


Пространство доверия для обеспечения  
юридической силы электронным документам;  
правовые основы обеспечения ЮС ЭД;  
проблемы доверия к результатам  
идентификации и аутентификации кредитными  
и некредитными организациями, способы их  
решения




Уральский Форум, 18 февраля 2016 г.

Алексей Сабанов к.т.н.,  
член Экспертного совета комитета  
ГосДумы по безопасности и  
противодействию коррупции

»

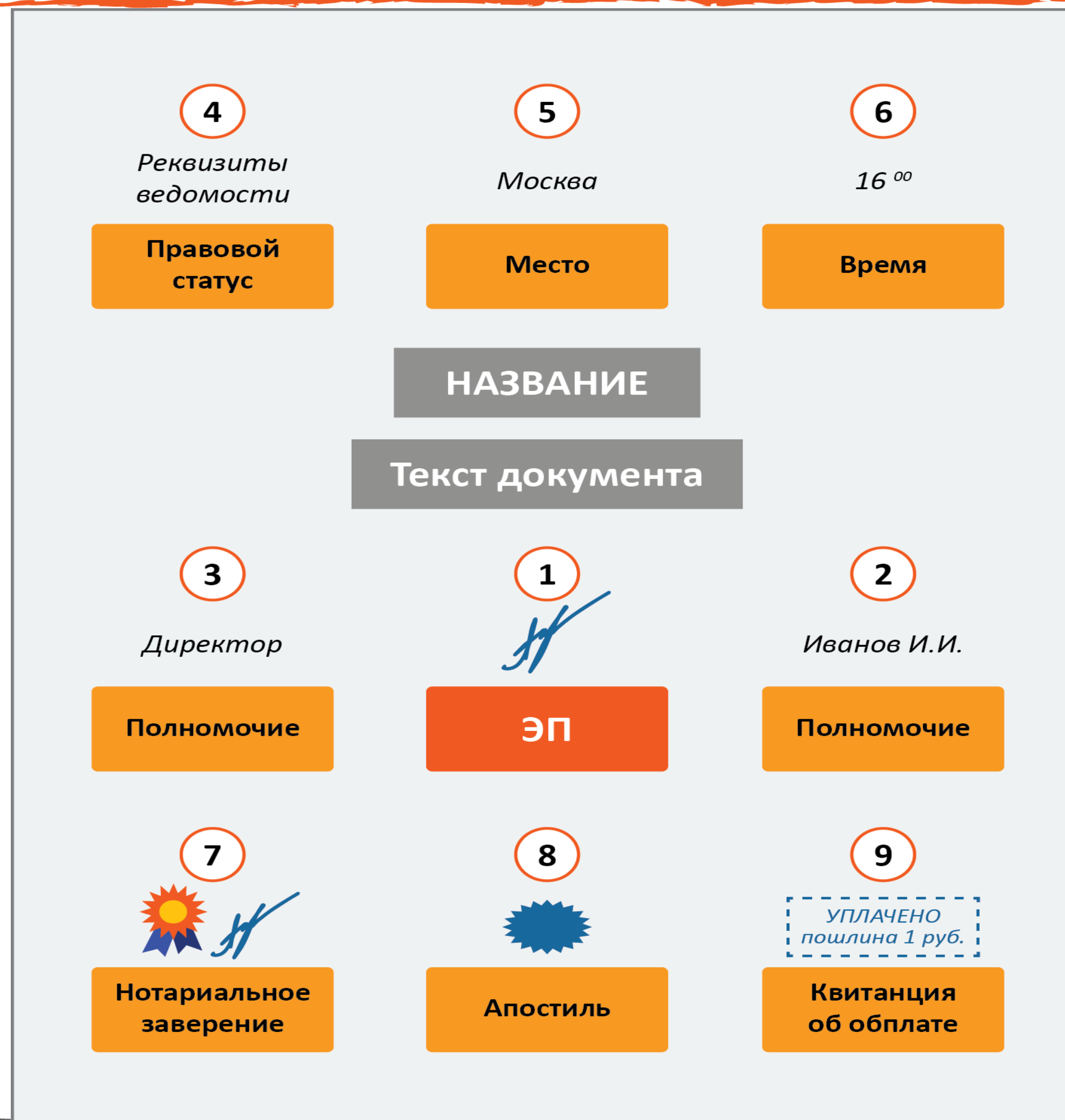


Пространство доверия для  
обеспечения юридической силы  
электронным документам



# Переход на безбумажный оборот

Аналогия с  
бланком  
бумажного  
документа



Постановление  
Правительства  
от 15.06.2009  
№477 для  
бумажных  
документов в  
ФОИВ  
(24 реквизита)

