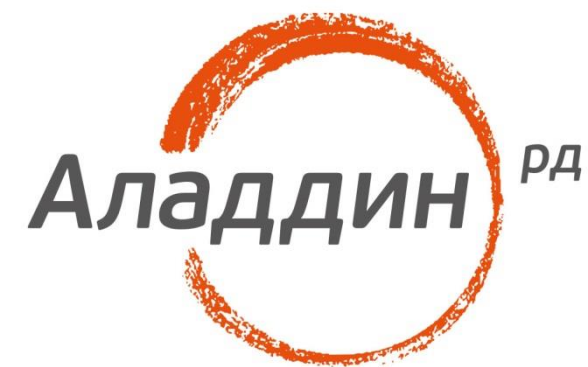


# Применение сервисов безопасности для обеспечения юридической силы электронных документов

---

Рускрипто, 23-25 марта 2016 г.



Алексей Сабанов, к.т.н.,  
Доцент МГТУ им. Н.Э.Баумана,  
Зам. генерального директора  
ЗАО «Аладдин Р.Д.»

# План доклада

---

1. Понятие "электронный документ" (ЭД)
  2. Понятие "юридическая сила" ЭД (ЮС ЭД)
  3. Сервисы безопасности: минимальный набор
  4. Проблемы регулирования ЮС ЭД в России
-

# Что такое электронный документ

---

- не имеет устоявшегося общепризнанного определения в законодательной и нормативной правовой базе Российской Федерации,
  - до сих пор не определены требования к его основным характеристикам
  - не утвержден минимально-достаточный набор электронных реквизитов, которые должны обеспечиваться сервисами безопасности.
1. связано с отсутствием системы доверия к электронному взаимодействию и решениям на базе РКІ
  2. Чем ждатель от юристов, лучше предложить нам самим
-

# Свойства (показатели качества) документированной информации

| Название характеристики           | Определение  | Источник                |
|-----------------------------------|--|-------------------------|
| <b>Надежность (достоверность)</b> | Свойство, характеризующее полноту и точность отражения в документах транзакций, деятельности и фактов, о которых эти документы свидетельствуют.  | ГОСТ Р ИСО 13008-2015   |
| <b>Достоверность</b>              | Свойство документа, содержание которого можно считать полным и точным представлением подтверждаемых операций, деятельности или фактов и которому можно доверять в последующих операциях или в последующей деятельности | ГОСТ Р ИСО 15489-1–2007 |
| <b>Целостность</b>                | Свойство документа, которое определяется его полнотой и неизменностью  | ГОСТ Р ИСО 15489-1–2007 |
|                                   | Свойство документа, состоящее в том, что при любой демонстрации документа заданные значения параметров демонстрируемого представления документа соответствуют специфицированным требованиям                            | ГОСТ Р 52292–2004       |

# Свойства (показатели качества) документированной информации

| Название<br>характеристики                   | Определение   | Источник                          |
|--|---|-----------------------------------|
| <b>Доступность</b>                           | Свойство документа, состоящее в том, что форма представления документа обеспечивает физическую возможность измерения заданных параметров этого представления документа (содержания, атрибутов, технологии) заданными средствами в заданных точках за конечное время | ГОСТ Р<br>52292–<br>2004          |
| <b>Пригодность<br/>для<br/>использования</b> | Свойство документа, состоящее в том, что его можно локализовать, найти, воспроизвести и интерпретировать.   | ГОСТ Р<br>ИСО<br>15489-1–<br>2007 |
| <b>Подлинность</b>                           | Свойство документа, сведения об авторе, времени и месте создания которого, содержащиеся в самом документе или выявленные иным путем, подтверждают достоверность его происхождения   | ГОСТ Р<br>51141-98                |

