DOI 10.37882/2223–2966.2020.08–2.03

ВОПРОСЫ ВНЕДРЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ

INTRODUCING ELECTRONIC SIGNATURES IN HIGHER EDUCATION INSTITUTIONS

D. Brechka

Summary. The article discusses the problem of implementing an electronic signature in the electronic document management system of a higher educational institution. Relevance is associated with the massive digitalization of business processes and the increasing distribution of electronic document management. The aim of the work is to develop a typical scheme for organizing an electronic signature infrastructure. The main results are:

- formulation of requirements for electronic document management systems, for the correct choice of systems that correspond to the tasks solved in modern higher educational institutions.
- characterization of the necessary elements of the electronic signature infrastructure for building a complete picture of all work-stages on implementing the electronic signature.
- offering a model for using various types of electronic signatures in accordance with the type of documents to be signed, correlated with the hierarchical structure of organization management.

Keywords: electronic signature, document management, electronic signature infrastructure, criteria for selecting an electronic document management system.

Бречка Денис Михайлович
К.т.н., доцент, ФГБОУ ВО «Сибирский государственный автомобильно-дорожный университет» (г. Омск)
dbrechkawork@yandex.ru

Аннотация. В статье рассматривается проблема внедрения электронной подписи в системе электронного документооборота высшего учебного заведения. Актуальность связана с массовой цифровизацией бизнес-процессов и все большим внедрением электронного документооборота в организациях. Целью работы является разработка типовой схемы организации инфраструктуры электронной подписи. Основными результатами является:.

- формулирование требований к системам электронного документооборота, для правильного выбора систем, соответствующих задачам, решаемым в современных ВУЗах.
- характеристика необходимых элементов инфраструктуры электронной подписи, для выстраивания полной картины всех этапов работ по внедрению ЭП.
- предложение модели использования различных видов электронных подписей в соответствии с типом подписываемых документов, соотнесенных с иерархической структурой управления ВУЗом.

Ключевые слова: электронная подпись, документооборот, инфраструктура электронной подписи, критерии выбора системы электронного документооборота.

Введение

Современные заведения высшего образования в Российской Федерации (ВУЗы) обычно имеют сложную иерархическую структуру управления. Осуществление бизнес-процессов в таких структурах неизбежно сопряжено с составлением и согласованием большого количества документов. Вопрос о необходимости автоматизации бизнес-процессов и документооборота на сегодняшний день чаще всего решается положительно, однако процедура автоматизации, в большинстве случаев, затягивается, что связано, в первую очередь, со сложностью самих бизнес-процессов. Однако опыт многих ВУЗов (вот примеры лишь некоторых опубликованных работ [1–4]) показывает, что процесс автоматизации все же осуществим, а результаты внедрения сказываются неизменно положительно на работе автоматизированных подразделений и всего ВУЗа в целом. В связи с этим, становится очевидно, что работы в указанном направлении следует продолжать и выводить на более высокий уровень.

Одним из аспектов автоматизации бизнес-процессов и документооборота является внедрение электронной подписи [5,6]. Данный процесс можно разбить на два основных этапа:

1. организация инфраструктуры электронной подписи в информационной среде ВУЗа;
2. внедрение электронной подписи в систему электронного документооборота ВУЗа.

Целью данной статьи является создание типовой схемы организации инфраструктуры электронной подписи в заведении высшего образования.

Автор отдает себе отчет в том, что экосистема каждого ВУЗа является уникальной и задача создания абсолютно универсальной, применимой для всех схемы, скорее всего является невыполнимой. Однако, анализ

Рис. 1. Пример иерархии должностных отношений

опубликованных работ по теме внедрения электронной подписи [7,8] показывает, что большинство организаций сталкиваются со схожими проблемами, а значит, результаты, опубликованные в данной статье, могут быть полезны специалистам, занимающимся обозначенным вопросом.

1. Иерархическая структура должностных отношений

В абсолютном большинстве случаев система управления ВУЗом имеет иерархическую структуру. Пример такой структуры, с отображением названий должностей приведен на рисунке 1.

Конечно, структура, представленная на рисунке 1 не является исчерпывающей, и в случае каждого конкретного ВУЗа может существенно отличаться, однако сохранение иерархичности отношений остается неизменным.

Выстраивание иерархии должностных отношений в ВУЗе может оказаться весьма непростой задачей, однако является важным этапом с точки зрения описания бизнес-процесса. В том числе, использование электронной подписи, как будет показано ниже, может быть ранжировано по уровням должностных полномочий.

