

# **СРАВНИТЕЛЬНЫЙ АНАЛИЗ ДЕЙСТВУЮЩИХ В РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКЕ БЕЛАРУСЬ НОРМАТИВНЫХ ПРАВОВЫХ ТРЕБОВАНИЙ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП И ИОК**

**Комисаренко В.В.**

**начальник сектора Государственной системы управления  
открытыми ключами Республики Беларусь  
РУП «Национальный центр электронных услуг»**



**Закон Российской Федерации «Об электронной цифровой подписи» № 1-ФЗ от 10.01.2002 г. (в ред. Федерального закона от 08.11.2007 N 258-ФЗ)**



**Закон Российской Федерации «Об электронной подписи» №63-ФЗ**

**Закон Республики Беларусь от 28 декабря 2009 г. №113-з «Об электронном документе и электронной цифровой подписи»**



## ПУТИ РЕШЕНИЯ



### Унификация

- Взаимное признание стандартов (унификация требований)
- Признание сертификатов на средства ЭЦП
- Сближение законодательства (заключение отдельного межгосударственного договора)

### ДТС

- Создание ДТС
- Опытная эксплуатация
- Ввод в действие
- Подключение информационных систем

### Частные решения

- Решение проблемы ввоза-вывоза СКЗИ
- Заключение соглашений (договоров) между организациями



## ПУТИ РЕШЕНИЯ



### Унификация

- Наиболее правильный
- Наиболее долгий
- В настоящий момент не начат

### ДТС

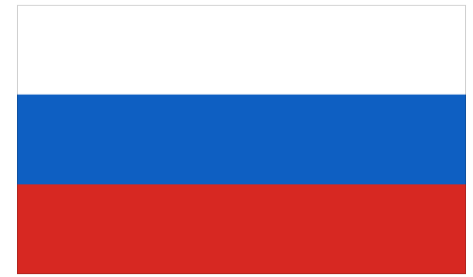
- Наиболее простой
- Не требует существенных изменений нормативной и правовой базы
- Требуется инвестиций на старте

### Частные (временные) решения

- Достаточно простой и понятный
- Имеет юридические проблемы



**Подлинный электронный документ** – электронный документ, целостность и подлинность которого подтверждаются *с применением сертифицированного средства* электронной цифровой подписи, использующего при проверке электронной цифровой подписи открытые ключи лица (лиц), подписавшего (подписавших) электронный документ



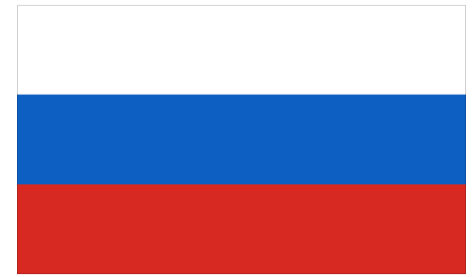
**Квалифицированной электронной подписью** является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:  
1) ключ проверки электронной подписи указан в квалифицированном сертификате;  
2) для создания и проверки электронной подписи используются средства электронной подписи, получившие *подтверждение соответствия требованиям*, установленным в соответствии с настоящим Федеральным законом.



**Статья 3. Законодательство**  
**Республики Беларусь об**

**электронных документах и  
электронной цифровой подписи**

**Если международным договором  
Республики Беларусь установлены  
иные правила, чем те, которые  
содержатся в настоящем Законе, то  
применяются правила  
международного договора**



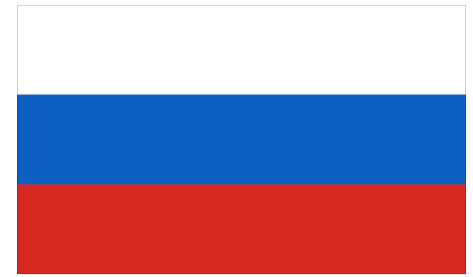
**Статья 7. Признание электронных подписей,**  
**созданных в соответствии с нормами  
иностранного права и международными  
стандартами**

- 1. Электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, в Российской Федерации признаются электронными подписями того вида, признакам которого они соответствуют на основании настоящего Федерального закона.**
- 2. Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки электронной подписи выдан в соответствии с нормами иностранного права**



### **Статья 30. Признание иностранного сертификата открытого ключа**

**Иностранный сертификат открытого ключа, соответствующий требованиям законодательства иностранного государства, в котором этот сертификат издан, признается на территории РБ в случаях и порядке, определенных международным договором РБ, предусматривающим взаимное признание сертификатов открытых ключей или другой способ придания юридической силы иностранным электронным документам.**

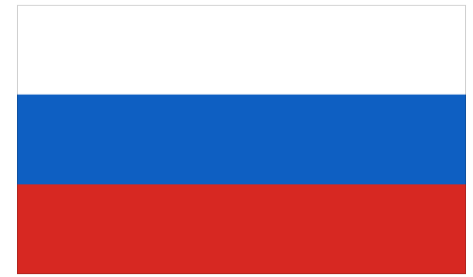


### **Статья 7. Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами**

- 1. Электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, в Российской Федерации признаются электронными подписями того вида, признакам которого они соответствуют на основании настоящего Федерального закона.**
- 2. Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки электронной подписи выдан в соответствии с нормами иностранного права**



**Статья 30. Признание иностранного сертификата открытого ключа**  
**Сертификат открытого ключа, изданный поставщиком услуг иностранного государства, аккредитованным в Государственной системе управления открытыми ключами, признается на территории Республики Беларусь.**



**Статья 7. Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами**

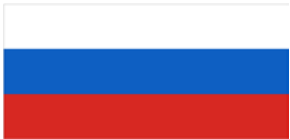
- 1. Электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, в Российской Федерации признаются электронными подписями того вида, признакам которого они соответствуют на основании настоящего Федерального закона.**
- 2. Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки электронной подписи выдан в соответствии с нормами иностранного права**





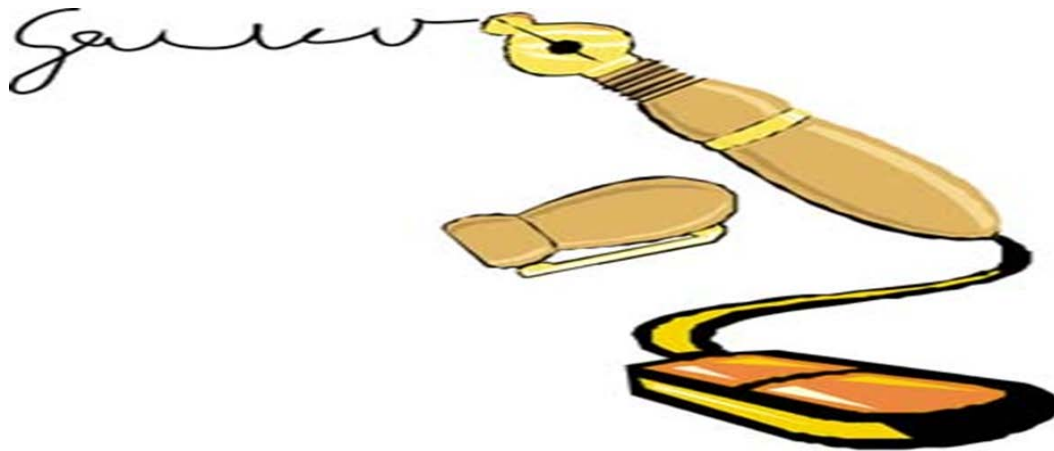
## НОРМАТИВНАЯ БАЗА РЕСПУБЛИКИ БЕЛАРУСЬ

- СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи»
- СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования»
- СТБ П 34.101.45-2011 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи на основе эллиптических кривых»
- СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»
- СТБ 34.101.47-2012 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»
- СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации» или СТБ П 34.101.43-2009 «Информационные технологии. Методы и средства безопасности. Профиль защиты технических и аппаратно-программных средств криптографической защиты информации»
- СТБ 34.101.18-2009 «Информационные технологии. Синтаксис обмена персональной информацией» с учетом использования СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.31-2011
- СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»
- СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»



## НОРМАТИВНАЯ БАЗА РОССИЙСКОЙ ФЕДЕРАЦИИ

- Федеральная служба безопасности Российской Федерации. Приказ от 27 декабря 2011 года №796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра»
- ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»
- ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»

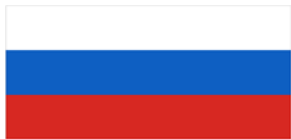




# НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



<b>Российская Федерация</b>	<b>Республика Беларусь</b>
<p>Приказ ФСБ РФ от 27 декабря 2011 г. №796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»</p>	<p>Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 25 мая 2012 г. №46 «О некоторых мерах по реализации Указа Президента Республики Беларусь от 8 ноября 2011 г. № 515».</p> <p>Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 16 октября 2012 г. №79 «О некоторых вопросах функционирования Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь»</p>



