КОРПОРАТИВНЫЙ ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ КАК КОМПОНЕНТ ИНФРАСТРУКТУРЫ ЭЛЕКТРОННОГО ГОСУДАРСТВА

Т.М. Пестунова, С.В. Триерс
Новосибирский государственный университет
экономики и управления – «НИНХ»
E-mail: ptm@nsuem.ru

В работе обобщается опыт авторов, связанный с внедрением элементов электронного документооборота в Новосибирском государственном университете экономики и управления в течение последних нескольких лет. Рассматриваются возможные варианты интеграции корпоративной инфраструктуры открытых ключей (ИОК)[1] в глобальную инфраструктуру, содействующие более полному использованию потенциала электронного документооборота на корпоративном, региональном и общероссийском уровнях.

Ключевые слова: электронный документ[2], электронный документооборот, электронная цифровая подпись[3], инфраструктура открытых ключей.

Особенности электронного документооборота в организациях, являющихся конечными пользователями ИОК

В настоящее время применение технологий *электронного документооборота* (ЭДО) в России непрерывно расширяется. Ускорение этого процесса в последние годы связано с реализацией Концепции создания в России электронного правительства и развитием системы предоставления государственных электронных услуг. Наряду с этим все большим числом руководителей коммерческих и бюджетных организаций осознаются объективные преимущества, которые обеспечивает ЭДО, что приводит к активизации процессов внедрения разного масштаба корпоративных *систем электронного документооборота* (СЭД).

В корпоративном ЭДО выделяются две составляющие, одна из которых замкнута на внутренние бизнес-процессы, а вторая обеспечивает взаимодействие с внешними сторонами. Исходя из этого, рассмотрим характерные свойства корпоративного ЭДО как внутренней информационной системы организации, которая может взаимодействовать с другими СЭД (государственными и корпоративными), поддерживающими юридическую значимость *электронных документов* (ЭД). При анализе конкретного содержательного наполнения СЭД

[1] Инфраструктура открытых ключей (англ. PKI – Public Key Infrastructure) – информационные технологии, которые предназначены для подтверждения авторства и подлинности ЭД на основе алгоритмов электронной подписи. ИОК включает в себя программно-аппаратное обеспечение и поддерживающую его функционирование организационную структуру. Основное назначение ИОК – обеспечение юридической значимости ЭД.

[2] Под электронным документом согласно Закону от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи» понимается документ, в котором информация представлена в электронно-цифровой форме.

[3] Электронная цифровая подпись (электронная подпись) – согласно Закону от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи»: реквизит ЭД, предназначенный для защиты данного ЭД от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в ЭД.

будем опираться на типичные процессы вузовского документооборота, в частности НГУЭУ.

Внутренний документооборот университета определяется формированием и движением электронных документов в рамках интегрированной информационной системы управления вузом. Сюда входят ЭД, формируемые в рамках системы автоматизации кадровой и финансовой деятельности, автоматизированного управления научно-образовательным процессом. Как правило, электронные документы при этом носят вспомогательный характер, юридически значимые оригиналы оформляются на бумажных носителях с традиционными подписями и печатями. Электронный проект документа может формироваться в информационной системе с последующей его распечаткой. Это происходит, например, в процессе формирования и распечатки финансовых документов в системе 1С: Предприятие. Хотя учетные реквизиты такого документа могут быть сформированы автоматически, а после сохранения уполномоченным лицом документ не может быть изменен, для повторного доступа к тексту ЭД может потребоваться повторное его формирование. В других случаях на основе информации, предоставляемой информационной системой, проект документа в нужном формате создается пользователем независимо (например, в текстовом редакторе). В информационной системе может быть предусмотрена лишь отметка о реквизитах бумажного документа, сопоставленного с определенной группой данных в информационной системе, отображаемых в виде электронной формы (например, приказ об утверждении тем дипломных работ студентов). Эта отметка проставляется оператором информационной системы после поступления твердой копии подписанного документа. Вторая составляющая документооборота НГУЭУ – классическая СЭД, которая автоматизирует процессы общего делопроизводства, касающиеся создания, обработки, исполнения и хранения входящих, исходящих, частично организационно-распорядительных и внутренних документов. Часть ЭД в этой системе является электронным аналогом бумажных оригиналов и позволяет повысить эффективность доступа к утвержденным документам, сократить количество циркулирующих бумажных копий. Они представлены либо в отсканированном виде, либо выгружены из описанных выше систем. Кроме того, в этой системе присутствуют ЭД, которые создаются, согласовываются и исполняются в СЭД, в силу чего могут не иметь бумажных оригиналов. В основном это некритичные и не относящиеся к категории документов длительного хранения ЭД, к которым не предъявляется высоких требований по целостности. Они преимущественно направлены на реализацию текущих запросов (например, служебные записки, задания, поручения) и после исполнения более не востребуются. Поэтому для отражения фактов их создания, согласования, утверждения, исполнения используется не *электронная цифровая подпись* (ЭЦП), а проставление признака подписания в сочетании с авторизованным доступом, реализованным в СЭД (в нашем случае – «Company Media»). Вместе с тем возникающее желание распространить преимущества ЭДО и на другие более критичные категории документов приводит к необходимости использования ИОК. Актуальность этой задачи возрастает в связи с требованиями закона о персональных данных, развитием технологий электронного дистанционного обучения и желанием более полного использования преимуществ ЭДО. Рассматривая варианты решения этой задачи, обратимся к имеющемуся опыту участия НГУЭУ в ИОК, создаваемых внешними сторонами.