Практически всегда бизнес-процесс в такой иерархической структуре сопровождается составлением и согласованием большого количества документов: договоры, соглашения, положения, служебные записки и прочее. Все эти документы будем делить на два класса:

- внешние — предназначенные для установления правоотношений со внешними, по отношению к ВУЗу, организациями;
- внутренние — предназначенные, для согласования бизнес-процессов между отдельными подразделениями ВУЗа и должностными лицами.

Внедрение систем электронного документооборота (СЭД) призвано повысить удобство обработки как внешних, так и внутренних документов и сократить время на осуществление бизнес-процессов.

2. Критерии выбора системы электронного документооборота

Количество СЭД, представленных сегодня на рынке, довольно велико, следовательно, необходимо выработать критерии выбора СЭД, удовлетворяющей запросам современного ВУЗа. Основой для выбора критериев может служить спецификация «Типовые требования к автоматизированным системам электронного документооборота» (англ. Model Requirements for the Management of Electronic Records, MoReq2010 [9]), содержащая обширный набор требований, которым должны удовлетворять современные СЭД. Рассмотрим наиболее значимые, с точки зрения обозначенных задач требования.

1. Система управления пользователями. Количество пользователей СЭД в ВУЗе может быть очень велико. Разные пользователи должны иметь разный

уровень доступа документам различных классов. Более того, очень часто один и тот же сотрудник выполняет несколько должностных обязанностей, поэтому один пользователь системы может иметь разные права доступа, в зависимости от того, какую роль он исполняет в конкретный момент времени. Таким образом, система контроля доступа и управления пользователями в СЭД должна быть достаточно развитой. В MoReq2010 предусматривается возможность задания прав доступа на документы как отдельным пользователям, так и группам пользователей. Также присутствуют требования по управлению ролями пользователей. То есть, СЭД должна поддерживать дискреционную, групповую и ролевую политики управления доступом [10].

2. Классификация и агрегация документов. Очевидно, что выработать универсальную номенклатуру классов документов, подходящую для всех организаций невозможно, как следствие, СЭД должна позволять пользователям создавать собственные классы. Более того, СЭД должна поддерживать возможность иерархической организации классов документов, что позволит соотносить документы с иерархической структурой управления в организации.
3. Поддержка жизненного цикла документов. Этапы жизненного цикла документов хорошо описаны в серии статей Е. М. Каменевой [11–13]. Из анализа источников видно, что жизненный цикл может быть довольно сложными и различаться для разных документов. Следовательно, СЭД должна позволять задавать этапы жизненного цикла для каждого класса документов и следить за правильной последовательностью прохождения этапов. Более того, СЭД должна вести журнал, в котором должны отображаться события, связанные прохождением этапов жизненного цикла каждым документом. Данное требование подтверждается в том числе ГОСТ Р 54471–2011 [14].
4. Кроссплатформенность СЭД. В современном мире практически каждый человек владеет несколькими вычислительными устройствами, например, рабочий компьютер, домашний компьютер, смартфон и т.д. Если клиентская часть СЭД может быть установлена только на одной платформе (например, на рабочем компьютере под управлением операционной системы Windows), то это резко снижает удобство использования системы. Хорошим вариантом будет наличие у СЭД web-интерфейса, а еще лучшим — наличие клиентской части для мобильных устройств.
5. Безопасность. Высокая доступность СЭД понуждает обратить пристальное внимание на вопросы безопасности. СЭД должна поддерживать гибкую настройку политики средств аутентификации пользователей и политики разделения доступа. При этом разделение доступа должно основываться не только на атрибутах пользователя, но и на атрибутах документа. Например, к некоторым категориям документов может потребоваться запретить доступ через web-интерфейс и мобильные приложения. Также СЭД должна уделять внимание контролю целостности документов, защите журналов событий, доступности самой системы, архивированию и защите архивов. Должна быть исключена возможность доступа к документам в обход системы контроля доступа СЭД.
6. Поддержка электронной подписи. Подписание является неотъемлемой частью жизненного цикла документа. При чем подписание (визирование) может требоваться на разных этапах жизненного цикла документа, на одном документе может требоваться подпись разных людей. Когда речь идет о СЭД, в качестве собственноручной подписи может использоваться электронная подпись (ЭП). Использование электронной подписи регламентируется Федеральным законом Российской Федерации № 63 от 06.04.2011 (ФЗ-63) [15]. СЭД должна поддерживать инфраструктуру электронной подписи, позволять осуществлять подписание документа и проверять подпись.
7. Расширяемость. Если СЭД не поддерживает одно или несколько из представленных требований, либо у организации есть требования, не учтенные в данном списке, то СЭД должна обеспечивать возможность расширения путем подключения дополнительных модулей, либо предоставлять возможность разработки новых подключаемых программных модулей.
8. Характеристика видов электронной подписи

