



носителе, заверенному подписью (подписью и печатью) составителя такого документа.

При этом в государствах-членах в соответствии с их законодательством обеспечение юридической силы электронных документов и организация защищенного документооборота построены на гарантиях их подлинности и целостности посредством применения национальных криптографических методов и средств.

Государства-члены используют национальные стандарты криптографических алгоритмов создания и проверки ЭЦП. Применяемые органами государственной власти государств-членов способы реализации криптографических алгоритмов между собой несовместимы, что обусловлено различными подходами к обеспечению информационной безопасности.

Применение единых криптографических средств ЭЦП при трансграничном электронном обмене данными между органами государственной власти государств-членов в настоящее время невозможно, поскольку в соответствии с нормативно-правовой базой государств-членов к использованию в государствах-членах допускаются только сертифицированные по национальным стандартам криптографические средства.

Решение задач надежной и эффективной интеграции территориально распределенных государственных информационных ресурсов и информационных систем органов государств-членов, обеспечения взаимодействия органов власти государств-членов в электронном виде, в том числе предоставление возможности обмена электронными документами, имеющими юридическую силу (или взаимно признаваемыми таковыми), является одним из ключевых направлений работ по созданию и внедрению интегрированной информационной системы Евразийского экономического союза (далее – интегрированная система).

Обеспечение трансграничного обмена имеющими юридическую силу электронными документами в интегрированной системе реализуется на основе применения создаваемой службы доверенной третьей стороны, основными задачами которой являются:

осуществление легализации (подтверждение подлинности) электронных документов и ЭЦП субъектов информационного взаимодействия в фиксированный момент времени;

обеспечение проверки ЭЦП отправителя, созданной в соответствии с законодательством государства-члена, в юрисдикции которого находится этот отправитель;

обеспечение гарантий доверия в международном (трансграничном) обмене электронными документами;

обеспечение правомерности применения ЭЦП в исходящих и (или) входящих электронных документах в соответствии с законодательством государств-членов и актами Евразийской экономической комиссии (далее – Комиссия).

Применение технологии ЭЦП на основе инфраструктуры открытых ключей позволит обеспечить надежную идентификацию отправителей электронных документов как подтверждение их волеизъявления и правомочности, а также неотказуемость авторства и контроль целостности передаваемых электронных документов.

## II. Определения

Для целей настоящей Концепции используются понятия, которые означают следующие :

«доверенная третья сторона» – организация, наделенная в соответствии с законодательством государств-членов правом осуществлять деятельность по проверке ЭЦП в электронных документах в фиксированный момент времени в отношении лица, подписавшего электронный документ;

«интеграционный шлюз» – программно-аппаратный комплекс, обеспечивающий взаимодействие межгосударственных и межведомственных информационных систем государств-членов и Комиссии при обмене данными;

«общая инфраструктура документирования информации в электронном виде» – совокупность информационно-технологических и организационно-правовых мероприятий, правил и решений, реализуемых в целях придания юридической силы электронным документам, используемым в рамках Союза;

«служба доверенной третьей стороны интегрированной системы» – совокупность сервисов доверенной третьей стороны государств-членов и Комиссии, обеспечивающих единое трансграничное пространство доверия ЭЦП при электронной форме взаимодействия субъектов средствами интегрированной системы;

«трансграничное пространство доверия» – совокупность правовых, организационных и технических условий, согласованных государствами-членами с целью обеспечения доверия при межгосударственном обмене данными и электронными документами между уполномоченными органами;

«электронная форма взаимодействия» – способ информационного взаимодействия, основанный на применении информационно-коммуникационных технологий;

«электронный вид документа» – информация, сведения, данные, представленные в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи и обработки с использованием информационно-коммуникационных технологий, с соблюдением установленных требований к формату и структуре;

«электронный документ» – документ в электронном виде, заверенный ЭЦП и отвечающий требованиям общей инфраструктуры документирования информации в электронном виде ;

«юридическая значимость электронного документа» – свойство электронного документа, позволяющее воспринимать содержание данного документа как подлинное;

«юридическая сила электронного документа» – свойство защищенного электронного документа, формы представления и оборота которого (его подлинность и целостность) подтверждены доверенной третьей стороной и которое при осуществлении международного (трансграничного) обмена электронными документами предоставляет возможность использовать электронные документы по н а з н а ч е н и ю и в качестве прямых доказательств в судебных спорах и разбирательствах.