Юридически значимый ЭДО в настоящее время реализован для организации внешнего информационного обмена с органами управления, ведомственными и финансовыми структурами. Внедрение таких технологий осуществляется либо по линии государственных ведомств, либо по инициативе банковских структур, создающих собственные *удостоверяющие центры* (УЦ)[1]. Университет в этой ситуации играет роль типичной организации – «конечного пользователя».

На сегодня такой электронный обмен данными осуществляется с региональными отделениями пенсионного фонда, налоговой инспекции, федерального казначейства и рядом банковских структур. Внедрение этих технологий позволило, в целом, существенно повысить оперативность взаимодействия, улучшило условия труда сотрудников, сократило затраты времени на подготовку и сдачу отчетности.

Вместе с тем важно обратить внимание и на ряд проблемных аспектов, с которыми приходится сталкиваться. Поскольку ведомственные и банковские структуры осуществляют процессы внедрения по своему усмотрению в условиях отсутствия единых организационно-правовых рекомендаций и технологических стандартов, то у конечного пользователя довольно быстро образуется целый «зоопарк» технологических решений, которые регулируются множеством договоров и соглашений, определяющих не меньшее разнообразие в части организационно-правовых условий. Все это требует дополнительных усилий по отслеживанию соответствующих обязательств, управлению клиентской частью ИОК и поддержке ее безопасности и, соответственно, приводит к снижению потенциально возможного положительного эффекта от внедрения передовых технологий.

На этапе оформления договорных отношений следует иметь в виду, что, как правило, форму соглашения (договора) определяет сторона, предлагающая услуги УЦ. В условиях отсутствия типовых форм таких документов разночтения могут возникать уже на уровне трактовки основных понятий, в том числе понятия электронного документа, а изложенные условия не всегда равновыгодны для обеих сторон. В предлагаемых к подписанию документах не всегда дается описание программно-технической основы ЭЦП, что не способствует поддержанию высокого уровня доверия к электронным документам. Особенно характерно это для банковских структур, которые ссылаются, с одной стороны, на конфиденциальность данной информации, а с другой – на положительную практику работы по данным технологиям при взаимодействии с другими клиентами. Различаются требования и в отношении организационных аспектов информационной безопасности на стороне клиента, а также обязательства поставщика услуг по поддержке пользователей. Выбор у конечного пользователя в такой ситуации, как правило, невелик: либо соглашаться с предложенными условиями, уповая на «имеющуюся положительную практику»; либо углубляться в процесс согласования вызывающих разногласия позиций, успех которого неочевиден; либо отказываться от предложений, оставаясь в «бумажной среде».

