta* [*Vestnik of the Irkutsk State Technical University*], 2012, no.11, pp. 263–270.

13. *SJeD (Rynok Rossii)* [The ERMS (Russian Market)]. Available at: <http://www.tadviser.ru/index.php> (accessed 11 May 2013).

14. *Federal'nyj zakon Rossijskoj Federacii ot 6 aprelja 2011 g. N 63-FZ "Ob Jelektronnoj Podpisi"* [Federal law of of the Russian Federation 6 April 2011. N 63-FZ "On electronic signature"]. Available at: <http://base.garant.ru/12184522> (accessed 11 May 2013).

Поступила в редакцию 29 мая 2013 г.