### III. Цели и область применения Концепции

Настоящая Концепция определяет общие подходы к организации процесса обеспечения юридически значимого взаимодействия в рамках Союза при трансграничном электронном взаимодействии в интегрированной системе.

Обеспечение юридически значимого взаимодействия в рамках Союза в соответствии с настоящей Концепцией является необходимым условием обеспечения юридической силы электронных документов, передаваемых в рамках интегрированной с и с т е м ы .

Настоящая Концепция разработана в соответствии с пунктом 13 Протокола об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза (приложение № 3 к Договору о Евразийском экономическом союзе от 29 мая 2014 года) с учетом мирового опыта и имеющейся практики обеспечения юридической силы электронных документов при трансграничном электронном взаимодействии на основе доверенных сервисов в соответствии с международными рекомендациями ITU-T серии X.842 комитета по стандартизации электросвязи Международного союза электросвязи.

Целями настоящей Концепции являются определение принципов реализации в интегрированной системе юридически значимого взаимодействия в рамках Союза и установление порядка признания юридического значения электронных документов с использованием необходимых организационных, технических и правовых подходов.

Положения, определенные настоящей Концепцией, могут быть использованы при разработке актов органов Союза и государств-членов по вопросам реализации межгосударственного информационного обмена электронными документами между уполномоченными органами государств-членов (уполномоченными органами государств-членов и Комиссией) (далее – участники информационного обмена), в том числе при официальном подтверждении в государствах-членах или Комиссии юридической силы электронных документов, сформированных во всех государствах-членах или Комиссии с использованием средств интегрированной с и с т е м ы .

Установление и применение условий признания юридической силы электронных документов и доверия к ЭЦП на электронных документах, сформированных в установленном порядке уполномоченными органами одного государства-члена при

обмене с уполномоченными органами другого государства-члена с использованием средств интегрированной системы, не зависят от выбора формы и форматов представления и оборота электронных документов и их ЭЦП, применяемых в информационных системах государств-членов.

Принципы настоящей Концепции могут быть применимы при расширении состава участников информационного обмена, в том числе при реализации межгосударственного информационного обмена электронными документами между субъектами предпринимательской деятельности, некоммерческими организациями и физическими лицами государств-членов.

Принципы, связанные с расширением области применения настоящей Концепции, должны быть определены в стратегии развития трансграничного пространства доверия.

#### IV. Обоснование подхода к обеспечению юридической силы передаваемых документов в рамках электронной формы взаимодействия

##### 1. Юридическая сила и юридическая значимость

Юридическая сила электронного документа обеспечивается на основании законодательства государств-членов с учетом содержания данного документа, а также системы отношений, в рамках которой соответствующий документ был передан от одного лица другому.

Юридическая значимость электронных и бумажных документов заключается в способности изменять правовой статус субъектов права, в том числе находящихся в различных юрисдикциях.

Юридическая значимость проистекает из содержания электронных и бумажных документов и обеспечивается в том числе за счет использования набора реквизитов для бумажных документов или совокупности доверенных информационно-безопасных сервисов (в том числе ЭЦП, метки времени, сервиса идентификации и аутентификации) и организационно-правовых механизмов (в том числе лицензирование, сертификация, аудит) для электронных документов.

Необходимый и достаточный набор доверенных сервисов и организационно-правовых механизмов, обеспечивающих юридическую значимость электронных документов с учетом поэтапного внедрения информационно-безопасных инфраструктур, определяется владельцем информационной системы или соглашением между владельцами взаимодействующих информационных систем.

Таким образом, обеспечение в рамках интегрированной системы юридически значимого взаимодействия обеспечивает юридическую силу электронных документов, передаваемых в процессе взаимодействия.

