Необходимость введения уровней доверия к идентификации и аутентификации (ИА). Кто может гарантировать достоверность ИА?

PKI-форум 16-18 сентября 2014 г.

Алексей Сабанов

Зам. генерального директора

ЗАО «Аладдин Р.Д.»

Доверие к идентификации

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

Имеются ошибки первого (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

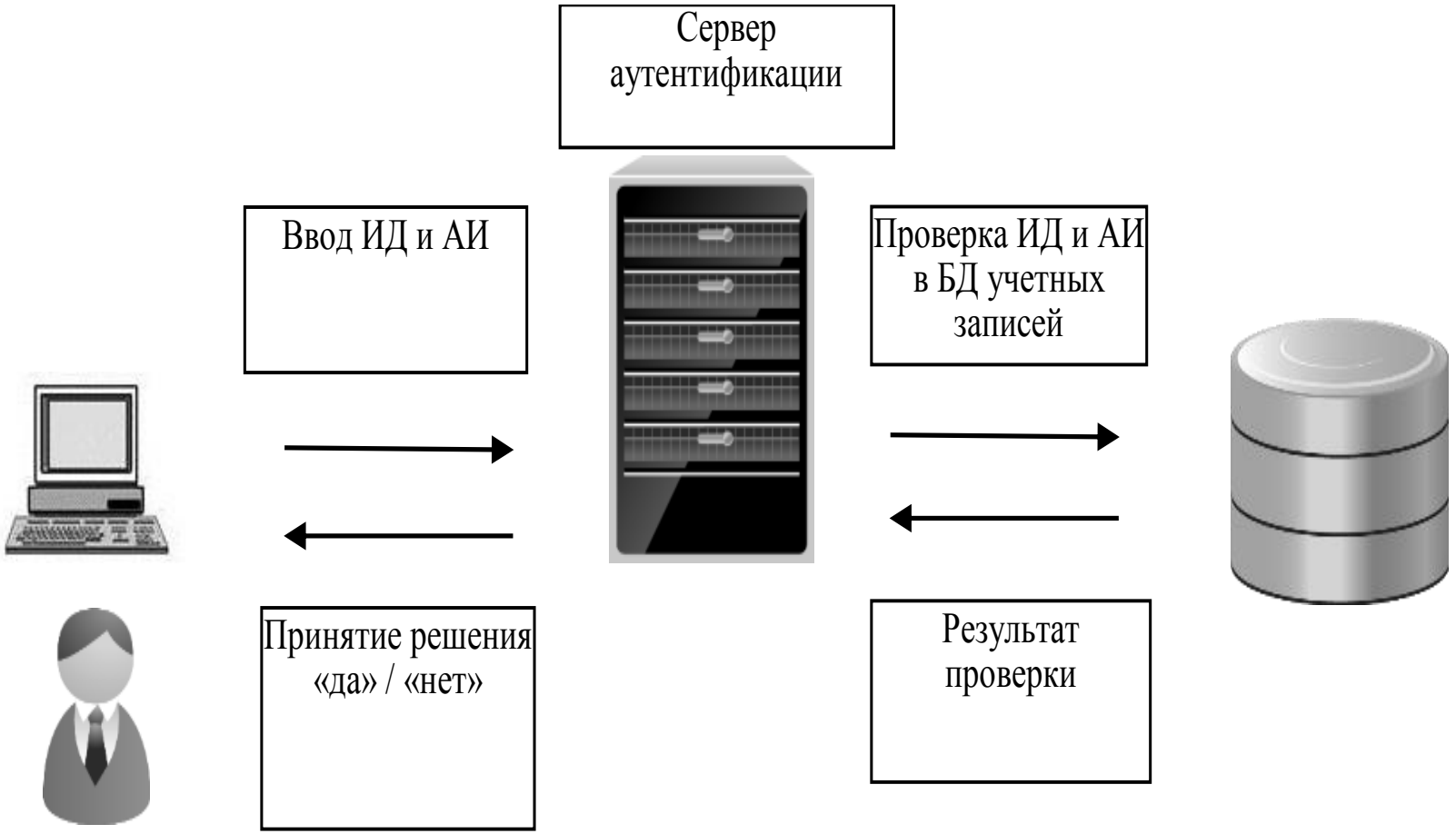
Только аутентификация доказывает привязку идентификаторов и аутентификатора к конкретной личности. Самая безопасная и надежная аутентификация основана на сертификате доступа с механизмом аутентификации в виде электронной подписи.

Основной Критерий – качество (безопасность и надежность) аутентификации.