# Электронный документ

---

Электронный документ – это документ, в котором информация представлена в электронной (компьютерной) форме с реквизитами, необходимыми для признания его действительным. Как правило, в число обязательных реквизитов входят: наименование организации, дата, регистрационный номер, должность и фамилия лица, подписавшего документ, электронная подпись.

Реквизит электронного документа - обязательные сведения, которые должны содержаться в электронном документе для признания его действительным.

---



# Единое пространство доверия ЮС ЭД

Создание правового поля  
для юридически -  
значимого электронного  
документооборота



Технологии обращения с  
электронными записями,  
документами и сообщениями,  
позволяющие обеспечивать  
юридическую их силу


Организация  
документирования,  
передачи , хранения и  
обработки информации  
для участников  
информационного  
взаимодействия

# ЕПД: техническая компонента


---

**Единое пространство доверия - совокупность взаимосвязанных доверенных сервисов, развернутых на базе инфраструктуры открытых ключей:**

- **сервисов, участвующие в создании, валидации, обработке, хранении электронных подписей**
- **меток доверенного времени,**
- **средств доставки и заверения электронных сообщений,**
- **разграничения и управления доступом,**
- **аутентификации, в том числе на на Web-сайтах,**
- **электронных сертификатов (в том числе атрибутивных),**
- **актуальных реестров (ролей участников электронного взаимодействия, уполномоченных лиц и др.),**
- **сервисы регистрации и документирования**



# Правовые основы обеспечения юридической силы электронным документам



# Юридическая сила

Юридическая сила бумажного документа – это категория, связанная с положением нормативно-правовых актов в иерархии таких актов. Юридическая сила закона или нормативно-правового акта определяется положением органа, издавшего акт, в общей системе правотворческих органов, его компетенцией и характером самих актов\*.

Электронный документ отличается от бумажного документа уточнением о средствах, с помощью которых документ может быть воспроизведен, передан и обработан.

63-ФЗ "Об электронной подписи": Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

Юридическая сила электронного документа может быть обеспечена комплексом нормативно - правовых, организационных и технических мер.

\*ГОСТ Р 51141-98 Делопроизводство и архивное дело



# Юридическая значимость

---

Понятие "юридическая значимость" пока не имеет законодательного определения

Юридически значимый документ – это документ, который может выступать в качестве доказательства (подтверждения) деловой или иной деятельности и имеет определенные правовые последствия для субъектов электронного взаимодействия.

Юридическая значимость позволяет судить о юридической силе электронного документа, но не обязательно является доказательством того, что электронный документ действительно имеет юридическую силу. Юридическую значимость принято связывать с наличием правовых последствий.

---

# Взгляд юриста: минимальные требования

## Процедура проверки юридической силы электронного документа

Допустимость оформления документа в электронной форме в соответствии с требованиями **действующего законодательства** Российской Федерации

**Определение лица,** подписавшего электронный документ электронной подписью

Правовая оценка наличия у подписавшего электронный документ лица **полномочий на подписание** такого вида документов

**Подтверждение целостности** электронного документа

# Как обеспечить юридическую силу?

---

- Необходимость определения личности владельца электронной подписи (идентификация)
  - Проверка полномочий на подписание (реестр)
  - Подтверждение целостности (электронная подпись)
  - Обеспечение неотказуемости от подписи (аутентификация, электронная подпись, валидация сертификата ключа подписи, метка времени)
  - Необходимость проверки полномочий подписанта
-



# Минимальный набор сервисов безопасности

---

- Аутентификация
  - Электронная подпись
  - Метка доверенного времени (RFC 3161 «**Time-Stamp Protocol (TSP)**»)
  - Валидация сертификата ключа проверки подписи (RFC 2459)
  - Проверка полномочий подписанта
-