Поскольку при трансграничном обмене проверка в государстве-члене ЭЦП, созданной в соответствии с законодательством другого государства, технологически невозможна в юрисдикции получателя (в силу несовместимости национальных криптографических алгоритмов), однако допускается юридически. Способом

обеспечения такой проверки является использование сервиса доверенной третьей стороны .

Положения, определяющие создание комплексных механизмов, направленных на обеспечение юридической значимости электронных документов в рамках трансграничного электронного документооборота, закрепляются в стратегии развития трансграничного пространства доверия.

## 2. Доверенная третья сторона

Доверенные третьи стороны организуются на уровне каждого государства-члена, а также в Комиссии. С технической точки зрения взаимосвязанная инфраструктура доверенных третьих сторон (программно-аппаратные комплексы) должна быть размещена во всех национальных сегментах и интеграционном сегменте интегрированной системы. Территориальное размещение комплексов доверенных третьих сторон необходимо с точки зрения обеспечения соответствия законодательным ограничениям на экспорт криптографических технологий в каждом из государств - членов .

Доверенные третьи стороны оказывают участникам межгосударственного информационного обмена услуги по проверке ЭЦП отправителя в криптографическом стандарте юрисдикции отправителя с подписанием квитанции как результата такой проверки. Электронный документ с результатом положительной проверки доверенной третьей стороной признается в юрисдикции получателя равнозначным электронному документу, подписанному собственной ЭЦП отправителя на основе нормы о признании ЭЦП, выданной в соответствии с законодательством другого государства.

При построении службы доверенной третьей стороны интегрированной системы необходимо создание юридических условий и договорных связей, соответствующих законодательству государств-членов (в части признания ЭЦП, созданной в другом государстве) , а также функциональным особенностям интегрированной системы и порядку предполагаемого взаимодействия .

Создание системы юридических условий и договорных связей предполагает разработку и принятие нормативных актов и договоров между участниками информационного обмена.

## V. Обеспечение юридической значимости при трансграничном обмене электронными документами в интегрированной системе

### 1. Общие принципы организации взаимодействия участников информационного обмена

Взаимодействие в электронном виде между участниками информационного обмена в интегрированной системе обеспечивается за счет создания и использования интеграционного сегмента Комиссии и национальных сегментов, представляющих собой совокупность защищенной системы передачи данных и интеграционных шлюзов

, входящих в состав каждого узла участников информационного обмена.

В составе интеграционного и национальных сегментов интегрированной системы должен функционировать свой программно-аппаратный комплекс доверенной третьей стороны. Программно-аппаратные комплексы доверенных третьих сторон разрабатываются в рамках работ по созданию интеграционного и национальных сегментов интегрированной системы. Обращение к сервисам конкретной доверенной третьей стороны интегрированной системы осуществляется посредством использования соответствующих интеграционных шлюзов.

Программно-аппаратные комплексы доверенных третьих сторон, входящие в состав национальных сегментов, могут также использоваться для решения задач по обеспечению юридической значимости электронных документов, не относящихся к процессам информационного взаимодействия в рамках интегрированной системы.

Процесс обеспечения юридической значимости при трансграничном обмене электронными документами в интегрированной системе базируется на следующих принципах:

признание ЭЦП обеспечивается посредством взаимодействия доверенных третьих сторон государств-членов и Комиссии, предоставляющих участникам информационного обмена услуги по проверке ЭЦП на соответствие установленным требованиям и заверению их электронных документов и ЭЦП путем формирования и проставления доверенной третьей стороной своей ЭЦП с проставлением метки времени совершения операции;

отправители (получатели) (пользователи ведомственных информационных систем государств-членов) при подписании и проверке ЭЦП используют криптографические стандарты, предусмотренные законодательством соответствующего государства-члена. Для применения пользователями информационных систем Комиссии используются криптографические стандарты, утверждаемые Комиссией;

при взаимодействии между отправителями (получателями) и доверенной третьей стороной, находящимися в одном сегменте государства-члена, используются криптографические стандарты соответствующего государства-члена;

при взаимодействии между отправителями (получателями) и сервисами доверенной третьей стороны, находящимися в интеграционном сегменте Комиссии, используется криптографический стандарт, утверждаемый для этих целей Комиссией;

при взаимодействии сервисов службы доверенной третьей стороны между собой используются согласованный криптографический стандарт ЭЦП и согласованный криптографический стандарт функции хэширования (стандарт службы доверенной третьей стороны), утверждаемые для этих целей Комиссией.