Как уже было сказано выше, использование электронной подписи в Российской Федерации регламентируется федеральным законом № 63. Данный документ выделяет три вида электронной подписи:

- простая электронная подпись (ПЭП);
- неквалифицированная электронная подпись (НЭП);
- квалифицированная электронная подпись (КЭП).

Все виды подписей, должны проверять целостность документов и позволять устанавливать лицо подписавшее документ (это свойство еще называют неотказуемостью). Ниже приведена краткая характеристика каждого вида подписи.

ПЭП — это вариант электронной подписи не предполагающий использование криптографических

преобразований. Обычно ПЭП реализуется средствами СЭД, которая может устанавливать/отслеживать специальные свойства электронного документа. ПЭП — это технически самый простой вариант электронной подписи, обычно она уже встроена в СЭД и редко требует сложных настроек и установки дополнительного программного обеспечения. Отсутствие криптографических преобразований снижает надежность такой подписи, как следствие ее следует использовать там, где риски подлога документов минимальны. Еще одним важным аспектом ПЭП является то, что она не признается аналогом собственноручной подписи без наличия специального соглашения между участниками электронного взаимодействия, устанавливающего порядок использования и способ проверки подписи. Такое соглашение может быть заключено между отдельными организациями (в нашем случае между ВУЗом и каждой внешней организацией) или между подразделениями одной организации (достаточно одного общего соглашения на весь ВУЗ), в любом случае соглашение должно быть юридически оформлено и соответствовать требованиям, представленным в ФЗ-63.

НЭП предполагает использование технологий электронной цифровой подписи (ЭЦП) для формирования и проверки подписи документа. Этот факт делает подпись более надежной, но, вместе с тем, технически более сложной — требуется наличие (поддержка) специальной инфраструктуры ЭЦП, о которой речь пойдет ниже. При этом НЭП, как и ПЭП, не признается без наличия дополнительного соглашения.

Наконец, самым надежным видом электронной подписи считается КЭП. Такая подпись, как и НЭП, основана на ЭЦП, но при этом предполагает государственный контроль за использованием криптографических средств. Самым большим плюсом КЭП является то, что она может быть признана без наличия дополнительных соглашений, но, при этом, техническая реализация, ожидаемо, еще более сложная чем у НЭП.

4. Инфраструктура электронной цифровой подписи

Для понимания того, что нужно для работы электронных подписей, использующих ЭЦП (такие подписи еще называют усиленными, к ним относят КЭП и НЭП) кратко охарактеризуем эту технологию. Наиболее распространенной на сегодняшний день технологией ЭЦП является ЭЦП, основанная на асимметричных алгоритмах шифрования [16]. В таких алгоритмах шифрование и дешифрование информации производится разными ключами, которые генерируются парами. Подписание электронного документа — это шифрование документа ключом, который хранится в секрете. Полученная криптограмма называется электронной подписью документа и распространяется совместно с исходным документом. Дешифрование криптограммы производится открытым (общедоступным) ключом, парным к секретному. Если результаты дешифрования совпали с исходным документом, то:

1. исходный документ не был изменен, таким образом подтверждается целостность документа;
2. документ был зашифрован парным к открытому ключом, принадлежащим подписанту, таким образом устанавливается личность подписанта.

Известной проблемой асимметричных алгоритмов является проблема доверия ключей. То есть необходим механизм, позволяющий удостовериться в том, что открытый ключ действительно принадлежит конкретному указанному пользователю. Для электронной подписи это означает, что у подписавшего лица не должно быть возможности отказаться от своей подписи (свойство неотказуемости ЭП).

Указанная проблема решается с помощью третей доверенной стороны. Этой стороне доверяют как подписант, так и лицо проверяющее подпись. Доверенная сторона выпускает так называемые сертификаты открытых ключей, которые распространяются свободно. Данный сертификат подтверждает, что открытый ключ действительно принадлежит указанному пользователю.