# Сервис аутентификации

---

- обеспечение доказательства подлинности предъявленного идентификатора (ISO/IEC 10181-2:1996, 9798-3:1998);
  - доказательство принадлежности аутентификатора, с помощью которого производится доказательство подлинности, конкретному объекту (ISO/IEC 24760-2:2015);
  - аутентификация сторон – подтверждение того, что взаимодействующая сторона является той, за которую себя выдает (ISO 29115: 2013).
-

# 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 9594-8);
  - невозможность отрицания авторства – сервис защиты от отрицания автором факта создания или отправления им сообщения (ISO/IEC 13888-1).
-

# Достоверность идентификации

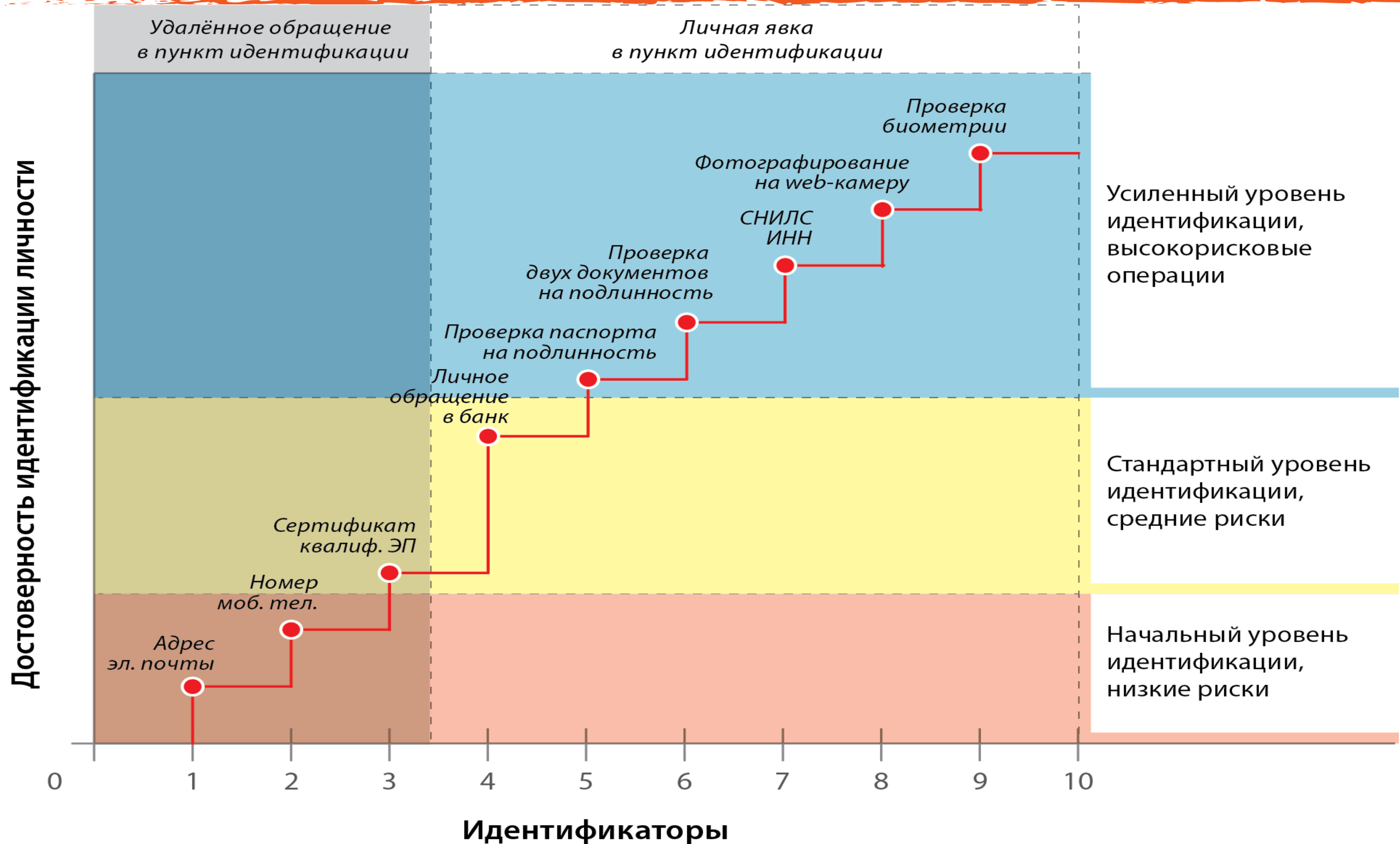
---

**Достоверность информации** - общая точность и полнота информации. **Достоверность информации** обратно пропорциональна вероятности возникновения ошибок в информационной системе.