## 2. Признание юридической силы электронных документов

Юридическая сила электронных документов при трансграничном обмене основывается на применении в юрисдикции участника информационного обмена

сервисов уполномоченной доверенной третьей стороны (сервисы которой входят в состав службы доверенной третьей стороны интегрированной системы), оказывающей участникам межгосударственного информационного обмена (отправителям и получателям) услуги по заверению или удостоверению их электронной корреспонденции (исходящих или входящих электронных документов) путем проставления ЭЦП доверенной третьей стороной (в стандарте службы доверенной третьей стороны и криптографическом стандарте юрисдикции получателя соответственно) с независимой от отправителя и получателя меткой (штампом) даты и времени. Обязательным условием предоставления указанной услуги является положительный результат проверки программно-аппаратным комплексом доверенной третьей стороны национальной ЭЦП отправителя или ЭЦП доверенной третьей стороны юрисдикции отправителя на электронной корреспонденции.

Удостоверенный в установленном порядке электронный документ признается в юрисдикции уполномоченной доверенной третьей стороны получателя равнозначным электронному документу, подписанному собственной ЭЦП отправителя.

Уполномоченные доверенные третьи стороны должны признавать юридическую силу электронных документов, исходящих от отправителей, находящихся в юрисдикции государства другой уполномоченной доверенной третьей стороны, если электронные документы подписаны (заверены) ЭЦП другой доверенной третьей стороной, находящейся в юрисдикции государства отправителя.

### 3. Общие требования к электронному документу

Для целей реализации настоящей Концепции должны применяться утверждаемые решением Коллегии Комиссии структура и правила формирования электронных документов и иных электронных сообщений, используемые для обмена информацией в рамках интегрированной системы.

В случае если в соответствии с законодательством требуется, чтобы документ или сведения были представлены в письменной форме, или предусматривается наступление определенных юридических последствий в случае несоблюдения письменной формы, это требование считается выполненным путем представления электронного документа, если этот электронный документ оформлен, подписан и защищен (с учетом проверки подписи) в соответствии с принципами взаимодействия участников информационного обмена в интегрированной системе, установленными с учетом положений настоящей Концепции, а содержащаяся в нем информация является доступной для ее раскрытия и последующего использования.

Критерием оценки целостности и подлинности электронного документа является положительная проверка ЭЦП, гарантирующая сохранение документированной информации в полном и неизменном виде.

Подписание электронного документа ЭЦП подтверждает его целостность и подлинность.



В случае если в соответствии с законодательством или соответствующим соглашением государств-членов требуется обеспечить конфиденциальность документа, информация, содержащаяся в электронном документе, может быть зашифрована (преобразована с использованием средств криптографической защиты информации). Порядок применения средств криптографической защиты информации в таких случаях устанавливается международными договорами в рамках Союза.

#### 4. Взаимодействие доверенных третьих сторон интегрированной системы

Для целей подписания передаваемых электронных документов отправители подписывают документ ЭЦП, сертификат ключа проверки которой выдан удостоверяющим центром своей юрисдикции. Дальнейшая проверка ЭЦП отправителя осуществляется в порядке взаимодействия доверенной третьей стороны национального сегмента отправителя и удостоверяющего центра отправителя по криптографическим алгоритмам государства отправителя.

Результат проверки ЭЦП отправителя оформляется в виде квитанции доверенной третьей стороны национального сегмента, подписанной ЭЦП по стандарту службы доверенной третьей стороны.

Доверенная третья сторона национального сегмента получателя по факту получения электронного сообщения проверяет ЭЦП квитанции доверенной третьей стороны национального сегмента отправителя (по криптографическому стандарту службы доверенной третьей стороны) и на основании положительной проверки ЭЦП формирует результат проверки в виде квитанции, подписанной по криптографическому алгоритму и при помощи сертификата ключей подписи удостоверяющего центра страны получателя.