На ИТ-уровне причины снижения эффективности ЭДО сходны с типичными причинами неэффективности «лоскутной автоматизации». Отсутствие или

[1] Удостоверяющий центр – центральный компонент ИОК, осуществляющий доверенное управление сертификатами открытых ключей пользователей. Более подробно функции УЦ описаны в ФЗ от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи».

громоздкость механизмов интеграции с действующими в университете информационными системами возрождает необходимость двойного ввода данных. Различия в механизмах генерации, распределения и хранения ключевой информации требуют разных механизмов организации ее защиты. Не всегда обеспечивается и эффективная поддержка пользователей со стороны поставщиков услуг ИОК. Поскольку ссылаются обычно на недостаток кадров в службе поддержки и их высокую загрузку, необходимо уделять больше внимания вопросам планирования процесса внедрения, а также тестированию и отладке внедряемых программно-технических решений.

Имея в виду, что развитие юридически значимого ЭДО – стратегически важная задача, направленная на повышение эффективности всех уровней управления и непосредственно связанная с идеей создания электронного государства, устранение проблемных аспектов помогло бы реализовать потенциал ЭДО и ИОК в полной мере. Актуальной задачей является разработка и реализация нормативно-методической базы, стандартизирующей организационно-правовую и технологическую стороны ЭДО, включая вопросы взаимодействия удостоверяющих центров, поддерживающих ЭДО в государственных, муниципальных и других корпоративных информационных системах, а также в информационных системах общего пользования[1]. Тогда конечный пользователь, в зависимости от особенностей своего ИТ-производства, сможет выбрать наиболее подходящий для него способ реализации своих потребностей в юридически значимом ЭДО: через один из действующих УЦ либо путем разворачивания собственного корпоративного УЦ и включения его в общую сеть УЦ посредством организации взаимодействия по стандартным регламентам с одним или несколькими действующими УЦ общего пользования.

Общая характеристика инфраструктуры открытых ключей в вузе

Исходя из того что основным видом деятельности любого вуза является образовательная деятельность, рассмотрим систему информационного обмена, который может реализовываться вузом в электронном виде. На верхних уровнях детализации он может быть структурирован (рис. 1). При этом в структуре информационного обмена выделяются два вида взаимодействий: предоставление информационных услуг в электронном виде (сотрудникам, студентам и другим заинтересованным субъектам) и реализация собственных потребностей по получению и передаче информации (сдача отчетности в электронном виде, размещение заказов на электронных торговых площадках, взаимодействие с деловыми партнерами и др.).

Рассмотрим электронный информационный обмен более детально с точки зрения отнесения его к категории внутренних либо внешних коммуникаций [1]. Внутренние коммуникации затрагивают взаимодействия внутри организации и осуществляются либо посредством локальной информационно-вычислительной

[1] Понятия государственных и муниципальных систем введены в ФЗ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В ФЗ от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи» информационные системы подразделяются на корпоративные и общего пользования. Особенности этих систем описаны ниже.

Рис. 1. Структура информационного обмена вуза

сети, либо с использованием интернет-соединений для связи с территориально удаленными подразделениями (пользователями).

Внешние коммуникации осуществляются посредством Интернет и могут включать информационный обмен с органами государственной власти, органами местного самоуправления, вышестоящими отраслевыми организациями, другими организациями, а также с физическими лицами.

В перечисленных случаях ИОК позволяет создать единую инфраструктуру безопасности, которая может использоваться для разных приложений корпоративной информационной системы. Рассмотрим варианты организации и использования корпоративной ИОК.

При предоставлении услуг внутренних коммуникаций в университете можно охватить две группы пользователей: сотрудников и студентов.

Сотрудникам можно предоставлять информационные услуги, касающиеся выдачи юридически значимых документов о доходах в электронном виде, заверенных ЭЦП уполномоченных лиц университета, справок о месте работы, о подтверждении трудового стажа и т.п. Кроме того, ИОК дает возможность создания юридически значимых ЭД общего делопроизводства в электронном виде без использования бумажных оригиналов.