Доверенной стороной выступает удостоверяющий центр (УЦ), другие названия этого объекта — центр сертификации (ЦС), certification authority (CA). Данный объект является обязательной частью инфраструктуры ЭЦП. В задачи УЦ входит следующее.

1. Генерация пар ключей. Для каждого лица, желающего подписывать электронные документы, УЦ генерирует пару открытый-закрытый ключ электронной подписи.
2. Распространение сертификатов ключей. Закрытый ключ должен быть надежным способом передан пользователю, например, лично, на специальном носителе или по защищенному каналу связи. Для открытого ключа формируется сертификат, который распространяется без ограничений, например, публикуется в общедоступном каталоге сертификатов.

Еще одним элементом инфраструктуры ЭЦП является криптопровайдер. Это клиентское программное обеспечение, в функции которого входит (как минимум) следующее.

1. Подписание электронного документа. Криптопровайдеру передаются электронный документ и сертификат закрытого ключа пользователя.

По этим данным криптопровайдер формирует электронную подпись документа.

2. Проверка электронной подписи. Криптопровайдеру передаются электронный документ, его электронная подпись и сертификат открытого ключа пользователя. По этим данным криптопровайдер делает заключение о корректности или некорректности подписи.

Третьим элементом инфраструктуры ЭЦП выступает рабочее место пользователя. Под этим термином будем понимать вычислительную систему, на которой установлена клиентская часть СЭД и выполнены определенные настройки, позволяющие использовать ЭЦП в СЭД.

Наконец четвертым, важным элементом инфраструктуры является нормативная документация, без которой, как было сказано выше, ПЭП и НЭП не признаются аналогами собственноручной подписи. Сюда же можно отнести документы, регламентирующие использование электронного документооборота в организации. Эти документы не относятся напрямую к ЭЦП, но, так как мы рассматриваем применение ЭЦП в рамках электронного документооборота, отсутствие этих документов сделает невозможным использование СЭД и, как следствие, ЭЦП. Ни в коем случае не стоит недооценивать значимость нормативной базы, как показывает практика, при наличии всех технических возможностей, но отсутствии регламентирующих документов ни СЭД, ни ЭЦП использоваться не будут.

Разобравшись с необходимыми для ЭЦП элементами инфраструктуры, стоит обратить внимание на особенности их реализации и использования. Первый, выделенный нами элемент — удостоверяющий центр, и есть большая разница между УЦ для КЭП и НЭП. Удостоверяющий центр для квалифицированной электронной подписи должен обязательно быть аккредитован государственным органом (см. требования ФЗ-63), для пользователей услуги такого УЦ предоставляются за отдельную плату. Таким образом, аккредитованный УЦ является внешним, по отношению к организации субъектом, выпускающим и распространяющим ключи электронной подписи. Ключи могут быть предоставлены на специальном защищенном носителе, а затем интегрированы в криптопровайдер. Актуальный список аккредитованных удостоверяющих центров можно получить на сайте Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации [17].

На удостоверяющий центр для НЭП не распространяется требование государственной аккредитации, и, следовательно, УЦ может быть создан силами сотрудников организации с использованием любой подходящей технологии. Примером такой технологии может служить Active Directory Certificate Services от компании Microsoft. Достоинством является то, что службы сертификатов интегрируются доменную службу Microsoft, которая часто уже используется в организациях. При этом службы сертификатов обладают достаточно широкими функциональными возможностями, а настройка производится с помощью удобного мастера и не вызывает серьезных затруднений. Подробно настройка удостоверяющего центра на основе Active Directory Certificate Services описана в [18]. Однако данная технология является проприетарной и коммерческой, в качестве альтернативы могут быть использованы открытые решения, одним из наиболее известных является OpenSSL [19].

Следующий, рассмотренный нами элемент инфраструктуры ЭЦП — криптопровайдер. Как уже было сказано выше, это клиентское программное обеспечение, которое должно быть установлено на каждое рабочее место пользователя. И снова есть отличия между криптопровайдерами для КЭП и НЭП.

Криптопровайдер для КЭП должен поддерживать российские криптографические алгоритмы, используемые при формировании квалифицированной электронной подписи [20] и иметь сертификат ФСБ (см. требования ФЗ-63). Такие криптопровайдеры устанавливаются как дополнительное программное обеспечение на клиентской операционной системе. Чаще всего это программное обеспечение является коммерческим и требует приобретения лицензии на каждое рабочее место.