Получатель проверяет ЭЦП доверенной третьей стороны своего национального сегмента в установленном порядке.

Реализация системы запросов к доверенной третьей стороне осуществляется интеграционными шлюзами интегрированной системы.

ЭЦП квитанций результатов проверок доверенной третьей стороной каждого сегмента удостоверяют юридическую значимость электронного документа на каждом этапе информационного обмена.

Орган или юридическое лицо, реализующие услуги доверенной третьей стороны, при исполнении процедур проверки ЭЦП действуют в соответствии с правилами, установленными в интегрированной системе.

Деятельность всех доверенных третьих сторон в интегрированной системе должна быть синхронизирована и урегулирована на нормативном и договорном уровнях. Взаимодействие доверенных третьих сторон, создающих условия для признания юридической значимости полученного электронного документа, обеспечивает создание ядра трансграничного пространства доверия.

## 5. Время отправления и получения электронных документов в интегрированной системе

Временем отправления электронного документа в интегрированную систему, равно как и подтверждения подлинности электронного документа, является момент, когда доверенная третья сторона национального сегмента отправителя осуществила проверку ЭЦП отправителя и подписала соответствующую квитанцию своей ЭЦП.

Временем получения в интегрированной системе и подтверждения подлинности электронного документа является момент, когда уполномоченная доверенная третья сторона национального сегмента получателя осуществила проверку ЭЦП доверенной третьей стороны национального сегмента отправителя и подписала соответствующую к в и т а н ц и ю с в о е й Э Ц П .

Единый источник точного времени, используемый для определения времени в сервисах доверенных третьих сторон, согласовывается уполномоченными органами государств-членов.

## 6. Деятельность службы доверенной третьей стороны интегрированной системы

Деятельность службы доверенной третьей стороны интегрированной системы осуществляется в соответствии с требованиями законодательства государств-членов, Договора о Евразийском экономическом союзе от 29 мая 2014 года, настоящей Концепции, а также нормативно-технических документов, которые могут разрабатываться Комиссией при взаимодействии с уполномоченными органами государств-членов и в которых определяется порядок технического (технологического) сопряжения уполномоченных доверенных третьих сторон.

Уполномоченные органы государств-членов и Комиссия определяют и назначают в установленном порядке уполномоченных операторов доверенных третьих сторон интеграционного и национальных сегментов интегрированной системы. Взаимодействие операторов доверенных третьих сторон между собой (в том числе права, обязанности и ответственность), согласование порядка архивирования и депозитарного хранения контрольных сведений о работе доверенной третьей стороны могут осуществляться в соответствии с заключаемым безвозмездным договором между н и м и .

Доверенные третьи стороны интегрированной системы руководствуются законодательством государств-членов в сфере применения, обмена и использования электронных документов и их ЭЦП, настоящей Концепцией и положением о доверенной третьей стороне, утверждаемым учредителем этой уполномоченной доверенной третьей стороны .

Требования к развитию и функционированию трансграничного пространства

доверия, в том числе к операторам доверенных третьих сторон интеграционного и национальных сегментов интегрированной системы, разрабатываются Комиссией во взаимодействии с уполномоченными органами государств-членов.

#### 7. Легитимность услуг доверенной третьей стороны

Легитимность услуг уполномоченных доверенных третьих сторон при межгосударственном информационном обмене в рамках функционирования интегрированной системы обеспечивается:

государственными полномочиями и контролем ведения деятельности и исполнения функций службы доверенной третьей стороны интегрированной системы со стороны Комиссии и уполномоченных органов государств-членов;

обеспечением конфиденциальности передаваемых электронных документов;

применением сертифицированных в соответствии с законодательством государств-членов программно-аппаратных средств и способов защиты;

комплексом технических, организационных и правовых мероприятий и процедур ( п о л и т и к ) ;

договорными обязательствами и ответственностью всех участников в обеспечении межгосударственного информационного взаимодействия;

управлением доступа к реестрам, базам данных, депозитариям, архивным документам, содержащим историю оказанных услуг по обработке электронных документов.