Студентам использование ИОК позволит:

- получить доступ к информации об успеваемости, платежах за обучение через Интернет с гарантией достоверности информации на основе электронного запроса, заверенного ЭЦП (при этом вуз имеет уверенность, что указанные данные персональных данных предоставляются именно субъекту этих персональных данных);
- предоставлять заверенные электронной цифровой подписью вуза справки в электронном виде в органы социального обеспечения, пенсионный фонд, налоговые органы и другие организации (по месту требования), которые также используют технологии ЭДО и ЭЦП.

Предоставление услуг по внутренним коммуникациям возможно осуществлять, организовав на базе университета удостоверяющий центр, который будет

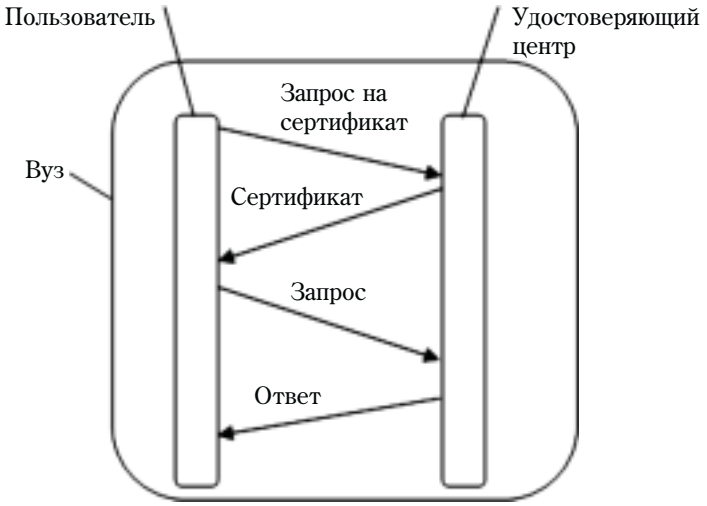

Рис. 2. Удостоверяющий центр в вузе

выдавать сертификаты и ключи пользователям информационной системы университета[1] (рис. 2).

С точки зрения глобальной инфраструктуры удостоверяющий центр на базе университета можно позиционировать двумя способами.

Первый способ. Доверенный абонентский пункт для формирования запросов пользователями на предоставление электронных государственных услуг (рис. 3). Например, у пользователя есть возможность самостоятельно формировать запросы в государственные органы, с которыми у вуза есть юридически значимый электронный документооборот. В этом случае пользователь имеет свой сертификат, а университет обеспечивает только доверенную точку доступа.

