УДК 621.396

НЕКОТОРЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ДОСТОВЕРНОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Юрий Гусаров
ЗАО «ОКБ САПР»

Аннотация: **Рассмотрены возможные подходы к созданию технологий и систем, отвечающих сегодняшним требованиям документационного обеспечения управления, комплекса нормативного и научно-методического обеспечения организации работы с документированной информацией на различных уровнях государственного, общественного и экономического управления.**
Summary: **Possible approaches to creation of technologies and the systems adequate{answering} to today's requirements of documentary maintenance of management, a complex of normative and scientific - methodical maintenance of the organization of work with the documentary information at various levels of the state, public and economic management are considered.**
Ключевые слова: **Информация, информационная система управления, сообщения, электронный документ, документооборот.**

Развитие электронного документооборота в стране тесно связано с такими приоритетами в деятельности правительства любого государства, как административная реформа, реформа государственной службы, бюджетная реформа и реформа образования. Именно системы электронного документооборота должны обеспечить техническую и информационную поддержку этих реформ, востребованность открытых государственных информационных ресурсов, создать основу технологий электронного правительства, обеспечить исполнение электронных административных регламентов. Уже сегодня мы можем видеть, что информационные системы управления деятельностью имеются во многих организациях, однако эти системы носят изолированный и фрагментарный характер. В части документооборота положение является наиболее тревожным – ибо отсутствуют технологии и системы, отвечающие сегодняшним требованиям документационного обеспечения управления. Фактически отсутствует комплекс нормативного и научно-методического обеспечения организации работы с документированной информацией на различных уровнях государственного, общественного и экономического управления. Кроме того, разрозненность усилий приводит к неоправданному дублированию работ и отсутствию решений, которые могли бы стать общеупотребительными.

Источник неудач таится не в отсутствии координации, а носит системный характер.

Рассмотрим возможные подходы к решению проблем.

Информация представляет собой результат отражения движения объектов материального мира в системах живой природы.

При этом **информация** обращается в коллективе однотипных организмов в **форме сведений** и **сообщений**. **Сведения** образуются в результате отражения организмами объектов материального мира, в том числе сообщений. **Сообщения** образуются организмами для передачи сведений другим организмам, содержат совокупность передаваемых сведений и представляют собой набор знаков, с помощью которого сведения могут быть переданы другому организму и восприняты им.

Преобразование сведений в сообщения и сообщений в сведения осуществляется **человеком** с использованием алгоритмов кодирования и декодирования поступившего набора знаков в элементы его «информационной» модели мира.

Таким образом, информация в форме сведений порождается в голове человека (и только там) и защите техническими методами не подлежит. Защите подлежат сообщения в процессе коммуникаций.

До последнего времени проблематика технической защиты исчерпывалась защитой компьютеров от НСД, разграничением доступа к данным, сетевой защитой – и все. Ни на одном из этих этапов не рассматривался вопрос о том, что именно мы защищаем. Очевидно, что если завод производит чайники, а фабрика – ботинки, то возможным объектом преступных посягательств они и будут. Компьютерные системы не производят информацию. Они обрабатывают одни сообщения и вырабатывают другие.

Подчеркнем – в информационных системах производятся электронные документы (ЭлД). В процессе изготовления ЭлД участвуют такие объекты, как:

- компьютеры;
- данные (другие ЭлД);
- сетевые (телекоммуникационные) средства;
- **информационные технологии**.

В процессе информационного взаимодействия на разных его этапах заняты люди (**операторы, пользователи**) и используются средства информатизации – технические (**ПЭВМ, ЛВС**) и программные (**ОС, ППО**). Сведения порождаются людьми, затем преобразовываются в **данные** и представляются в автоматизованных системах (АС) в виде **электронных документов**, объединенных в **информационные ресурсы**. Данные между компьютерами передаются по **каналам** связи. В процессе работы АС ЭлД преобразовываются в соответствии с реализуемой **информационной технологией**. В соответствии с этим, в мероприятиях по технической защите можно выделить:

1) аутентификацию участников информационного взаимодействия;
2) защиту технических средств от НСД;
3) разграничение доступа к документам, ресурсам ПЭВМ и сети;
4) защиту электронных документов;
5) защиту данных в каналах связи;
6) защиту информационных технологий;
7) разграничение доступа к потокам данных.

Заметим, что пункты 1, 2, 3, 5 и отчасти 7 в совокупности и составляют предмет традиционно понимаемой «защиты информации». Очевидно, что реально предмет гораздо шире, ибо есть еще по крайней мере пункты 4 и 6. Этим вполне можно объяснить отсутствие значимых успехов в традиционных подходах к решению практических задач.

Жизненный цикл электронного документа протекает в трех средах существования, вложенных одна в другую: электронная – среда цифровых процессов; аналоговая – среда объектов, предметов; социальная – среда мыслящих субъектов. Внешняя оболочка – подмножество мыслящих субъектов социальной среды, образует *сектор действенности* документа, *диктующий* правила обмена информацией своим членам-субъектам, в том числе, требования к технологии взаимодействия. Если эти правила и требования выполнены, то сообщение признается документом, а содержащаяся в нем информация признается *сектором* как (юридический) *факт* – формальным основанием для возникновения, изменения, прекращения конкретных отношений между субъектами общества.