#### 8. Функции службы доверенной третьей стороны

Для обеспечения гарантий доверия и правомерности применения электронных документов при межгосударственном взаимодействии участников информационного обмена доверенные третьи стороны (интеграционного сегмента и национальных сегментов) интегрированной системы должны обеспечивать выполнение следующих основных функций службы доверенной третьей стороны:

заверение и (или) удостоверение исходящих и (или) входящих электронных документов и Э Ц П ;

проверка подлинности и целостности электронных документов и ЭЦП на соответствие требованиям законодательства государства нахождения уполномоченной доверенной третьей стороны и стандарта службы доверенной третьей стороны ;

исполнение иных действий, необходимых для поддержания деятельности службы доверенной третьей стороны интегрированной системы.

### VI. Реализация Концепции

#### 1. Правовые основы реализации Концепции

В целях реализации настоящей Концепции должны быть разработаны и приняты соответствующие документы, направленные на унификацию правовых требований к операторам доверенных третьих сторон и порядку их деятельности, которые в

дальнейшем могут быть рекомендованы к имплементации в законодательство государств-членов. В состав таких документов могут входить:

- межправительственное соглашение о трансграничном электронном взаимодействии государств-членов и Комиссии;
- модельный кодекс института международного электронного нотариата на основе сервисов и служб доверенных третьих сторон государств-членов;
- положение о правовом статусе доверенной третьей стороны Комиссии;
- регламент доверенной третьей стороны Комиссии;
- положение об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств-членов между собой и с Комиссией.

В целях обеспечения функционирования службы доверенной третьей стороны интегрированной системы Комиссией принимаются нормативно-технические документы, определяющие технологию, регламенты, форматы и структуры данных, необходимые для реализации трансграничной передачи электронных документов с обеспечением их юридической значимости между информационными системами государств-членов.

## 2. Электронный реестр

Доверенные третьи стороны интегрированной системы ведут и поддерживают в актуальном и безопасном состоянии электронный реестр (базу данных), в котором регистрируется каждый факт заверения (удостоверения) электронного документа и формирования ЭЦП.

## 3. Удостоверяющие центры

В Комиссии создаются удостоверяющий центр для обеспечения сертификатами ключей подписи для взаимодействия уполномоченных доверенных третьих сторон интеграционного и национальных сегментов интегрированной системы и удостоверяющий центр для обеспечения сертификатами ключей подписи членов Коллегии Комиссии и сотрудников Комиссии.

Обеспечение доверенной третьей стороны национальных сегментов сертификатами ключей подписи удостоверяющего центра Комиссии позволит сформировать единую сеть признания сертификатов ЭЦП доверенной третьей стороны на трансграничном уровне на основе единых стандартов сертифицированных криптографических алгоритмов, протоколов и форматов, что в том числе обеспечит повышение уровня информационной безопасности в сфере административных правоотношений между уполномоченными органами государств-членов и Комиссии за счет явного ограничения действий с применением ключа ЭЦП (через атрибуты выдаваемых сертификатов) и единой системы учета отозванных сертификатов, а также позволит сократить затраты на модернизацию интегрированной системы при присоединении к Союзу новых членов.

Удостоверяющие центры создаются на основе Инфраструктуры открытых ключей (Public Key Infrastructure) в соответствии с рекомендациями X.509 Public Key Infrastructure.

Необходимые для функционирования удостоверяющих центров документы утверждаются Комиссией.

#### 4. Средства криптографической поддержки

Для использования в целях, определенных настоящей Концепцией, в части взаимодействия уполномоченных доверенных третьих сторон между собой применяются криптографические стандарты, утверждаемые Комиссией.

Для обеспечения деятельности Комиссии и функционирования удостоверяющего центра Комиссии применяются криптографические стандарты, утверждаемые Комиссией.

#### VII. Заключительные положения

От реализации принципов и подходов, содержащихся в настоящей Концепции, ожидаются следующие результаты:

- совершенствование права Союза;
- минимизация рисков оспаривания электронных документов, передаваемых в рамках интегрированной системы;
- создание инфраструктуры для реализации юридически значимого электронного взаимодействия на основе использования международных стандартов и современных информационных технологий.