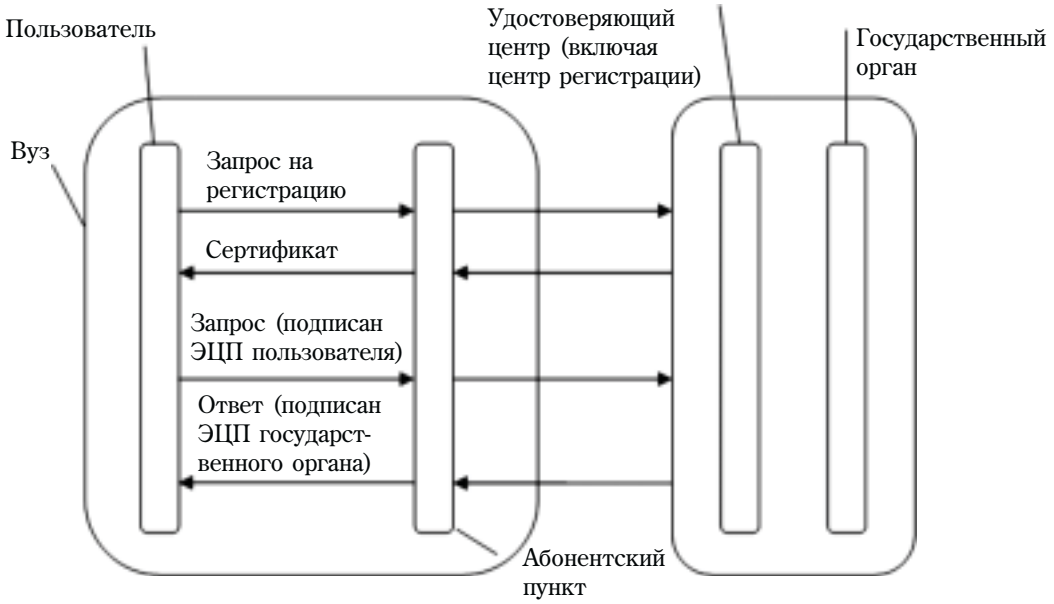

Рис. 3. Схема обмена электронными документами без центра регистрации в вузе

[1] Следует отметить, что модели взаимодействия удостоверяющих центров, представленные в данной статье (рис. 1–5), не опираются на принципиальную специфику вуза, в силу чего могут рассматриваться как универсальные.

При реализации этого способа *абонентский пункт* (АП) в вузе должен удовлетворять всем требованиям, которые предъявляются к АП удостоверяющим центром по техническому и программному обеспечению [3].

С целью повышения доступности электронных услуг с применением ЭЦП для пользователей можно развернуть на базе университета центр регистрации, который позволит вузу отправлять заявки пользователей на получение сертификатов и оперативно включать их в систему ИОК (рис. 4).

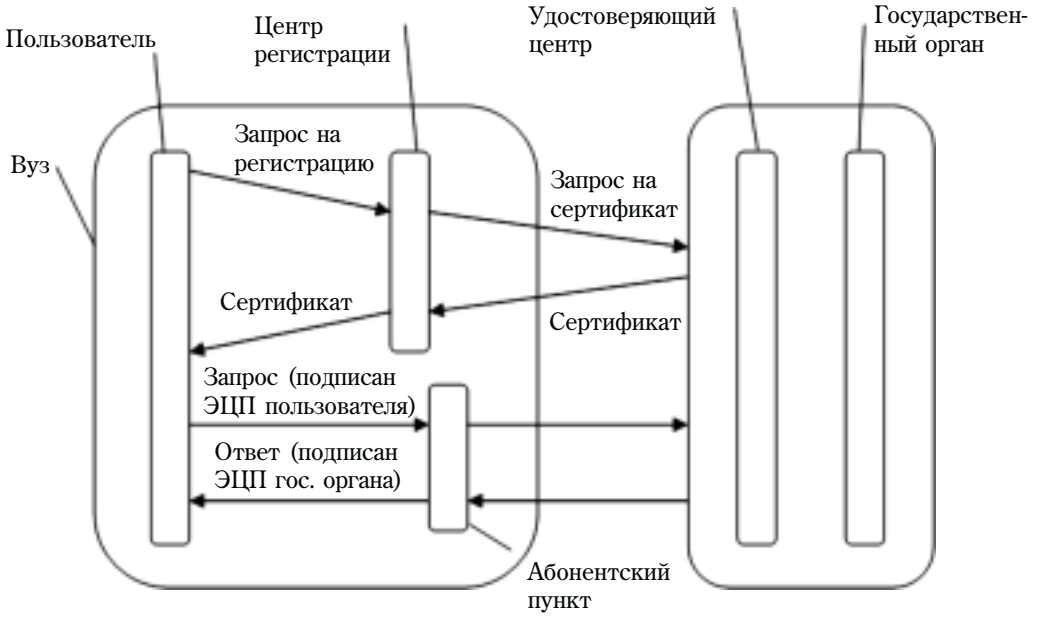

Рис. 4. Схема обмена электронными документами при наличии центра регистрации в вузе