**Достоверность идентификации и аутентификации (ИА)** - мера доверия к результатам ИА при условии безошибочности выполнения процедур идентификации и аутентификации. Поскольку безошибочность может иметь уровни точности ее определения, то и мера доверия (то есть достоверность) может иметь уровни достоверности, называемые в западных нормативных источниках уровнями гарантий.

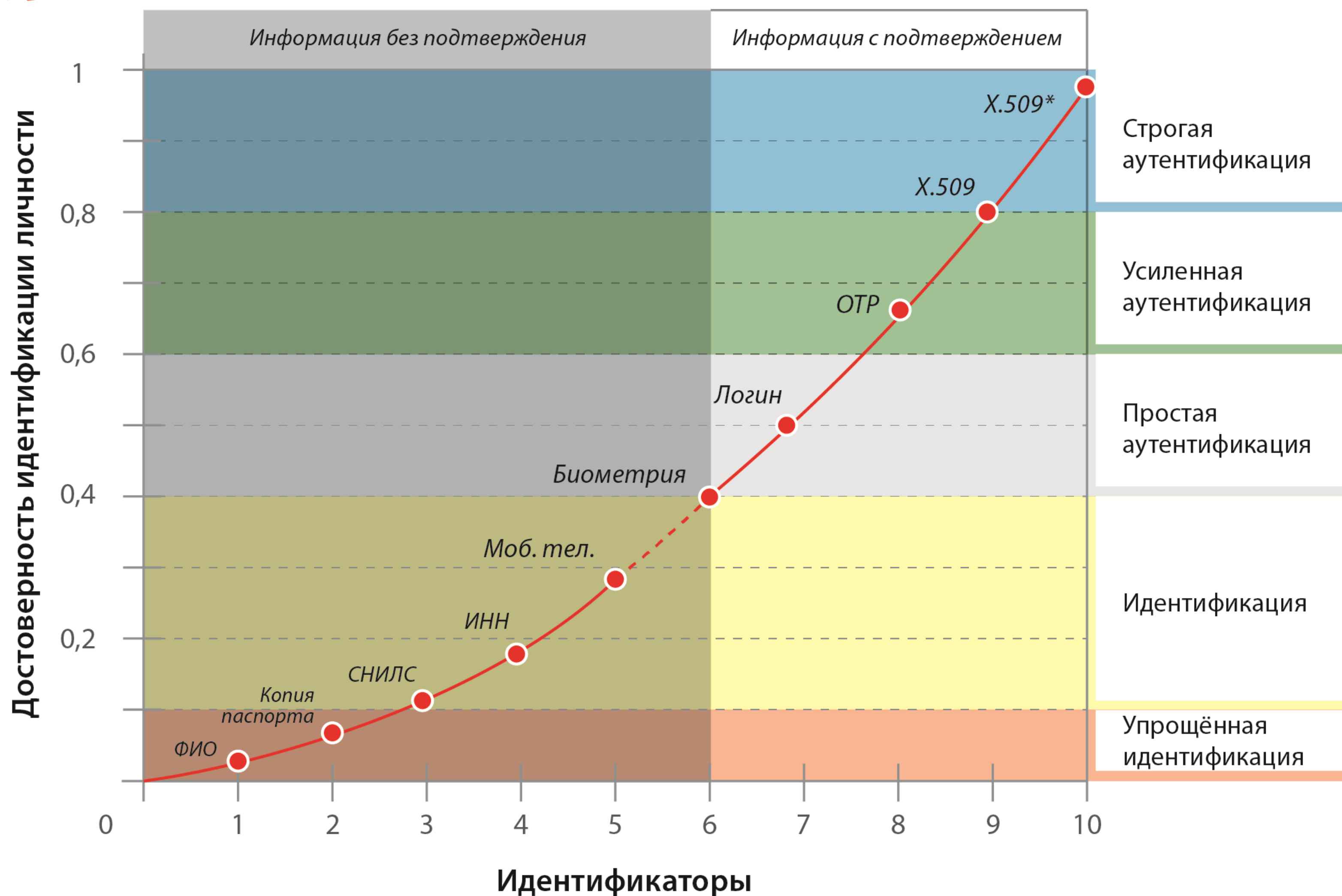
---

# Достоверность можно накапливать





# Достоверность идентификации



# Доверие к идентификации

---

Основной критерий – Качество идентификации – отличие одного субъекта от другого путем сравнения предъявленных идентификаторов с занесенными в БД.