# Свойства (показатели качества) документированной информации

|                                  |   |                   |
|----------------------------------|---|-------------------|
| <b>Легитимность</b>              | Свойство документа, состоящее в том, что демонстрируемое представление документа содержит параметры, объективно подтверждающие правомерность использованных на протяжении жизненного цикла документа технологий<br><i>(примечание: это означает, что в ходе работы над ним использовались только допустимые операции в допустимой последовательности)</i> | ГОСТ Р 52292–2004 |
| <b>Юридическая сила</b>          | Свойство официального документа, сообщаемое ему действующим законодательством, компетенцией издавшего его органа и установленным порядком оформления  | ГОСТ Р 51141-98   |
|                                  | Свойство официального документа вызывать правовые последствия   | ГОСТ Р 7.0.8-2013 |
| <b>Юридическая значимость ЭД</b> | Комплекс свойств, обеспечивающих аутентичность, целостность, достоверность, конвертируемость и пригодность для использования, порождающего правовые последствия электронного документа, подписанного ЭП в порядке, установленном законодательством РФ   | Полякова Т. А.    |
|                                  | Свойство документа выступать в качестве подтверждения деловой деятельности либо событий личного характера   | ГОСТ Р 7.0.8-2013 |

# Аутентичность документ. информации

|  |                         |
|--|-------------------------|
| Свойство документа, которое состоит в том, что он: соответствует установленным правилам; был создан или отправлен лицом, уполномоченным на это; был создан или отправлен в то время, которое обозначено в документе  | ГОСТ Р ИСО 15489-1–2007 |
| Свойство документа, в отношении которого может быть доказано, что он является именно тем, чем претендует быть; что он был создан или послан именно тем лицом, которое указано в качестве его создателя или отправителя; и что он был создан или послан именно в то время, которое в нем указано. | ГОСТ Р ИСО 13008-2015   |
| Свойство документа быть тем, о чем заявлено в нем самом, т.е. содержать информацию, подтверждающую его происхождение (авторство, время и место создания и т.п.), причем таким образом, чтобы это гарантировало документ от подделок  | Тихонов В.И.            |
| Свойство быть подлинным, т.е. документ является именно тем, чем он претендует быть ( <i>примечание: свойство аутентичности не касается вопросов достоверности фактов, изложенных в документе, оно подтверждается его видом, и/или способом хранения</i> ).                                       | Спецификация MoReq      |
| Неизменность во времени оригинальных характеристик документа по отношению к контексту, структуре и содержанию  | Межд.совет архивистов   |
| Свойство электронного документа, гарантирующее, что электронный документ идентичен заявленному   | ГОСТ Р 7.0.8-2013       |

# Анализ таблицы → Выводы: достоверность

---

Для обеспечения достоверности (надежности) электронные документы должны создаваться во время или сразу после операции или случая, к которым они относятся, лицами, достоверно знающими факты, или средствами, обычно используемыми в деловой деятельности при проведении данной операции.

Для электронного документа достоверность может опосредованно определяться статусом организации, издавшей документ, идентификацией этой организации, а также автора документа и его полномочиями.

---



# Доступность

На доступность ЭД существенно влияет надежность СЭД, которая должна обеспечивать гарантированный доступ ко всем относящимся к определенному вопросу документам и связанным с ними метаданным за время, не превышающее установленные ограничения.

Например, согласно "Требований к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающих в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения", доступ к регистрационно-контрольной карточке должен занимать не более 5 секунд, а восстановление ЭД из резервной копии должно занимать не более 30 минут.

# Целостность

- на организационном уровне обеспечивается за счет реализации политики и процедур управления документами, которые должны указывать, какие дополнения или примечания могут быть добавлены к документу после его создания, при каких обстоятельствах дополнения или примечания могут быть разрешены и кто уполномочен сделать это.
- на техническом уровне обеспечивается применением электронной подписи (ЭП), одним из главных назначений которой является верификация того, вносились ли какие либо изменения в текст ЭД. Электронная подпись всегда связана с конкретным ЭД, процесс подписания на математическом языке означает вычисление хэша документа и его шифрование на закрытом ключе электронной подписи. Проверка ЭП осуществляется с помощью соответствующего открытого ключа, который должен быть доступен всем, кому необходимо выполнить проверку.