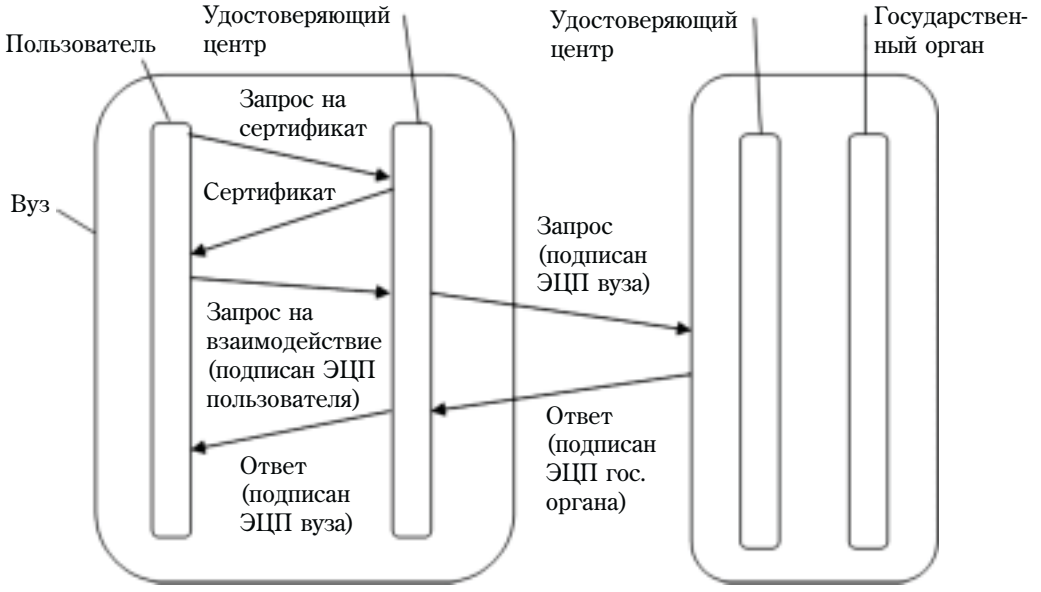

Рис. 5. Схема обмена электронными документами при наличии удостоверяющего центра в вузе

Второй способ. Доверенная сторона для формирования запросов на предоставление государственных услуг. В этом случае пользователь формирует запрос в государственные органы с использованием ЭЦП, выданной удостоверяющим центром университета. При передаче в другой удостоверяющий центр данный запрос заверяется ЭЦП университета (рис. 5).

Таким образом, разворачивание УЦ в университете позволит применить ИОК для организации юридически значимого электронного взаимодействия сотрудников и студентов. В частности, это позволит формировать официальные электронные запросы на предоставление информации, вести юридически значимый внутренний безбумажный документооборот (формирование, согласование и утверждение внутренних и организационно-распорядительных документов в электронном виде), в том числе отражающий ход учебного процесса (электронные ведомости и зачетные книжки, сертификаты и другие документы о прохождении обучения).

Требования к инфраструктуре открытых ключей со стороны законодательства

Достичь того состояния, когда электронные документы будут реально признаваемы юридически, возможно только при условии соблюдения требований законодательства [2, 3]. В соответствии со статьей 4 ФЗ «Об электронной цифровой подписи» ЭЦП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Этим же законом определяются и требования к инфраструктуре открытых ключей, зависящие от того, какие информационные системы она поддерживает. Различают информационные системы общего пользования и корпоративные информационные системы.

Информационная система общего пользования – это информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано. В корпоративной информационной системе участниками может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Законодательство не предъявляет жестких требований к ИОК корпоративных информационных системах в части сертификации средств и получения лицензий на право такой деятельности. Статус удостоверяющего центра определяется владельцем информационной системы или соглашением ее участников, если данная система не взаимодействует с информационными системами общего пользования. Использование ЭЦП регулируется внутренними нормативными

документами, такими как соглашение между участниками системы или между владельцем системы и пользователями. Функции удостоверяющего центра могут выполняться одним из участников системы.

Применительно к информационной системе университета это можно интерпретировать следующим образом. Если участниками электронного взаимодействия являются сотрудники и студенты, а существующие в электронном виде документы предназначены исключительно для внутренних целей и не предоставляются во внешние организации, то такая информационная система электронного документооборота может быть рассмотрена как корпоративная. Статус корпоративной информационной системы может сохраниться и при подключении к ней некоторых категорий сторонних пользователей на основании соответствующих соглашений. Такой подход может быть полезен, в частности, при организации взаимодействия с деловыми партнерами.

В ряде случаев возникает необходимость подключения университета к другим корпоративным информационным системам (например, при взаимодействии по системам типа «клиент–банк») – в этом случае в университете обычно устанавливается абонентский пункт без разворачивания удостоверяющего центра, и необходимо соблюдать требования к ИОК, определенные во внешней корпоративной информационной системе.