Имеются ошибки первого (легальный пользователь не идентифицирован) и второго рода (злоумышленник идентифицирован как легальный user).

Требует уровней доверия к результатам сравнения в зависимости от числа идентификаторов и механизмов сравнения. Требует протоколирования результатов для разбора конфликтных ситуаций.

---

# Доверие к аутентификации

---

Только аутентификация доказывает привязку идентификаторов и аутентификатора к конкретной личности. Самая безопасная и надежная аутентификация основана на сертификате доступа с механизмом аутентификации в виде электронной подписи.

Основной Критерий – качество (безопасность и надежность) аутентификации.

Необходимо ввести уровни доверия к аутентификации.

---

# Уровни аутентификации и подписи

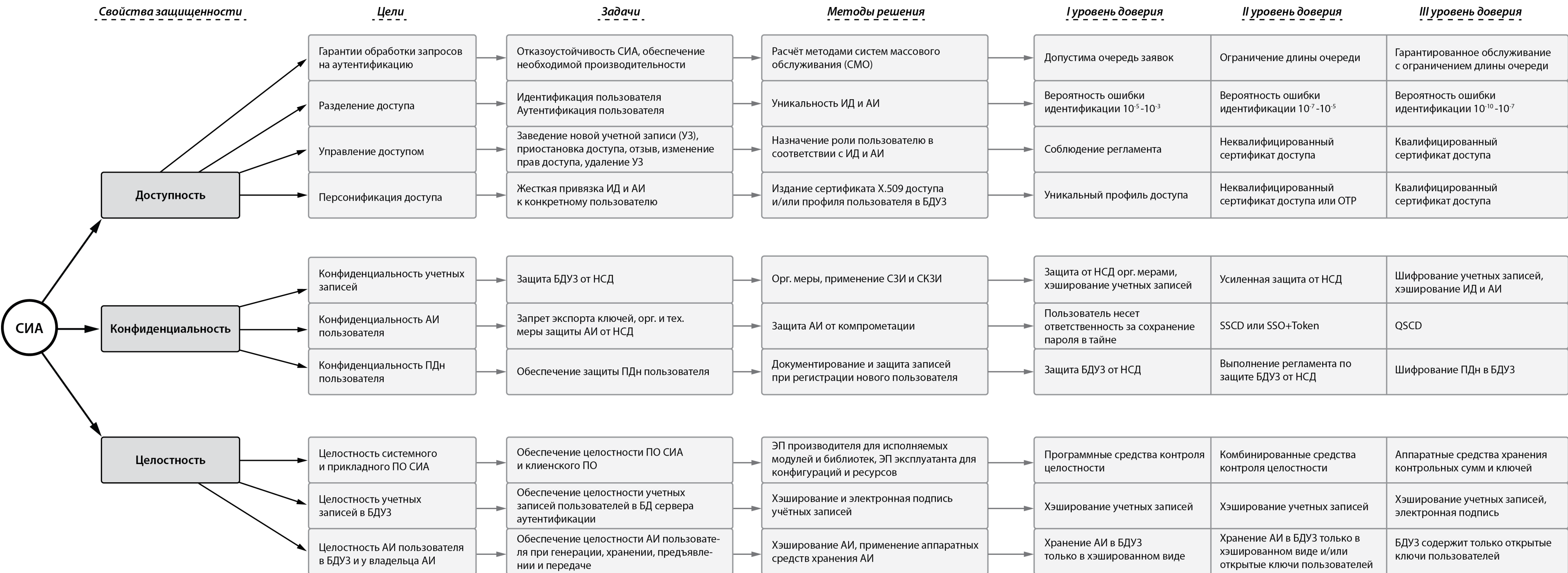
	виды ЭП		
Типы аутентификации	простая	усиленная	строгая
простая	+	-	-
усиленная	+	+	-
строгая	+	+	+