# Аутентичность

---

Свойство "аутентичность" в отношении документов практически полностью совпадает со свойством "подлинность", в ряде случаев они являются синонимами. При анализе аутентичности основное внимание уделяется метаданным (МД).

В стандарте ГОСТ Р ИСО 15489-1–2007 метаданные определяются как данные, описывающие контекст, содержание, структуру документов и управление документами в течение определённого времени. В СЭД именно МД делают электронные документы пригодными для использования, понятными и аутентичными, гарантируют неизменность, достоверность и юридическую силу (ЮС) ЭД.

---

# Аутентичность эл.документа

- "соответствует установленным правилам" – в подавляющем числе случаев это принадлежность к конкретной **СЭД**, системе документооборота органа власти, имеющего **право издания документа или подчинение установленным требованиям** к определённым видам документов для индивидуальных актов (правила составления договора, доверенности и т.д.);
- "был создан или отправлен лицом, уполномоченным на это" – для обеспечения этого условия требуется, как минимум, три сервиса безопасности – **аутентификация, электронная подпись и реестр полномочий**, поддерживаемый в актуальном состоянии;
- "был создан или отправлен в то время, которое обозначено в документе" – обеспечивается применением сервиса **доверенного времени**.

# Юридическая сила электронного документа

Это свойство официального документа вызывать **правовые последствия**. Обеспечивается **комплексом** нормативно-правовых, организационных и технических мер.

Юридическую силу электронному документу придают:

- обязательные реквизиты (метаданные);
- идентификация издателя и аутентификация автора электронной подписи;
- положение издателя документа относительно других участников электронного взаимодействия (для гос. органов это иерархия нормативных документов согласно ст. 15 Конституции РФ);
- подтверждение полномочий автора электронной подписи;
- аутентичность (подлинность) ЭД;
- порядок оформления, определенный в законодательстве или иных нормативных правовых актах

# Сервисы безопасности: подпись

---

- аутентификация источника данных – подтверждение подлинности источника полученных данных (ISO 7498-2);
  - обеспечение целостности данных, означающее, что данные не были модифицированы или уничтожены неавторизованным образом (ISO 29115);
  - невозможность отрицания авторства – сервис защиты от отрицания автором факта создания или отправления им сообщения (ISO/IEC 13888-1).
-

# Сервис аутентификации

---

- обеспечение доказательства подлинности предъявленного идентификатора (ISO/IEC 29115);
  - доказательство принадлежности аутентификатора, с помощью которого производится доказательство подлинности, конкретному объекту (ISO/IEC 10181-2);
  - аутентификация сторон – подтверждение того, что взаимодействующая сторона является той, за которую себя выдает (ISO 9798-3).
-

# Сервис доверенного времени

---

Сервис меток доверенного времени совместно с сервисом штампов времени (RFC 3161 "Time-Stamp Protocol (TSP)") образуют Службу доверенного времени.

Суть сервиса состоит в синхронизации серверного времени для всех удостоверяющих центров, участвующих в формировании и проверки статуса сертификата