Для признания сообщения документом необходимо, чтобы параметры технологий, использованных при его формировании, преобразовании, передаче и хранении лежали бы в рамках допустимых отклонений от некоторого *эталона*, *предписываемого сектором* для документального электронного взаимодействия.

Легкость и простота модификации ЭлД заложена самой средой его существования: операции копирования и замены являются фундаментальными в машине Тьюринга. ЭлД многократно преобразуется в течение жизненного цикла. Физическая индикация искажения ЭлД трудна. Здесь требования соответствия применяемых информационных технологий эталонным технологиям крайне значимы. Поэтому защита электронного обмена информацией включает два класса задач:

обеспечение эквивалентности документа в течение его жизненного цикла исходному ЭлД – эталону;

обеспечение эквивалентности примененных электронных технологий эталонным, предписываемым сектором действенности.

Таким образом, статус документа предполагает не только идентичность (соответствие эталону) собственно документа, но и соответствие эталонным требованиям примененных информационных технологий.

Защищенность объекта индицируется сопоставлением эталона (объекта в исходной точке пространства и времени) и результата (объекта в момент наблюдения). В нашем случае в точке наблюдения (получения ЭлД) имеется только весьма ограниченная контекстная информация об эталоне (содержании исходного ЭлД), но зато имеется полная информация о результате (наблюдаемом документе). Это означает, что ЭлД должен включать в свой состав атрибуты, удостоверяющие соблюдение технических и технологических требований, а именно – неизменность сообщения на всех этапах изготовления и транспортировки документа. Одним из вариантов атрибутов могут быть защитные коды аутентификации (ЗКА).

Необходимость защиты информационных технологий была осознана лишь в последнее время. До сих пор в сознании общества электронный документ воспринимается как файл, подписанный ЭЦП. Это неправильно. Вот две иллюстрации – шифрограмма и денежная купюра. И шифрограмма, и купюра не имеют ни подписей, ни печатей – но документами являются. Почему мы воспринимаем их как документы? Лишь потому (и этого достаточно), что **доверяем технологии** их изготовления. Если командир воинской части получает расшифровку приказа своего начальства из рук шифровальщика – он имеет все основания воспринимать полученный текст как документ (приказ). А если тот же текст окажется на рабочем столе неизвестно как – впору проводить служебное расследование. Для этого есть свои методы, мало известные в широких кругах. По-другому дело обстоит с купюрами – редко кто из нас получает их непосредственно из фабрики Госзнака. Чаще пути, которыми купюры попадают к нам, известны не досконально. И поведение наше отличается –

купюры, полученные в отделении Сбербанка мы, как правило, лишь пересчитываем, а вот сдачу из рук рыночного торговца не грех и изучить на предмет подлинности внимательнее.

Технология электронного взаимодействия должна соответствовать сертифицированному эталону, а ее соблюдение должно контролироваться.

При защите *технологии*, в отличие от защиты ЭлД, достоверно известны характеристики требуемой *технологии – эталона*, но имеются ограниченные сведения о выполнении этих требований – о результате. Единственным объектом, который может нести информацию о фактической технологии (как последовательности операций), является собственно ЭлД, а точнее – входящие в него атрибуты. Как и ранее, одним из видов этих атрибутов могут быть ЗКА. Эквивалентность технологий может быть установлена тем точнее, чем большее количество функциональных операций привязывается к сообщению через ЗКА. Механизмы при этом не отличаются от применяемых при защите ЭлД. Более того – можно считать, что наличие конкретного ЗКА характеризует наличие в технологическом процессе соответствующей операции, а значение ЗКА – характеризует целостность сообщения на данном этапе технологического процесса.

Если это так, то соответствует ли этому сегодняшнее состояние нормативной правовой базы?

Достаточно отметить ошибки *федеральных* законов и законопроектов в сфере электронного взаимодействия. Например:

- «Электронная информация есть сведение, факт» – это человеческие понятия, не конструктивные в электронной среде;
- «Электронный документ – *зафиксированная* информация» – фиксация неприемлема для активизированного ЭлД в форме процесса;
- «Все экземпляры ЭлД на машинном носителе являются *оригиналами* и имеют *одинаковую* юридическую силу» – выполнение предписания в случае использования электронных платежных документов парализует финансовую сферу;
- «ЭлД *не может* иметь электронных *копий*» – фактически означает запрет на архивирование электронной информации, так как бессмысленно хранить десятки лет аннулированную цифровую подпись оригинала;
- «ЭлД должен *сохранять формат* в процессе его обработки и передачи» – это требование невозможно осуществить технологически.

Столь ответственные документы дезориентируют пользователей и строить электронный документооборот на подобной основе, по меньшей мере, проблематично.

Принятие в России Федерального закона "Об электронной цифровой подписи" (№ 1 ФЗ от 10. 01. 02 р.) заложило основу правового регулирования электронного документооборота в сферах государственных и гражданских отношений, но, конечно, не решило всех вопросов.