В качестве криптопровайдера НЭП для операционной системы Windows может использоваться уже встроенный набор API-функций — CryptoAPI. Эти API-функции реализуют весь необходимый функционал криптопровайдера, однако доступны только через посредство дополнительного приложения, обращающегося к этим функциям, стандартного приложения в Windows для работы с CryptoAPI на данный момент нет. Таким образом, для работы с криптопровайдером на пользовательском уровне все равно потребуется устанавливать дополнительное программное обеспечение, хотя в некоторых случаях будет достаточно установить клиентскую часть СЭД, которая может обращаться к CryptoAPI напрямую (например, СЭД ELMA ECM+ [21]). В случае операционной системы отличной от Windows, можно использовать тот же криптопровайдер, что и для КЭП (большинство криптопровайдеров КЭП поддерживают работу с НЭП, например, КриптоПро [22]). Существуют также и свободные решения, например, уже упомянутый OpenSSL или GPG [23].

Что касается настроек рабочего места пользователя, то для КЭП и НЭП они практически не отличаются. Чаще всего потребуется:

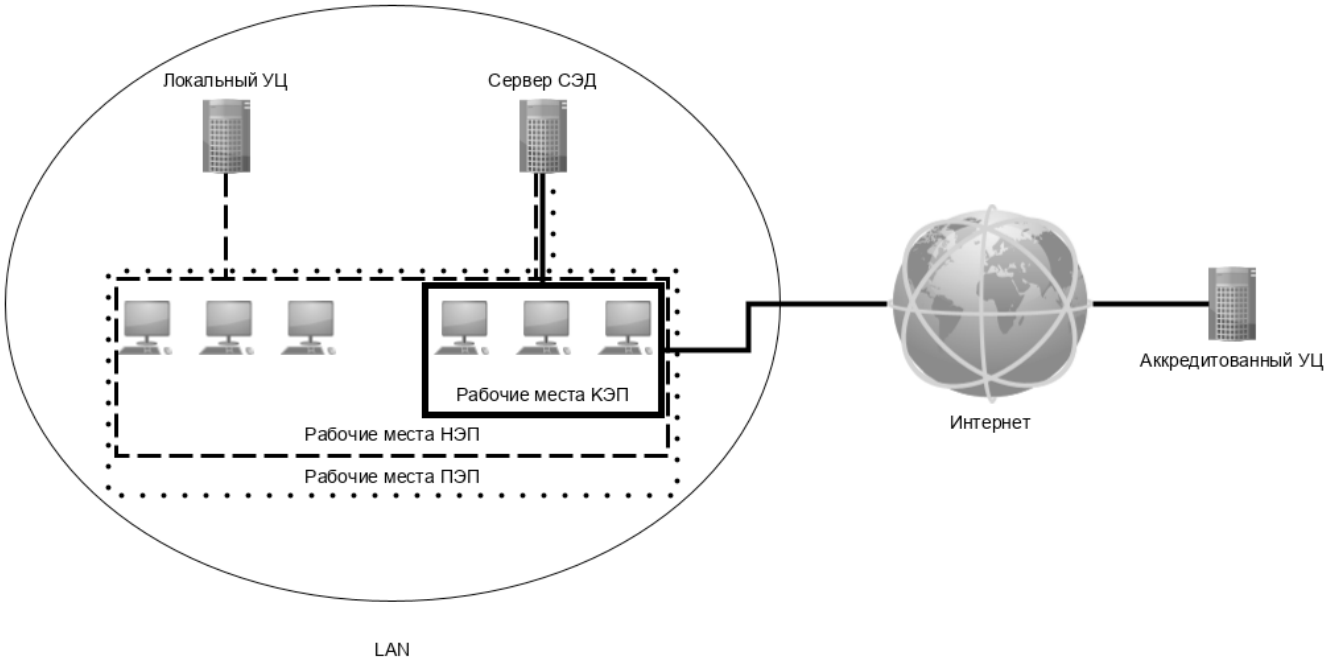


Рис. 2. Элементы инфраструктуры электронной подписи

- установить криптопровайдер;
- установить и настроить клиентскую часть СЭД (конкретные настройки зависят от СЭД, но, как минимум, необходимо настроить работу СЭД с соответствующим криптопровайдером);
- установить расширение браузера для работы с электронной подписью;
- установить сертификат (сертификаты) удостоверяющего центра;
- импортировать ключи электронной подписи;
- установить драйверы для работы с защищенными носителями ключевой информации (если используются).

Нормативная документация должна отвечать на ряд вопросов относительно того какие пользователи (группы, роли) в каких случаях могут использовать тот или иной вид электронной подписи. Здесь вероятнее всего, придется учитывать иерархическую структуру управления организацией и ранжировать использование ЭП по уровням иерархии. Рассмотрим подробнее эти моменты в следующем разделе.

5. Применение электронной подписи в системе документооборота высшего учебного заведения

Рассмотрим модель применения различных видов электронной подписи в иерархической структуре управления ВУЗом. Наиболее удобной в применении могла бы быть квалифицированная электронная подпись, так как она имеет юридическую силу без дополнительных соглашений. Но, как было сказано выше, использование КЭП требует закупки ключей и сертифицированных криптопровайдеров. Поэтому применять КЭП выгоднее всего только для подписания внешних документов, это позволит воспользоваться преимуществами электронного документооборота и избавит от необходимости заключения соглашений об использовании ЭП с каждой внешней организацией. Предоставить возможность использования КЭП необходимо только тем сотрудникам, в чьи должностные обязанности входит согласование внешних документов, что позволит сократить затраты на закупку сертифицированных средств. Если обратиться к рисунку 1, то это сотрудники нулевого, первого и, возможно, второго уровня иерархии.

Для согласования внутренних документов одинаково подойдет ПЭП и НЭП, однако, при выборе между ними, следует учитывать уровень надежности того и другого вида подписи. По мнению автора, в ВУЗе можно найти применение обеим видам подписей, ограничив круг задач, решаемых каждой из них.

Если ПЭП, реализуемая средствами СЭД, гарантирует целостность и неотказуемость, то она вполне пригодна для использования в рамках данной СЭД. Безусловным преимуществом в этом случае выступает отсутствие необходимости организации инфраструктуры ЭЦП. К сожалению, не всегда система электронного документо-

оборота поддерживает качественную ПЭП. Более того, очень часто в ВУЗах используется несколько различных информационных систем (в том числе СЭД), и периодически возникает необходимость обмена документами между этими системами. В таких ситуациях использовать ПЭП будет крайне неудобно, так как сложно однозначно идентифицировать автора документа, не говоря уже о гарантии целостности. Таким образом, использовать простую электронную подпись рекомендуется в рамках одной системы документооборота и то, при условии соответствия ПЭП необходимым требованиям, в остальных случаях лучшим решением будет неквалифицированная подпись.

Рис. 2 обобщает сказанное, на нем изображены элементы инфраструктуры электронной подписи и связи между ними.

Выводы

В данной статье были рассмотрены особенности использования электронной подписи в рамках системы электронного документооборота в ВУЗе. Было показано, что введение электронного документооборота, являющегося одним из этапов автоматизации бизнес-процессов, неизменно сопряжено с необходимостью использования электронной подписи.

Сформулированы требования к системам электронного документооборота, позволяющие правильно выбрать систему, соответствующую задачам, решаемым в современных ВУЗах. Показана необходимость поддержки инфраструктуры электронной подписи со стороны СЭД.

Также были затронуты вопросы технической реализации инфраструктуры электронной подписи, показаны и охарактеризованы необходимые элементы инфраструктуры, что позволяет выстроить полную картину всех этапов работ по внедрению ЭП.

Наконец были показаны возможности применения различных видов электронных подписей в соответствии с типом подписываемых документов, соотнесенных с иерархической структурой управления ВУЗом.

Таким образом, сформирована типовая схема применения электронной подписи в системе электронного документооборота ВУЗа. Схема может быть дополнена, с учетом особенностей конкретной организации, но основные ее элементы останутся неизменными в абсолютном большинстве случаев.