# Триада информационной безопасности

Уровни достоверности (типы аутентификации)	Доступность	Целостность	Конфиденциальность
Простая (пароль)	+	-	-
Усиленная (ОТР)	+	-	-
Усиленная (сертификат доступа X.509)	+	+	+
Строгая (X.509 выдан доверенным УЦ)	+	+	+

# Классификация систем идентификации и аутентификации





# Связь уровней идентификации с банковскими рисками



# Матрица рисков и уровни идентификации

СВР угроз ИБ	Уровни идентификации в зависимости от СТП нарушения ИБ			
	минимальная	средняя	высокая	критическая
нереализуемая	Низкий	Низкий	Средний	Высокий
минимальная	Низкий	Средний	Высокий	Запрещенная операция
средняя	Средний	Высокий	Запрещенная операция	Запрещенная операция
высокая	Средний	Запрещенная операция	Запрещенная операция	Запрещенная операция
критическая	Запрещенная операция	Запрещенная операция	Запрещенная операция	Запрещенная операция

Методика оценки рисков нарушения ИБ. Распоряжение Банка России от 11.11.2009 № Р-1190





# Зарубежный опыт



# Пример Норвегии

---

Имеется 3 системы идентификации граждан:

Государственная Min ID (MyID - для граждан с 13 лет), использует национальный Id, возможна первичная идентификация по номеру мобильного телефона с OTP, который приходит по SMS. Доступ к онлайн-сервисам более 50 госуслуг.

Банковская – более высокий уровень гарантий, чем Min ID. Использует набор механизмов безопасности, включая смарт-карты и ЭП на SIM. На июнь 2010г. охвачено более 2,5 млн. из 4.7 млн населения

BuyPass. Использует смарт-карты и мобильные телефоны

---

# Документы для первичной идентификации

## List 1

### Evidence of link between photo & signature

- Australian driver's licence
- Australian passport
- Australian firearm's licence
- Defence force/Police ID card
- Department of Immigration and Citizenship (DIAC) certificate with of evidence of residence status
- WA Photo Card, Over 18 or Proof of Age Card
- Australian learner driver's permit card

## List 2

### Evidence of operating in the community

- Debit or Credit card (one or the other, not both) issued by a financial institution
- Document of Identity issued by the Passport Office
- Entitlement card issued by the Commonwealth or State Government (Centrelink, Health Care card, Veterans Affairs card etc)
- Full birth certificate issued in Australia (birth extracts not accepted)
- Medicare card
- Naturalisation, citizenship or immigration papers issued by Department of Immigration & Boarder Protection (DIBP)
- Overseas passport with current Australian Entry Permit
- Security guard or crowd control licence (Australian)
- Student identity document or Statement of enrolment issued by an educational institution, including Tertiary (should include photo and/or signature)
- Working with children card

## List 3

### Evidence of current residential address

- Driver's licence renewal notice
- Financial institution statement less than six months old
- Motor vehicle registration
- Property lease or tenancy agreement
- Shire/water rates notice
- School or other educational report or certificate less than twelve months old
- Utility account less than six months old (e.g. gas, electricity, home phone etc)

# Международные стандарты

---

- ITU-T X.811 (04/1995) Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework [Основы безопасности для открытых систем: Основы аутентификации]
  - ITU-T Rec.X.509 (2012) The Directory: Public-key and attribute certificate frameworks
  - ITU-T Rec.X.1254 (2012) Общая структура комбинированной аутентификации в среде с несколькими поставщиками услуг определения идентичности
  - ITU-T Rec.X.1154 (2013) Структура гарантии аутентификации объекта
-