Если же планируется использовать реквизиты инфраструктуры открытых ключей университета при взаимодействии с априори неограниченным множеством других удостоверяющих центров, среди которых могут быть удостоверяющие центры органов государственной власти и информационные системы общего пользования, то подход к созданию корпоративного УЦ университета должен быть другим. Его нужно разворачивать в соответствии с максимальными требованиями по безопасности, предъявляемыми к информационным системам, с которыми планируется взаимодействие. В частности, необходимо иметь в виду, что использование несертифицированных средств электронной цифровой подписи и созданных ими ключей электронных цифровых подписей в корпоративных информационных системах федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления не допускается. В целом, нужно ориентироваться на требования, предъявляемые к удостоверяющим центрам информационных систем общего пользования:

- удостоверяющим центром является юридическое лицо, выполняющее функции, предусмотренные законодательством РФ;
- обязательным требованием в отношении имущества удостоверяющего центра информационной системы общего пользования является применение сертифицированных средств электронной цифровой подписи;
- сертификат ключа удостоверяющего центра подлежит обязательной регистрации в едином государственном реестре сертификатов ключей подписей;
- материальные и финансовые возможности удостоверяющего центра должны позволять возместить убытки пользователям информационной системы;

- обеспечение пользователей системы электронного документооборота ключевой информацией (включая ее формирование и распределение) является лицензируемым видом деятельности по предоставлению услуг в области шифрования информации [2].

Таким образом, если целью внедрения корпоративной ИОК университета является только сокращение внутреннего «бумагооборота», без выхода на электронное взаимодействие с другими удостоверяющими центрами, то при выборе технологических средств поддержки ЭЦП можно рассматривать все доступные решения, в том числе встроенные в тиражные решения систем электронного документооборота. Для создания и функционирования такого удостоверяющего центра не является обязательным использование сертифицированных программных и программно-аппаратных средств и не требуется получение организацией никаких лицензий на право деятельности в области технической и криптографической защиты информации.

Если же планируется разворачивание корпоративного удостоверяющего центра как УЦ информационной системы общего пользования (рис. 5), то необходимо выполнение следующих требований.

Требование 1. При создании удостоверяющего центра применять только специализированные сертифицированные программные и программно-аппаратные средства (примерами таких сертифицированных технологий являются, в частности, решения на базе продуктов «VipNet», «Континент», «Контур-экстерн»).

Требование 2. Организация должна получить лицензии на следующие виды деятельности:

- Лицензия ФСБ России на распространение криптографических средств защиты информации;
- Лицензия ФСБ России на техническое обслуживание криптографических средств защиты информации;
- Лицензия ФСБ России на предоставление услуг в области криптографической защиты информации;
- Лицензия ФСТЭК России на право осуществления деятельности по технической защите конфиденциальной информации.

Данный подход является более затратным на начальном этапе, но его реализация открывает широкие перспективы, связанные с интеграцией корпоративного УЦ в глобальную ИОК, которая развивается в рамках создания электронного государства. При реализации схемы (рис. 4) возможно определенное сокращение затрат за счет того, что часть функций, подпадающих под требования лицензирования, берет на себя головной удостоверяющий центр, на базе которого создается центр регистрации в вузе. Кроме того, в головном удостоверяющем центре также будет сосредоточена основная часть дорогостоящего сертифицированного программно-аппаратного обеспечения ИОК.

Перспективы расширения спектра услуг, предоставляемых пользователям ИОК, здесь в полной мере зависят от двух факторов. С одной стороны – от возможностей тех УЦ, через которые будет организовано взаимодействие с государственными органами и другими внешними по отношению к университету абонентами ИОК. С другой – от того, насколько организация, создавшая УЦ

общего пользования, сумеет привлечь в качестве клиентов своего УЦ другие организации, услуги которых могут быть востребованы ее сотрудниками и другими абонентами.

Литература

1. *Adams C., Lloyd S.* Understanding PKI. Concepts, Standards and Deployment. Second Edition, Addison-Wesley, 2002.
2. Статья 17 Федерального закона от 08.08.2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности».
3. Федеральный закон от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи».