ПРИЛОЖЕНИЕ № 6
к протоколу заседания подкомиссии
по использованию информационных технологий
при предоставлении государственных и муниципальных услуг
Правительственной комиссии
по использованию информационных технологий
для улучшения качества жизни и условий ведения
предпринимательской деятельности
от 31 марта 2017 г. № ____

ОДОБРЕНО
подкомиссией по использованию информационных технологий
при предоставлении государственных и муниципальных услуг
Правительственной комиссии
по использованию информационных технологий
для улучшения качества жизни и условий ведения
предпринимательской деятельности
(протокол от 31 марта 2017 г. №___)

КОНЦЕПЦИЯ
хранения и использования электронных документов с обеспечением их юридической силы для финансового рынка

СОДЕРЖАНИЕ

стр.

1. ОБЩИЕ ПОЛОЖЕНИЯ …… 2
1.1. Общая характеристика..…… 2
1.2.Субъекты концепции ...…….... 2
1.3. Объекты концепции ...……. 3
2. ЮРИДИЧЕСКАЯ СИЛА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ …….…..... 3
2.1. Условия признания юридической силы электронных документов при использовании различных видов электронной подписи и технологий ее применения ……. 3
2.2. Обеспечение юридической силы электронного документа при хранении в режиме оперативного доступа ……... 6
2.3. Обеспечение юридической силы электронного документа в режиме долговременного хранения ……. 6
2.4. Юридическая сила документа при преобразовании формы его представления (из бумажной в электронную и из электронной в бумажную) …….. 7
3. ХРАНЕНИЕ И УНИЧТОЖЕНИЕ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ …... 8
3.1. Технологическое обеспечение долговременного хранения электронных документов ……... 8
3.2. Нормативная, методическая и технологическая поддержка мероприятий по обеспечению долговременного хранения …… 9
3.3. Особенности уничтожения электронных документов участников финансового рынка …… 10
4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, СОХРАННОСТЬ И ЗАЩИТА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ НА ВСЕХ ЭТАПАХ ИХ ЖИЗНЕННОГО ЦИКЛА. ЗАЩИТА СРЕДЫ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ …… 11
5. ДОСТУП К ЭЛЕКТРОННЫМ ДОКУМЕНТАМ И ИХ ПРЕДОСТАВЛЕНИЕ…….…… 12
5.1. Принципы доступа к документам в электронной форме на финансовом рынке. Обеспечение режимов конфиденциальности электронных документов. Технологии, используемые для доступа к электронным документам …… 12
5.2. Требования к системам управления документами и другим информационным системам в части обеспечения установленного правового режима информации ….. 13
6. ТЕРМИНЫ И СОКРАЩЕНИЯ …..... 14

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Общая характеристика

В настоящее время в Российской Федерации отсутствует полноценная нормативно-технологическая основа и единые подходы к хранению и использованию электронных документов участниками финансового рынка, что приводит к дублированию электронных и бумажных технологий, тормозит переход к эффективному безбумажному взаимодействию субъектов финансового рынка как между собой, так и с их клиентами.

Одним из барьеров, препятствующих дальнейшему развитию электронного документооборота между участниками финансового рынка, является проблема обеспечения юридической силы электронных документов в процессе их долговременного хранения. В отличие от бумажных документов, которые могут храниться длительное время, сохраняя свою юридическую силу и доступность для восприятия, электронные документы неразрывно связаны с динамично меняющимися технологиями и требуют целого комплекса периодических мероприятий по обеспечению их физической сохранности и доступности, а также сохранению их юридической силы.

Для преодоления указанного барьера необходима разработка комплекса мер, включающих:

- установление нормативных требований непосредственно к электронным документам, информационным системам и сервисам работы с ними;
- выбор мер, необходимых и достаточных для сохранения юридической силы электронных документов и пригодности их к использованию в течение всего жизненного цикла документа;
- определение оптимальных форм организации работы с электронными документами участников финансового рынка (включая их создание, обращение, хранение и уничтожение),
- осуществление мероприятий по внедрению организационно-технологических требований, соблюдение которых будет обеспечивать юридическую силу электронных документов для финансового рынка.

Настоящая концепция базируется на изучении многолетнего мирового опыта нормативного регулирования электронного документооборота и хранения электронных документов, а также передовой отечественной практики. В ней определены основные подходы к обеспечению юридической силы при хранении и использовании электронных документов, сформулированы принципиальные подходы и рекомендации по применению современных технологий для долговременного хранения электронных документов.

В результате реализации мероприятий, обоснованных данной концепцией, доля документов, создаваемых в настоящее время на бумажном носителе, должна последовательно сокращаться при соответствующем расширении применения электронного документооборота между участниками финансового рынка.

1.2. Субъекты концепции

Субъектами концепции являются участники финансового рынка – кредитные и некредитные финансовые организации Российской Федерации, иные участники финансового рынка (например, эмитенты эмиссионных ценных бумаг), а также их клиенты – юридические и физические лица.

Субъектом концепции может быть также Центральный банк Российской Федерации в случаях, когда он осуществляет деятельность на финансовом рынке в качестве субъекта финансового рынка.

Субъекты концепции существенно различаются по роли на финансовом рынке, масштабу деятельности и объему документооборота. Кроме того, субъекты финансового рынка осуществляют электронный документооборот на разной организационно-технологической основе. Указанные обстоятельства являются существенными и определяют сложность решения проблем хранения и использования электронных документов участниками финансового рынка. С одной стороны, требуется организовать эту работу на общих принципах, единых подходах и тиражируемых технологических решениях, с другой стороны – предусмотреть поэтапное осуществление этой работы по мере готовности конкретных групп субъектов финансового рынка.

1.3. Объекты концепции

Объектами концепции являются электронные документы субъектов финансового рынка, используемые при их взаимодействии между собой, а также с клиентами. Вопросы внутреннего управленческого документооборота в организациях в рамках данной концепции не затрагиваются. В настоящей концепции не рассматриваются вопросы хранения документов, содержащих сведения, составляющие государственную тайну.

К объектам концепции относятся преимущественно документы операционного (функционального) документооборота участников финансового рынка, а также связанные с ними организационно-распорядительные документы, применяемые для информационного взаимодействия участников финансового рынка.

2. ЮРИДИЧЕСКАЯ СИЛА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

2.1. Условия признания юридической силы электронных документов при использовании различных видов электронной подписи и технологий ее применения

Юридическая сила ЭД проистекает из содержания ЭД, его оформления (представления), способов передачи и обеспечивается, в том числе, за счет регистрации документа, использования набора реквизитов и/или совокупности доверенных сервисов (включая электронную подпись, метку времени, сервис идентификации и аутентификации), а также - организационно-правовых механизмов (в том числе лицензирование, сертификация, аудит).

В настоящее время, исходя из положений действующего законодательства, в качестве основного атрибута, обеспечивающего юридическую силу ЭД, признается ЭП установленного вида, хотя в некоторых обстоятельствах электронный документ без ЭП может быть признан в качестве документа, имеющего юридическую силу, например, по решению суда.

Однако даже усиленная квалифицированная электронная подпись (УКЭП) является необходимым, но недостаточным условием обеспечения юридической силы ЭД. Например, если установлены требования к форме и формату представления документа, срокам его представления, адресу электронной почты, с которого электронный документ должен быть отправлен, неисполнение этих требований влечет оспаривание юридической силы ЭД. Кроме того, юридическая сила ЭД может быть обеспечена и без применения электронной подписи, за счет создания доверенной среды электронного взаимодействия, требования к которой согласованы участниками такого взаимодействия.

Не исключен также вариант придания ЭД юридической силы не с помощью ЭП, а путем использования иных технологий, например, подтверждения на доверенном сайте авторизации субъекта - автора документа и целостности созданного ЭД с опорой на уже ранее выполненную операцию идентификации субъекта в иной (смежной) доверенной системе, например, платежной системе банковских карт, на портале ЕСИА или

использования технологии подтверждения авторства и целостности информации (документа) дополнительным одноразовым паролем (технология 3DSECUR). Внедрение этих технологий требует внесения изменений в федеральное законодательство, как это и было сделано на рынке страховых услуг, путем внесения изменений и дополнений в Федеральный закон от 27 ноября 1992 года № 4015-1 «Об организации страхового дела в Российской Федерации».

Учитывая условия получения и использования УКЭП, нецелесообразно устанавливать обязательные требования применения УКЭП физическими лицами при создании ими ЭД.

При дальнейшем развитии электронного документооборота на финансовом рынке необходимо:

- обеспечить развитие удостоверительных сервисов (в первую очередь, меток времени, подтверждающих время подписания документа электронной подписью);
- для целей доступа физических лиц к личным кабинетам и информационным системам субъектов финансового рынка целесообразно применять простую ЭП или авторизацию с использованием Единой системы идентификации и аутентификации;
- при использовании простой или неквалифицированной (без создания сертификата) ЭП проводить двухфакторную идентификацию подписанта.

Вопрос признания юридической силы ЭД неразрывно связан с процедурой проверки ЭП. При этом для обеспечения возможности введения ЭД в полноценный гражданско-правовой оборот, он должен быть зарегистрирован в системе учета отправленных/полученных ЭД. Результаты проверки подписи, регистрационные номера, необходимые реквизиты должны отражаться в метаданных ЭД, неразрывно связанных с самим ЭД.

Условия признания юридической силы ЭД должны закрепляться в нормативных правовых актах разного уровня. В федеральном законе целесообразно указывать документ, который должен быть представлен исключительно в электронной форме, подписывающее такой ЭД лицо, вид используемой ЭП, требования по защите конфиденциальности (при необходимости). В иных нормативных правовых актах – особенности создания ЭП (отделенная/присоединенная), кодировку или формат ЭП, формат и форму представления ЭД, формат сканирования и требования к разрешению при преобразовании документа на бумажном носителе в электронный документ, требования по аутентификации, использованию систем шифрования и другие).

При долговременном хранении юридическую силу ЭД будет обеспечивать процедура обработки ЭД для долговременного хранения, в том числе формирование файла метаданных по каждому ЭД.

2.2. Обеспечение юридической силы электронного документа при хранении в режиме оперативного доступа

Хранение ЭД, находящегося в стадии обращения, то есть в режиме оперативного доступа (оперативного хранения) осуществляется в информационной системе субъекта финансового рынка, в которой он был создан и зарегистрирован, либо в которую был включен после получения от другого субъекта финансового рынка или клиента.

При хранении ЭД в режиме оперативного доступа, в силу простоты реализации наиболее предпочтительным выглядит вариант хранения ЭД, подписанного УКЭП, что в соответствии с законодательством Российской Федерации обеспечивает его юридическую силу. При поступлении субъекту финансового рынка ЭД, имеющих ЭП иного вида, ЭД

сохраняется в том виде, в котором он поступил, а соответствующее описание ЭП отражается в его метаданных. Учитывая, что ЭД, хранящиеся в режиме оперативного доступа, в дальнейшем переводятся в иные режимы хранения, необходимо обеспечить сохранность и неизменность ЭД и его метаданных, начиная с момента его создания.

Если метаданные ЭД в режиме оперативного доступа хранятся в информационной системе субъекта финансового рынка, то при передаче ЭД на долговременное хранение, они должны быть сформированы в едином файле, структура и формат которого должны быть уставлены единообразно. Существует несколько способов обеспечения целостности метаданных ЭД, выбор которых может быть рекомендован Банком России. В период срока действия сертификата ЭП его проверка технически не представляет каких-либо затруднений.

ЭД может храниться вместе с УКЭП, при этом он сохраняет свою юридическую силу, а копии соответствующего файла, подписанного УКЭП, равнозначны оригиналу и имеют такую же юридическую силу.

2.3. Обеспечение юридической силы электронного документа в режиме долговременного хранения

Хранение ЭД в режиме долговременного хранения осуществляется в специализированной информационной системе субъекта финансового рынка, в которую была осуществлена передача ЭД из системы, обеспечивавшей его оперативное хранение.

Применительно к системам долговременного хранения, механизмы обеспечения юридической силы ЭД могут базироваться на подходе, включающем следующие процедуры:

- формирование системой-источником и передача в специализированную информационную систему архивной единицы хранения, включающей ЭД, УКЭП, метаданные;
- проверка действительности ЭП на момент подписания ЭД при принятии на хранение с фиксацией результата проверки в метаданных;
- формирование метаданных ЭД, включающих в том числе: сведения об УКЭП и сертификате ключа проверки подписи, а также иные сведения, описывающие действия, совершенные с документом в ходе его подготовки, рассмотрения, исполнения и хранения, идентификационные данные;
- обеспечение аутентичности архивной единицы хранения, включающей ЭД, УКЭП, метаданные;
- обеспечении надежного соответствия и принадлежности документа его метаданным с возможностью проверки этого соответствия и принадлежности на всем периоде хранения документа путем подписания документа и его метаданных технологической ЭП. В том числе, перед прекращением срока действия сертификата технологической ЭП должны быть сформированы метаданные о результате проверки текущей технологической ЭП. После проведения указанных процедур, документ должен быть подписан новой технологической ЭП. Образованная таким способом цепочка метаданных, подписанных технологической ЭП, обеспечивает аутентичность данных о проверке достоверности исходной ЭП документа на момент его передачи на хранение. При реализации данной технологии необходимо руководствоваться следующими требованиями и спецификациями:

  ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Процедуры проверки ЭП в части построения корректной цепочки сертификации должны соответствовать методике Test Suite – «Public Key Interoperability Test Suite (PKITS) Certification Path Validation» с учетом использования отечественных криптографических алгоритмов;

- заверение документа УКЭП (ЭП хранилища) при выдаче его по запросу после проверки цепочки метаданных и самого документа с использованием упомянутого ГОСТ.

Этот подход позволяет существенным образом упростить процедуры хранения и обслуживания массивов данных, содержащихся в электронных документах, и сосредоточить внимание на управлении метаданными ЭД, включая обеспечение их целостности.

В этом случае ЭП и иные атрибуты ЭД проверяются один раз при передаче его на долговременное хранение. При выдаче ЭД из хранилища проверяется целостность файла ЭД и его метаданных, проставляется УКЭП организации (хранилища) и необходимые реквизиты предоставляемого ЭД, что в совокупности должно придавать ЭД соответствующую юридическую силу.

Важным вопросом является простановка и проверка метки времени в метаданные документа при совершении упомянутых действий, а также технологических процедур поддержки сохранности и целостности данных. Целесообразно рассмотреть возможность простановки и проверки метки времени с использованием централизованной системы единого времени или посредством информационной системы головного удостоверяющего центра.

Порядок долговременного хранения ЭД и выдачи выписок из ЭД, находящихся на хранении у субъектов финансового рынка, должен быть определен нормативным актом Банка России в соответствии с установленными законодательством Российской Федерации полномочиями Банка России.

2.4. Юридическая сила документа при преобразовании формы его представления (из бумажной в электронную и из электронной в бумажную)

Преобразование бумажных документов в электронные осуществляется путем сканирования документа на бумажном носителе. В российском законодательстве для результата такого преобразования нередко используется термин «электронная копия документа», понимаемый как копия документа, созданная в электронной форме (например, Постановление Правительства РФ от 15.06.2009 № 477 «Об утверждении Правил делопроизводства в федеральных органах исполнительной власти»). Однако полученный в результате преобразования документ в электронной форме при соблюдении установленных условий может иметь юридическую силу оригинала.

В общем случае равная документу на бумажном носителе юридическая сила документа в электронной форме, полученного в результате преобразования, обеспечивается подписанием его ЭП лица, подписавшего документ на бумажном носителе. То есть экземпляры документа, представленные на бумажном носителе или в электронной форме, подписанные одним и тем же лицом, должны иметь равную

юридическую силу. Законодательством Российской Федерации могут быть установлены права иного лица, исполняющего полномочия подписанта, на подписание полученного в результате преобразования документа в электронной форме для обеспечения его юридической силы. При этом целесообразно устанавливать требования к формату ЭД, обеспечивающему точную визуализацию такого документа при переводе его в электронный вид. Кроме прав подписания полученного в результате преобразования ЭД должны быть установлены обязанности подписывающего лица удостовериться в тождественности содержания изготовленного ЭД содержанию документа, представленного на бумажном носителе.

Правила (требования) к обеспечению юридической силы преобразованного документа могут быть предметом законодательства Российской Федерации, регулирующего соответствующие вопросы в рамках деятельности кредитных и некредитных финансовых организаций.

Необходимо также регламентировать процедуры обеспечения юридической силы документа на бумажном носителе, полученного при преобразовании исходного ЭД. В данном случае также должен быть решен вопрос о лице, которое вправе подписывать документ на бумажном носителе, а также о метаданных ЭД, которые должны быть отражены в документе на бумажном носителе.

Преобразование ЭД в документ на бумажном носителе также не означает получение документа иной юридической силы. Юридическая сила документа, полученного в результате такого преобразования, должна быть определена законодательством в зависимости от установленных процедур преобразования (включая подписание) и реквизитов такого документа. Таким образом, необходимо установить условия, при которых документы, полученные в результате преобразования их формы, будут иметь равную (экземпляр) или более низкую юридическую силу по сравнению с преобразованным документом (копия).

При долговременном хранении ЭД, может возникнуть необходимость в получении копии или дубликата такого документа. Для таких случаев необходимо установить процедуру создания копии и процедуру создания дубликата хранимого ЭД, учитывающие как особенности удостоверения ЭД (например, наличие УКЭП или простой ЭП), так и особенности удостоверения производного документа (кто и какой ЭП вправе подписывать копию ЭД, а кто и какой ЭП – дубликат ЭД).

3. ХРАНЕНИЕ И УНИЧТОЖЕНИЕ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

3.1. Технологическое обеспечение долговременного хранения электронных документов

Документы на бумажном носителе хранятся длительное время и доступны человеку непосредственно. Поэтому базовая функция традиционного архивного хранения - обеспечение сохранности поступившего в архив физического носителя с записанным на нем документом.

Электронные же документы хранятся на носителях в специальных форматах и доступны человеку лишь при использовании специального оборудования и программных средств. Это оборудование и программные средства существенно менее устойчивы во времени. В течение нескольких лет или десятилетий происходит физическое/моральное устаревание носителей, оборудования, программных средств и связанных с ними носителей и форматов. Существенной проблемой может также оказаться недоступность

спецификаций форматов, в которых хранятся документы, и лицензионные ограничения, связанные с их использованием.

Серьезные риски потери информации, возможности ее воспроизведения и интерпретации при долговременном хранении в электронном архиве требуют комплекса технологических мероприятий, называемого электронной сохранностью (digital preservation). Подробным и общепринятым описанием концепции электронного архива с функцией обеспечения электронной сохранности является стандарт ISO 14721:2012 «Открытая архивная информационная система – Эталонная модель» (Open archival information system (OAIS) — Reference model).

Мероприятия по электронному сохранению могут включать:

1) консервация технологий;
2) эмуляция;
3) инкапсуляция;
4) миграция/конвертирование.

Наиболее распространенным в мировой практике методом обеспечения долговременной сохранности электронных документов в настоящее время является миграция, под которой, в широком смысле, понимается преобразование электронных документов и информации в новые форматы и/или перенос в новые информационные системы.

Для целей долговременного хранения предпочтительно использовать форматы архивного хранения, отвечающие следующим требованиям:

- открытость (общедоступность) спецификаций, отсутствие лицензионных ограничений при их использовании;
- независимость от аппаратно-программной среды создания документа при обеспечении сохранения содержания документа

Архивные форматы могут использоваться как непосредственно при создании и передаче в архив документов, подлежащих длительному хранению, так и в процессе архивного хранения

3.2. Нормативная, методическая и технологическая поддержка мероприятий по обеспечению долговременного хранения

В связи с динамичным развитием технологий, сложностью и спецификой задач долговременного хранения, необходимо разработать рекомендации по выбору и использованию технологических решений в сфере долговременного хранения для участников финансового рынка. Указанные рекомендации должны включать, в том числе вопросы использования архивных форматов, процедур и программных средств миграции в эти форматы. Достаточную точность миграции может обеспечить комплекс правовых, технических и организационных мер, в число которых должны входить контроль качества миграции, а также аудит и сертификация технических систем и персонала. Правовое обеспечение процедуры преобразования электронных документов в архивный формат с точки зрения сохранения его юридической силы, потребует внесения изменений в законодательство Российской Федерации.

Каждый участник финансового рынка и организации, оказывающие данным участникам услуги хранения ЭД, на основании рекомендаций регулятора вырабатывают соответствующие планы и регламенты электронного сохранения, обеспечивающие сохранность и доступность электронных документов в зависимости их форматов, сроков хранения, а также в случае наступления аварийных ситуаций и стихийных бедствий.

3.3. Особенности уничтожения электронных документов участников финансового рынка

Необходимость своевременного уничтожения ЭД вытекает из общих требований по обеспечению эффективности деловой деятельности, а также по защите прав и интересов самой организации, её контрагентов и клиентов. Ряд таких требований содержится законодательстве Российской Федерации, которые:

- определяют порядок уничтожения деловых документов с истекшими сроками хранения;

- регулируют защиту конфиденциальности информации, составляющей, в том числе, профессиональную тайну участников финансового рынка (банковскую, аудиторскую и др.);

- регламентируют вопросы обеспечения информационной безопасности организации, её сотрудников и клиентов, в том числе уничтожение информации.

В действующем законодательстве правовое регулирование процессов уничтожения документов не учитывает специфику уничтожения электронных документов.

В целом, вопрос уничтожения ЭД гораздо более сложен, чем уничтожения его бумажного аналога. Так, например, уничтожение (удаление) ЭД из одной базы данных или хранилища вовсе не означает, что будут уничтожены его экземпляры, находящиеся в других базах данных.

Уничтожение ЭД предполагает удаление файла данных, составляющих содержание ЭД, а также удаление метаданных, позволяющих восстановить юридическую силу ЭД в случае, если его копия хранится в иных базах данных.

Удаление учетных реквизитов уничтоженного ЭД их систем учета, действующих в организации или используемых в системе хранения, представляется необязательным, поскольку позволяет проследить историю ЭД, что может быть полезным в деловой деятельности.

В случае использования носителей информации с одноразовой записью данных, они подлежат физическому уничтожению.

При использовании носителей информации с возможностью многократной записи, в зависимости от степени конфиденциальности информации, могут использоваться либо штатные механизмы удаления данных, либо специальные механизмы, обеспечивающие полное уничтожение данных путем форматирования носителя или многократной перезаписи на носитель бессмысленного текста, как правило, случайной последовательности.

Любая процедура по уничтожению документов, независимо от вида носителя и формы хранения должна быть подробно регламентирована также, как регламентирована процедура уничтожения бумажных документов.

Порядок уничтожения ЭД устанавливается Банком России в соответствии с возложенными на него законодательством Российской Федерации полномочиями.

4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, СОХРАННОСТЬ И ЗАЩИТА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ НА ВСЕХ ЭТАПАХ ИХ ЖИЗНЕННОГО ЦИКЛА. ЗАЩИТА СРЕДЫ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ

Обеспечение сохранности и конфиденциальности ЭД, защита элементов среды электронного взаимодействия от НСД, компьютерных атак и воздействий вредоносного программного обеспечения в целом обеспечивается применением следующих мер защиты:

- использованием средств антивирусной защиты и систем защиты от воздействия вредоносного кода в точках соединения систем обработки, хранения и передачи сообщений (документов) с публичными сетями, контролем подозрительных активностей в информационной системе;
- контролем целостности передаваемых юридически значимых сообщений (ЭД, квитанций, подтверждений и т.д.);
- использованием механизма дополнительного подтверждения содержания сообщения (документа) отправителем при использовании простой электронной подписи;
- использованием средств защиты от несанкционированного доступа на оборудовании;
- реализацией систем управления доступом к ЭД на базе метаданных ЭД и использованием систем аутентификации субъектов доступа;
- обеспечением аутентичности ЭД и их метаданных на всем сроке хранения;
- контролем целостности информации.

Защита электронных документов в системах офисного электронного документооборота обеспечивается средствами защиты от несанкционированного доступа и антивирусной защиты. При этом эти сервисы безопасности могут быть представлены средствами системы информационной безопасности самой организации.

Целесообразно обеспечить соответствие системы хранения электронных документов требованиям по безопасности информационных систем, программно-аппаратных комплексов и программного обеспечения, установленным федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

5. ДОСТУП К ЭЛЕКТРОННЫМ ДОКУМЕНТАМ И ИХ ПРЕДОСТАВЛЕНИЕ

5.1. Принципы доступа к документам в электронной форме на финансовом рынке. Обеспечение режимов конфиденциальности электронных документов. Технологии, используемые для доступа к электронным документам

Основными принципами обеспечения доступа к информации субъектов финансового рынка являются:

1) открытость и доступность информации о деятельности субъектов финансового рынка, за исключением случаев, предусмотренных законодательством Российской Федерации;

2) достоверность информации о деятельности субъектов финансового рынка и своевременность ее предоставления;

3) обеспечение возможности доступа к документам их владельцам, законным представителям, по их поручению (разрешению) – ограниченному кругу заинтересованных лиц, а также в случаях, предусмотренных федеральными законами, определенному или неограниченному кругу заинтересованных лиц;

4) соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, защиту их чести и деловой репутации, права субъектов финансового рынка на защиту их деловой репутации при предоставлении информации об их деятельности;

5) обеспечение юридической силы документов, предоставляемых по запросу;

6) обеспечение конфиденциальности хранимых и обрабатываемых документов, предполагающей возможность их предоставления только владельцам этих документов, уполномоченным ими лицам и недоступность для иных субъектов, не имеющим на это прав.

Требования по обеспечению доступа к документам субъектов финансового рынка и правовой режим таких документов, в основном, регламентированы законодательством Российской Федерации. В частности, выделяются документы (сведения, содержащиеся в реестрах и базах данных), которые должны быть общедоступны либо ограниченно доступны в каком-либо режиме конфиденциальности. Как следует из положений части третьей статьи 55 Конституции Российской Федерации, ограничения на доступ к информации участников финансового рынка могут быть установлены федеральным законом. В настоящее время наиболее полно регламентирован режим банковской тайны. Регламентация режимов конфиденциальности сведений, составляющих профессиональную тайну участников финансового рынка, также должна быть установлена нормативными правовыми актами.

Конфиденциальность ЭД в системах их обработки, передачи и хранения обеспечивается путем использования установленных законодательством Российской Федерации технических средств защиты и применения организационных мер, поэтому не требует дополнительного нормативного регулирования. Возможна и целесообразна унификация организационных и технических мер обеспечения конфиденциальности сведений, охраняемых в режимах профессиональной тайны участников финансового рынка с учетом требований по обеспечению безопасности персональных данных при их обработке, поскольку персональные данные составляют большую часть сведений, охраняемых в режиме профессиональной тайны.

Доступ к документам их авторам, владельцам, законным представителям и заинтересованным лицам (авторизация в системе) должен быть предоставлен после проведения процедур их идентификации и аутентификации.

Аутентификация может осуществляться путем:

- предъявления субъектом полученного ранее при идентификации в системе аутентификатора (сертификата, ключа, кода, логина, пароля или их комбинации). При использовании механизмов простой ЭП для получения доступа к сайту или в личный кабинет, возможно усиление процедуры аутентификации путем предъявления субъектом дополнительного одноразового пароля;
- использования сервиса ЕСИА. При этом, идентификация субъекта осуществляется один раз при его регистрации в ЕСИА.

Для решения задачи управления доступом субъектов к документам в системе хранения, после прохождения ими процедуры аутентификации и авторизации, следует использовать информацию метаданных запрашиваемого документа, которые в конечном итоге определяют режим предоставления доступа к нему с учетом уже совершенных действий и режима хранения.

5.2. Требования к системам управления документами и другим информационным системам в части обеспечения установленного правового режима информации

Правовой режим информации определяется нормами, устанавливающими:

- порядок документирования информации,

- права на информацию и информационные системы (имущественные и интеллектуальные),
- режимы доступа к информации,
- режимы распространения (предоставления) информации,
- порядок хранения информации,
- порядок правовой защиты информации.

Система управления документами и иные информационные системы должны соответствовать нормативным требованиям, в частности, обеспечивать установленный режим конфиденциальности информации, дифференцируя субъектов доступа к такой системе, ограничивать возможность распространения информации, содержащейся в системе, а также обеспечивать необходимый уровень защиты информации.

Система управления документами должна создавать доверенную среду для выполнения основных функций работы с электронными документами/метаданными и их хранения, а также функций смешанного бумажно-электронного документооборота в соответствии с требованиями действующего законодательства Российской Федерации: импорт (прием), регистрацию, экспорт (отправку) ЭД, хранение, управление доступом, визуализацию, поиск, отчеты и анализ, поддержание деловых процессов, информационный аудит, систематизацию дел, экспертизу ценности, процедуры архивного хранения.

На техническом уровне следует выделить следующие условия:

- доступ к документам должен предоставляться только после прохождения процедуры аутентификации, позволяющей с достоверностью установить, что обращающееся лицо именно то, за кого оно себя выдает;

- документ должен предоставляться с использованием системы ~~доверенной~~ доставки сообщений, позволяющей гарантировать что:

а) документ будет доставлен адресату,

б) не будет искажен при передаче;

в) будет подтверждено, что документ получен и прочитан адресатом, а ЭП проверена и дала положительный результат.

6. ТЕРМИНЫ И СОКРАЩЕНИЯ

Аутентичный электронный документ - электронный документ, точность, надежность и целостность которого сохраняются с течением времени (ГОСТ Р 54989-2012/ISO/TR 18492:2005 «Обеспечение долговременной сохранности электронных документов»).

База данных – представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ) (пункт 2 статьи 1260 Гражданского кодекса Российской Федерации (часть четвертая)).

Документ - материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения (Федеральный закон от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов»).

Доверенная среда электронного взаимодействия – среда, создающая технологическую основу для обеспечения юридической силы ЭД.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Долговременная сохранность электронных документов - период времени, в течение которого электронные документы поддерживаются в качестве доступного и аутентичного свидетельства (доказательства). (ГОСТ Р 54989-2012/ISO/TR 18492:2005 Обеспечение долговременной сохранности электронных документов).

Долговременное хранение электронных документов - процесс обеспечения долговременной сохранности электронных документов, установленный срок хранения которых превышает срок использования программно-технических средств, применяемых для создания и поддержания этих документов.

Достоверность (электронного документа) - Свойство электронного документа, при котором содержание электронного документа является полным и точным представлением подтверждаемых операций, деятельности или фактов и которому можно доверять в последующих операциях или в последующей деятельности (ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения (утв. Приказом Росстандарта от 17.10.2013 № 1185-ст)).

ЕСИА – единая система идентификации и аутентификации - федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Инкапсуляция - сохранение описания данных в одном пакете с самими данными, что позволяет уменьшить зависимость архивных данных от аппаратно-программной среды, в которой они были созданы.

Консервация технологий - сохранение исходных или использование совместимых аппаратно-программных средств для работы с документами в ретроспективных форматах.

Метаданные - данные, описывающие контекст, содержание, структуру документов и управление ими. (ГОСТ Р ИСО 15489-1-2007. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования).

Миграция/конвертирование - перенос документов на другие носители или аппаратно-программные средства, в том числе с переформатированием.

НСД – Несанкционированный доступ.

Носитель (документированной) информации - материальный объект, предназначенный для закрепления, хранения (и воспроизведения) речевой, звуковой или изобразительной информации (ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения (утв. Приказом Росстандарта от 17.10.2013 № 1185-ст))

Пригодность для использования (электронного документа) - Свойство электронного документа, позволяющее его локализовать и воспроизвести в любой момент

времени ((ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения (утв. Приказом Росстандарта от 17.10.2013 № 1185-ст))).

ПО – Программное обеспечение.

ПЭП – Простая электронная подпись.

Реквизит документа - Элемент оформления документа (ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения (утв. Приказом Росстандарта от 17.10.2013 № 1185-ст)).

СДХ – Система доверенного хранения.

УЭП – Усиленная электронная подпись.

УКЭП– Усиленная квалифицированная электронная подпись.

УЦ – Удостоверяющий центр.

Целостность электронного документа - свойство электронного документа, при котором содержание электронного документа является полным и точным представлением подтверждаемых операций, деятельности или фактов и которому можно доверять в последующих операциях или в последующей деятельности (Приказ Минкомсвязи РФ от 02.09.2011 № 221 «Об утверждении Требований к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающих в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения».)

Электронный документ (ЭД) – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Эмуляция - программное воспроизведение функциональности морально устаревшей системы для обеспечения работы с устаревшими форматами данных.

ЭП – Электронная подпись.

Юридическая сила электронного документа - возможность использовать электронный документ по назначению и в качестве прямых доказательств в судебных спорах и разбирательствах.