# СТАНДАРТЫ, СВЯЗАННЫЕ С ТЕХНОЛОГИЙ ЭЦП



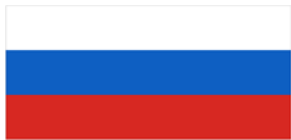
<b>Российская Федерация</b>	<b>Республика Беларусь</b>
ГОСТ Р 34.10-2012 ГОСТ Р 34.10-2001 ГОСТ Р 34.11-2012 ГОСТ Р 34.11-94	СТБ 1176.2-99, СТБ 1176.1-99, СТБ 34.101.17-2012, СТБ 34.101.18-2009, СТБ 34.101.19-2012, СТБ 34.101.21 – 2009, СТБ 34.101.23-2012, СТБ 34.101.26-2012, СТБ 34.101.27-2011, СТБ 34.101.31-2011, СТБ П 34.101.43-2009, СТБ П 34.101.44-2011, СТБ П 34.101.45-2011, СТБ 34.101.47-2012, СТБ 34.101.49-2012



# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



Термин	Российская Федерация	Республика Беларусь
<b>Электронная подпись, электронная цифровая подпись</b>	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию	Последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности



# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



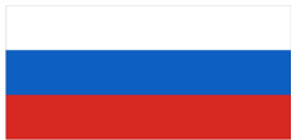
<b>Термин</b>	<b>Российская Федерация</b>	<b>Республика Беларусь</b>
<b>Сертификат ключа проверки электронной подписи, сертификат открытого ключа</b>	Электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом УЦ и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи	Электронный документ, изданный поставщиком услуг и содержащий информацию, подтверждающую принадлежность указанного в нем открытого ключа определенным организации или физическому лицу, и иную информацию, предусмотренную настоящим Законом и иными актами законодательства Республики Беларусь



# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



<b>Термин</b>	<b>Российская Федерация</b>	<b>Республика Беларусь</b>
<b>Квалифици- рованный сертификат ключа проверки электронной подписи (квалифици- рованный сертификат)</b>	Сертификат ключа проверки электронной подписи, выданный аккредитованным УЦ или доверенным лицом аккредитованного УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи	-



# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



Термин	Российская Федерация	Республика Беларусь
<b>Владелец сертификата ключа проверки электронной подписи</b>	Лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи	-





# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



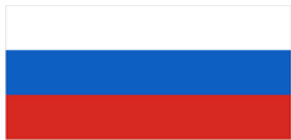
<b>Термин</b>	<b>Российская Федерация</b>	<b>Республика Беларусь</b>
<b>Ключ электронной подписи, личный ключ электронной цифровой подписи</b>	Уникальная последовательность символов, предназначенная для создания электронной подписи	Последовательность символов, принадлежащая определенным организации или физическому лицу и используемая при выработке электронной цифровой подписи



# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



<b>Термин</b>	<b>Российская Федерация</b>	<b>Республика Беларусь</b>
<b>Ключ проверки электронной подписи, открытый ключ проверки электронной цифровой подписи</b>	Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи	Последовательность символов, соответствующая определенному личному ключу, доступная для всех заинтересованных организаций или физических лиц и применяемая при проверке электронной цифровой подписи



# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



Термин	Российская Федерация	Республика Беларусь
<b>Удостоверяющий центр, организация, оказывающая услуги по распространению открытых ключей (поставщик услуг)</b>	Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом	Организация, выполняющая одну или несколько из следующих функций: достоверное подтверждение принадлежности открытого ключа определенным организации или физическому лицу, издание, распространение, хранение сертификатов открытых ключей и списков отозванных сертификатов открытых ключей



# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



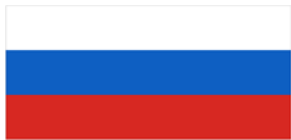
Термин	Российская Федерация	Республика Беларусь
<b>Аккредитация УЦ</b>	Признание уполномоченным федеральным органом соответствия УЦ требованиям настоящего Федерального закона	<p>Аккредитацию поставщиков услуг в Государственной системе управления открытыми ключами и контроль за соблюдением условий аккредитации осуществляет Национальный банк Республики Беларусь.</p> <p>Условия аккредитации поставщиков услуг в Государственной системе управления открытыми ключами, порядок проведения аккредитации и осуществления контроля за соблюдением ее условий устанавливаются Национальным банком Республики Беларусь</p>



# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



<b>Термин</b>	<b>Российская Федерация</b>	<b>Республика Беларусь</b>
<b>Средства электронной подписи, средство электронной цифровой подписи</b>	Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи	Программное, программно-техническое или техническое средство, с помощью которого реализуются одна или несколько из следующих функций: выработка электронной цифровой подписи, проверка электронной цифровой подписи, выработка личного ключа или открытого ключа



# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



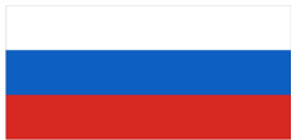
<b>Термин</b>	<b>Российская Федерация</b>	<b>Республика Беларусь</b>
<b>Средства УЦ</b>	Программные и (или) аппаратные средства, используемые для реализации функций УЦ	-



# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



Термин	Российская Федерация	Республика Беларусь
<b>Карточка открытого ключа проверки электронной цифровой подписи</b>	-	Документ на бумажном носителе, содержащий значение открытого ключа проверки электронной цифровой подписи (далее – открытый ключ), информацию, подтверждающую его принадлежность определенным организации или гражданину, в том числе индивидуальному предпринимателю (далее – физическое лицо), а также содержащий иную информацию, предусмотренную настоящим Законом и иными актами законодательства Республики Беларусь

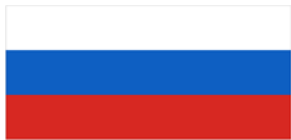


# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



<b>Термин</b>	<b>Российская Федерация</b>	<b>Республика Беларусь</b>
<b>Отзыв открытого ключа</b>	-	Процедура, закрывающаяся в досрочном прекращении действия открытого ключа

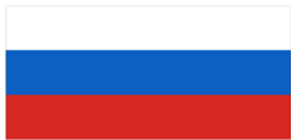




# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



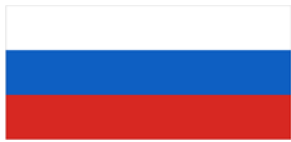
<b>Термин</b>	<b>Российская Федерация</b>	<b>Республика Беларусь</b>
<b>Подлинность электронного документа</b>	-	Свойство электронного документа, определяющее, что электронный документ подписан действительной электронной цифровой подписью (электронными цифровыми подписями)



# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СФЕРЕ ТЕХНОЛОГИИ ЭЦП



Термин	Российская Федерация	Республика Беларусь
<b>Подлинный электронный документ</b>	-	Электронный документ, целостность и подлинность которого подтверждаются с применением сертифицированного средства электронной цифровой подписи, использующего при проверке электронной цифровой подписи открытые ключи лица (лиц), подписавшего (подписавших) электронный документ



# ОСНОВНЫЕ КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ



	<b>Метод</b>	<b>Стандарт Российской Федерации</b>	<b>Стандарт Республики Беларусь</b>
1	<b>Электронная цифровая подпись</b>	ГОСТ Р 34.10-2012	СТБ1176.1-99, СТБ П 34.101.45-2011
2	<b>Шифрование</b>	ГОСТ 29147-89	ГОСТ 29147-89 СТБ 34.101.31-2011
3	<b>Хэширование</b>	ГОСТ Р 34.11-2012 (взамен ГОСТ Р 34.11-94)	СТБ1176.1-99, СТБ 34.101.31-2011
4	<b>Генерация случайных (псевдослучайных) данных</b>	отсутствует	СТБ 34.101.47-2012
5	<b>Разделение секрета</b>	отсутствует	СТБ П 34.101.44-2011



# ОСНОВНЫЕ КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ



	<b>Формат</b>	<b>Стандарт Российской Федерации</b>	<b>Стандарт Республики Беларусь</b>
1	<b>Синтаксис обмена персональной информацией</b>	отсутствует	СТБ 34.101.18-2009
2	<b>Сертификат открытого ключа</b>	ITU-T X.509 Допускается использование альтернативных форматов	СТБ 34.101.19-2012
3	<b>Список отозванных сертификатов</b>	ITU-T X.509 Допускается использование альтернативных форматов	СТБ 34.101.19-2012
4	<b>Синтаксис криптографических сообщений</b>	отсутствует	СТБ 34.101.23-2012
5	<b>Запрос на получение сертификата</b>	отсутствует	СТБ 34.101.17-2012
6	<b>Карточка открытого ключа, сертификат ключа проверки ЭП на бумажном носителе</b>	ITU-T X.509	СТБ 34.101.49-2012