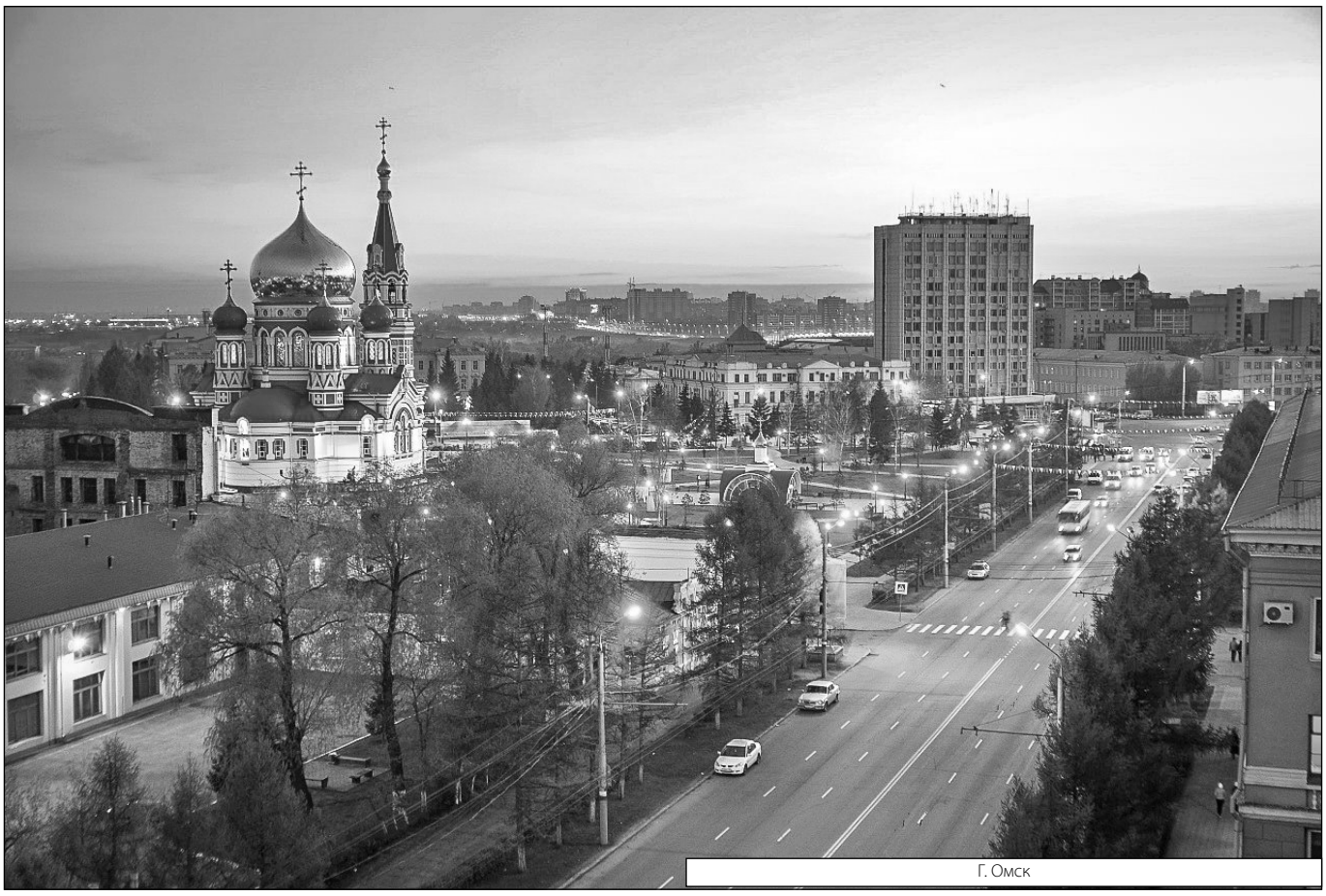
Как видно, задача внедрения электронной подписи довольно сложная, требует временных и финансовых затрат. При внедрении любой новой технологии в бизнес-процесс всегда следует оценивать риски затраты и положительные эффекты. Однако, в современных условиях, когда цифровизация бизнес-процессов приобретает массовый характер, внедрение электронной подписи становится необходимым условием эффективности работы предприятия. Автор надеется, что приведенные в данной статье результаты, помогут специалистам в решении указанных проблем.