В соответствии со статьей 4 Закона отправитель электронных документов должен иметь доказательства момента подписания для подтверждения действенности сертификата на момент подписания.

Необходимо также иметь доказательства момента времени выставления им требования немедленного приостановления действия сертификата ключа подписи в соответствии со статьей 12 Закона.

В соответствии со статьями 12 и 13 Закона удостоверяющий центр обязан оповестить всех заинтересованных участников электронного документооборота о приостановлении действия или аннулировании сертификата ключа подписи.

Момент времени этого оповещения имеет большое значение при решении споров сторон о действенности сертификата ключа подписи на момент подписания электронного документа.

Более того, часто важнейшее значение имеет собственно время подписания того или иного документа – например, при разборе конфликтов в области авторского права, регистрации товарных знаков, патентов, заключении сделок при электронном ведении бизнеса и т. д.

Очевидно, что для этих целей нельзя использовать отсчеты времени каждого отдельного персонального компьютера. Необходима служба меток единого времени, обеспечивающая адекватность отсчетов времени с приемлемой точностью на территории всей страны. Возникает вопрос – кто это может реализовать на практике?

Принципиальным положением является то, что Минсвязи может без значительных затрат создать службу единого времени на основе и за счет использования ресурсов службы синхронизации.

Выводы

Таким образом, в сфере технического обеспечения электронного документооборота и использования информационного ресурса выделяются три основных аспекта, реализация которых взаимосвязана и взаимообусловлена: теоретический, технологический, юридический.

Теоретический аспект. Теория электронных документов и электронного документооборота находится в самом начале разработки. Нашедшая распространение трактовка электронного документа как некоторого аналога традиционного документа, показала свою ограниченность в правовом поле. На современном этапе внедрения электронного взаимодействия отсутствие тщательно проработанной теоретической базы становится фактором, препятствующим разработке и совершенствованию прикладных технологий. Теоретическая и понятийная база электронного документооборота нуждается в более глубокой проработке. В связи с этим необходимо и далее поддерживать работы по созданию прикладной теории электронного документа.

Технологический аспект. Технически задача формирования, обработки, передачи и хранения электронного сообщения решена. Актуальной остается задача обеспечения унификации технологий защиты электронного документооборота, включая: собственно защиту информации; защиту среды формирования и обработки электронного документа; формирование и сохранение атрибутов электронного документа, подтверждающих его юридическую значимость.

Юридический аспект. Для того чтобы сообщение могло иметь статус электронного *документа*, оно обязательно должно включать в свой состав ряд атрибутов, позволяющих удостоверить соблюдение ряда специальных требований, которые обеспечат признание электронного документа субъектами права как *юридически* полноценного. Выполнение технических и технологических требований изготовления и транспортировки документа должно фиксироваться общепризнанным способом. Технология электронного взаимодействия должна соответствовать сертифицированному эталону, а ее соблюдение должно контролироваться уполномоченными органами. Необходима разработка соответствующей нормативной правовой базы.

Таким образом, **сообщение становится документом при условии доверия к технологии его формирования** и делает его таковым **инфраструктура электронного документооборота**.

Инфраструктура электронного документооборота представляет собой взаимоувязанную совокупность нормативных, законодательных, методических материалов, организационных решений и механизмов, технических, программных и технологических объектов. Эта совокупность должна гарантировать достаточность использованной технологии электронного взаимодействия для признания электронного документа юридически полноценным. Она должна обеспечивать полноту, аутентичность, доступность и актуальность государственного информационного ресурса и их информационную безопасность.

В состав такой инфраструктуры должны включаться следующие подсистемы:

- управляющая;
- нормативная и организационно–методическая;
- исполнительная (удостоверяющие центры, служба меток единого времени, электронный нотариат, обеспечение качества, арбитраж);
- управление рисками (аудит, мониторинг, аттестация, лицензирование, сертификация, надзор, страхование).

Литература: ***1.*** *Стрельцов А. А.. Обеспечение информационной безопасности России. Теоретические и методологические основы. – М.: МЦНМО, 2002. – 296 с.* ***2.*** *Гадасин В. А., Конявский В. А. От документа – к электронному документу. Системные основы. – М.: РФК-Имидж Лаб, 2001. – 192 с.* ***3.*** *Конявский В. А. Управление защитой информации на базе СЗИ НДС Аккорд. – М.: Радио и связь, 1999. – 325 с.*

УДК 681.3

ПЕРСПЕКТИВНЫЙ МЕТОД ЗАЩИТЫ ИФОРМАЦИОННЫХ РЕСУРСОВ КОРПОРАТИВНЫХ СЕТЕЙ ИНТРАНЕТ

Вячеслав Шорошев

НИИ Национальной академии внутренних дел Украины

Аннотация: **В дополнение к традиционным предлагается использовать новый перспективный мониторинго-адаптивный метод защиты путем обнаружения атак НСД, рассматриваемый как основной механизм реализации адаптивной безопасности сети Интранет организации.**

Summary: **In addition to traditional it is offered to use a new perspective monitoring-adaptive method of protection by detection of attacks UAA, considered(examined) as the basic mechanism of realization of adaptive safety of a network Intranet of organization.**