# Модели

Один домен  
Однофакторная аутентификация



Один домен  
Комбинированная аутентификация



Случай федерации

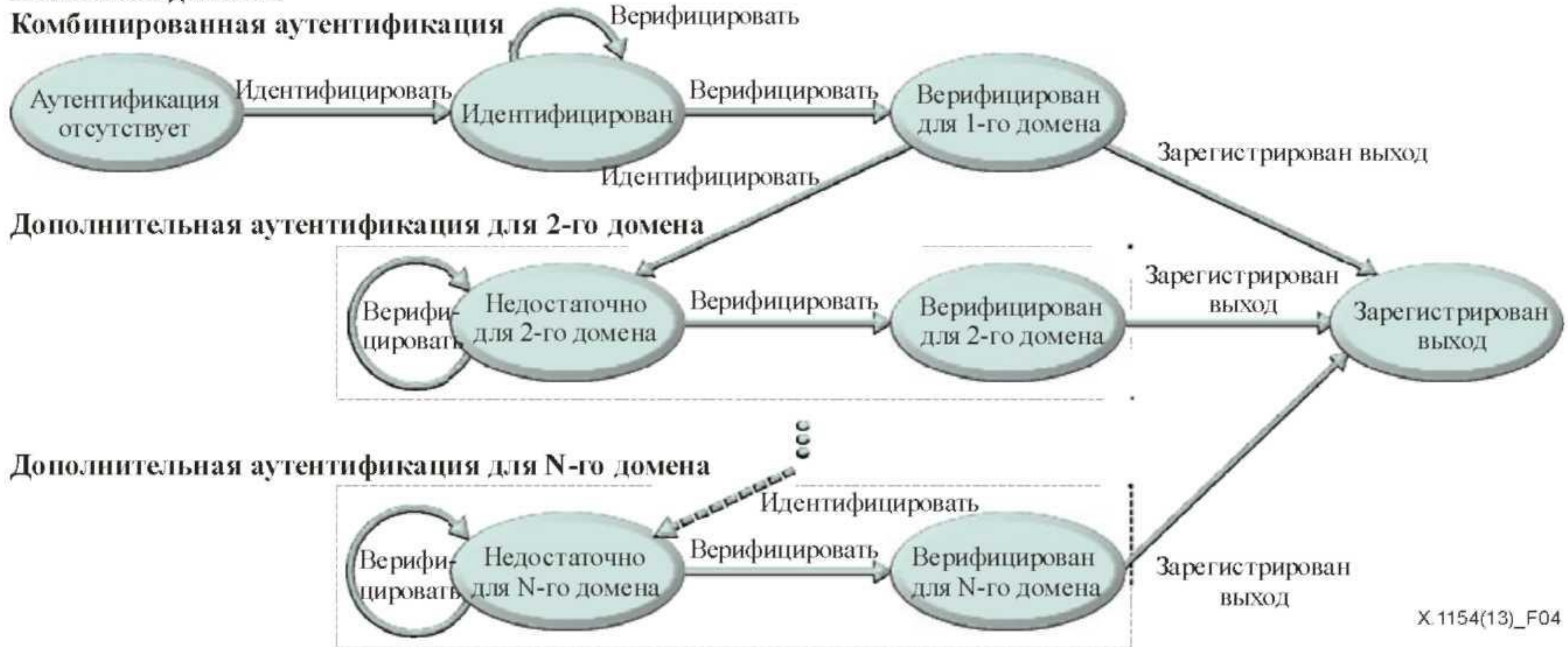




# Комбинированная аутентификация

Несколько доменов

Комбинированная аутентификация

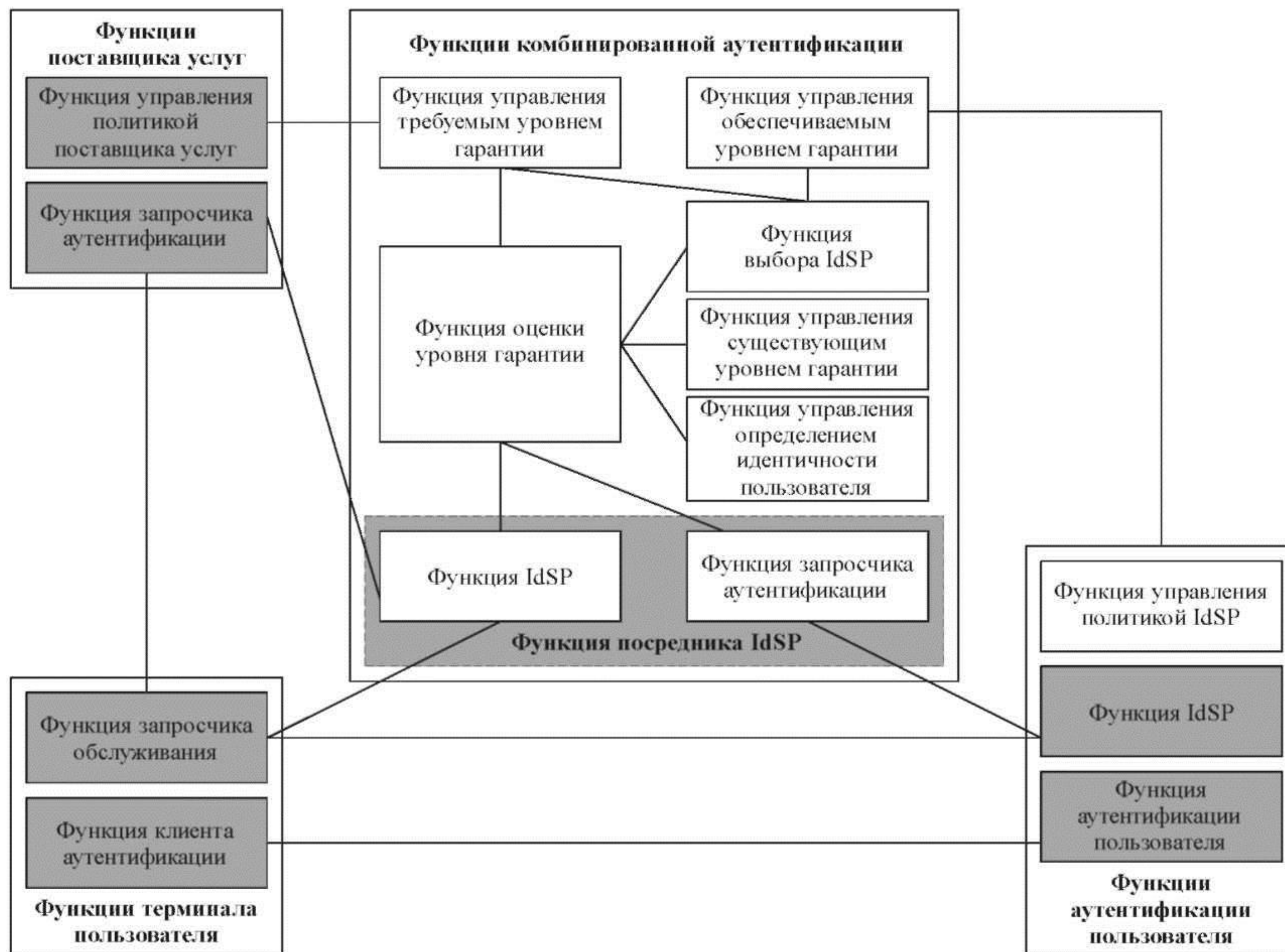


Дополнительная аутентификация для 2-го домена

Дополнительная аутентификация для N-го домена



# Взаимосвязь с ITU-T X.1141



# Сценарии разделения по рискам

---

Для малорисковых операций можно использовать облегченные модели и технологии идентификации

Для среднерисковых операций требуется создание и использование федеративной модели трансляции доверия

Высокий уровень СВР угроз и СТП последствий требует создания высоконадежных схем и технологий трансляции доверия

---



# Итоги. Пространство доверия ААА

---

- Переход от "плоских" моделей к пространственным
- Опора на международные стандарты
- Создание доверенных отношений между центрами первичной идентификации клиентов
- Утверждение критериев и метода построения пространства доверия к идентификации и аутентификации клиентов

# Итоги. Юридическая сила ЭД

---

- Инфраструктура и доверенные средства генерации, применения и проверки усиленной квалифицированной электронной подписи (УКЭП);
- Развитая системы проставления меток доверенного времени, синхронизированного в каждом аккредитованном удостоверяющем центре с временем корневого УЦ;
- Поддерживаемая в актуальном состоянии с заданным интервалом времени (в часах) система реестров полномочий и правомочий владельцев УКЭП;
- Доверенные сервисы идентификации и аутентификации, строго регламентированные для каждого аккредитованного УЦ с регулярным внешним контролем порядка и правил выполнения основных процедур.

# Спасибо за внимание!

---



[a.sabanov@aladdin-rd.ru](mailto:a.sabanov@aladdin-rd.ru)

A decorative footer pattern consisting of a horizontal band of small, light gray hexagonal shapes.