ЛИТЕРАТУРА

1. Магомедова П. Р., Лачинов Н. З. Автоматизация процесса назначения стипендий с помощью модуля «Стипендия» для аналитической системы вуза (на примере Дагестанского государственного университета) // Международный научно-исследовательский журнал. — 2016. — № 1 (43) Часть 2. — С. 47–49.
2. Полупанова С. П., Скороход С. В. Автоматизация учёта абитуриентов при поступлении в вуз // Известия ЮФУ. Технические науки. 2007. № 1. URL: https://cyberleninka.ru/article/n/avtomatizatsiya-uchyota-abiturientov-pri-postuplenii-v-vuz (дата обращения: 20.07.2020).
3. Андреева К. А., Когай В. Н. Необходимость и степень внедрения электронного документооборота в вузе // Достижения науки и образования. 2019. № 2 (43). URL: https://cyberleninka.ru/article/n/neobhodimost-i-stepen-vnedreniya-elektronnogo-dokumentooborota-v-vuze (дата обращения: 20.07.2020).
4. Клишин А. П., Волкова Н. Р., Еремина Н. Л., Мытник А. А., Клыжко Е. Н. Подходы к автоматизации документооборота в вузе // Вестник НГУ. Серия: Информационные технологии. 2017. № 1. URL: https://cyberleninka.ru/article/n/podhody-k-avtomatizatsii-dokumentooborota-v-vuze (дата обращения: 20.07.2020).
5. Попов, С. С. Система электронной подписи в современном документообороте // Молодой ученый. — 2019. — № 6 (244). — С. 86–88. — URL: https://moluch.ru/archive/244/56451/ (дата обращения: 20.07.2020).
6. Астахова Т. С., Чадаева Е. П. Электронная цифровая подпись как фактор сохранения целостности и аутентичности документа // Известия ТПУ. 2012. № 6. URL: https://cyberleninka.ru/article/n/elektronnaya-tsifrovaya-podpis-kak-faktor-sohraneniya-tselostnosti-i-autentichnosti-dokumenta (дата обращения: 20.07.2020).
7. Середа К. В. Проблемы внедрения электронной подписи // Электронный вестник Ростовского социально-экономического института. 2014. № 3. URL: https://cyberleninka.ru/article/n/problemy-vnedreniya-elektronnoy-podpisi (дата обращения: 20.07.2020).
8. Ермоленко А. В. Практика применения электронной цифровой подписи в деятельности организаций: реальность и перспективы // Правовая информатика. 2013. № 3. URL: https://cyberleninka.ru/article/n/praktika-primeneniya-elektronnoy-tsifrovoy-podpisi-v-deyatelnosti-organizatsiy-realnost-i-perspektivy (дата обращения: 20.07.2020).
9. DLM Forum Foundation, European Commission Modular Requirements for Records Systems. Version 1.1.

10. Девянин П. Н. Модели безопасности компьютерных систем: Учеб. Пособие для студ. высш. учеб. заведений [текст] /П.Н. Девянин.— М.: Издательский центр «Академия», 2005.— 144 с.
11. Каменева Е. М. Жизненный цикл входящего документа // Секретарь-референт. 2010. № 3. URL: https://www.eos.ru/upload/Lib/17–24%20%283%29.pdf (дата обращения: 20.07.2020).
12. Каменева Е. М. Жизненный цикл внутреннего документа // Секретарь-референт. 2010. № 4. URL https://www.eos.ru/upload/Lib/17–24%20(4).pdf (дата обращения: 20.07.2020).
13. Каменева Е. М. Жизненный цикл исходящего документа // Секретарь-референт. 2010. № 5. URL https://www.eos.ru/upload/Lib/17–22%20(5).pdf (дата обращения: 20.07.2020).
14. ГОСТ Р 54471–2011. Системы электронного документооборота. Управление документацией. Информация, сохраняемая в электронном виде. Рекомендации по обеспечению достоверности и надежности.
15. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ — Доступ из справ.-правовой системы КонсультантПлюс.— Текст: электронный.
16. Тарасов А. М. Криптография и электронная цифровая подпись // Российский исследователь. 2014. № 1 С. 50–54.
17. Список аккредитованных удостоверяющих центров URL https://digital.gov.ru/ru/activity/govservices/certification_authority (дата обращения: 20.07.2020).
18. Гайкова П. Д. Реализация инфраструктуры неквалифицированной электронной подписи в системе электронного документооборота ELMA: выпускная квалиф. работа. Федеральное государственное учреждения высшего образования «Сибирский государственный автомобильно-дорожный университет (СибАДИ)», Омск, 2020.
19. OpenSSL Cryptography and SSL/TLS Toolkit URL https://www.openssl.org (дата обращения: 20.07.2020).
20. ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
21. ELMA ECM+ URL https://www.elma-bpm.ru/KB/help/Docflow/content/Introduction.html (дата обращения: 20.07.2020).
22. КриптоПро URL https://www.cryptopro.ru (дата обращения: 20.07.2020).
23. GnuPG URL https://www.cryptopro.ru (дата обращения: 20.07.2020).

Журнал «Современная наука: актуальные проблемы теории и практики»



Г. Омск