---



# Сервис валидации (RFC 2459)

---

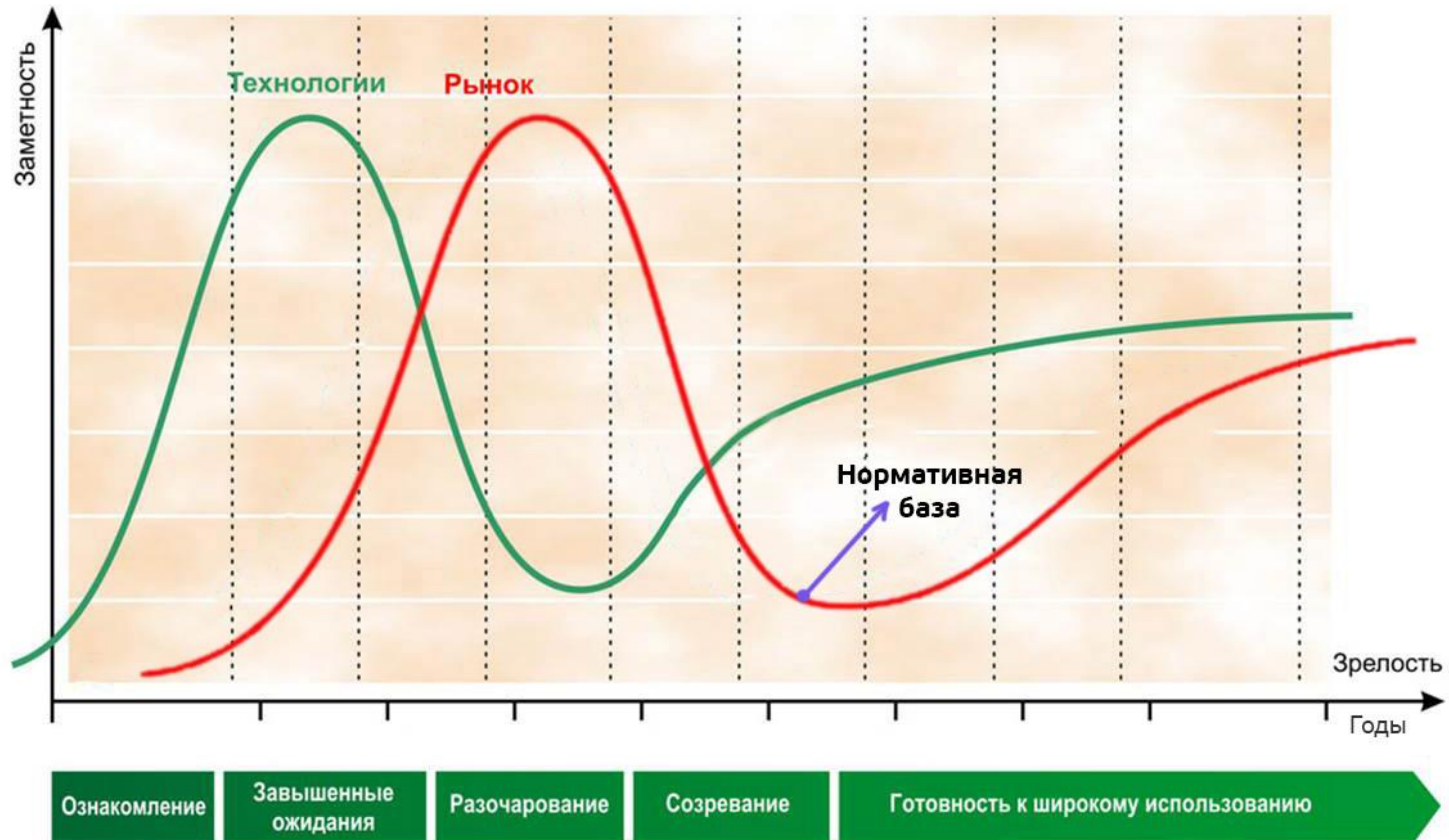
- проверка действительности данных, связанных с подписанным сообщением или документом, а также сертификатов ключей подписи.

Может проводиться по стандартизованному протоколу Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS) с квитанцией за подписью сервера (RFC 3029). Для проверки статуса сертификата также используется On-line Certificate Status Protocol - OCSP (RFC 2560).

Отдельно может проводиться проверка действительности сертификата открытого ключа – Validation of Public Key Certificates (VPKC)

---

# Влияние регулирования



# Спасибо за внимание!

---