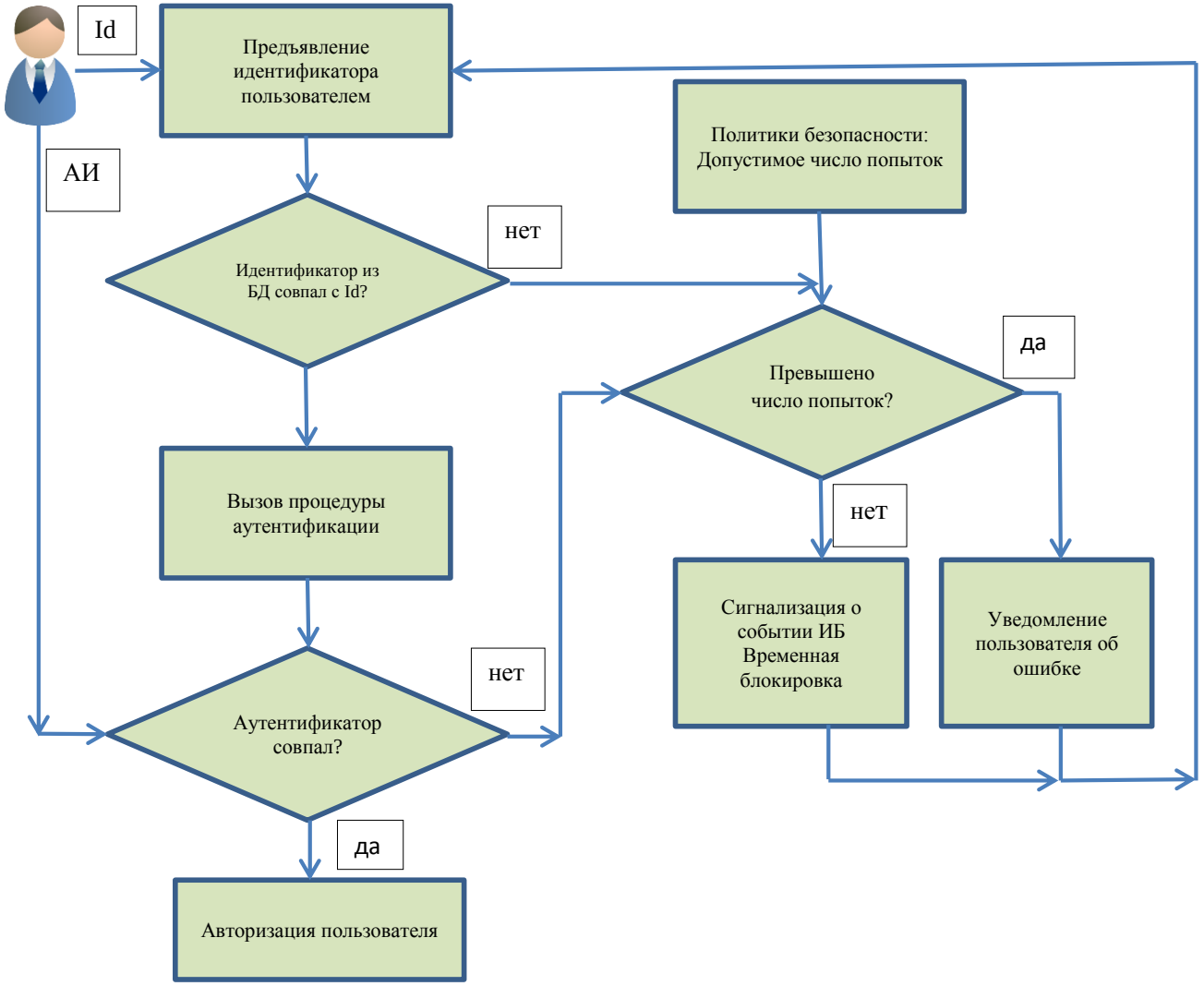
Необходимо ввести уровни доверия к аутентификации.

Основная нерешенная Проблема – трансляция доверия от одной ИС к другой.

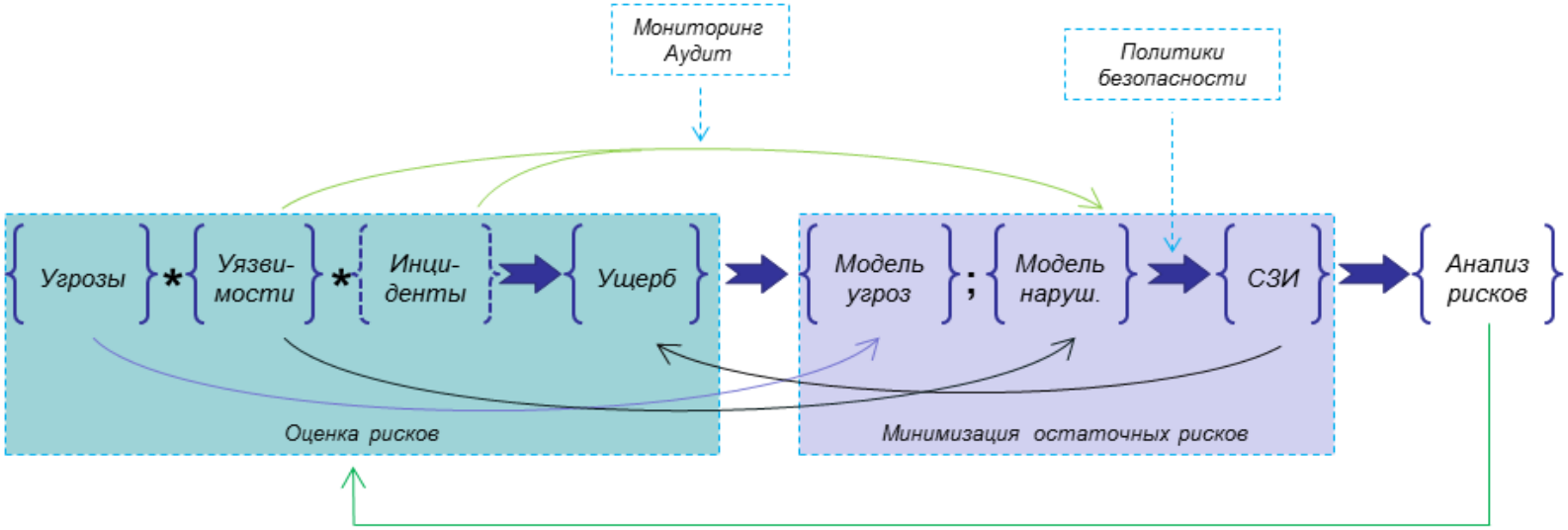
Схема проверки информации претендента



Блок - схема аутентификации



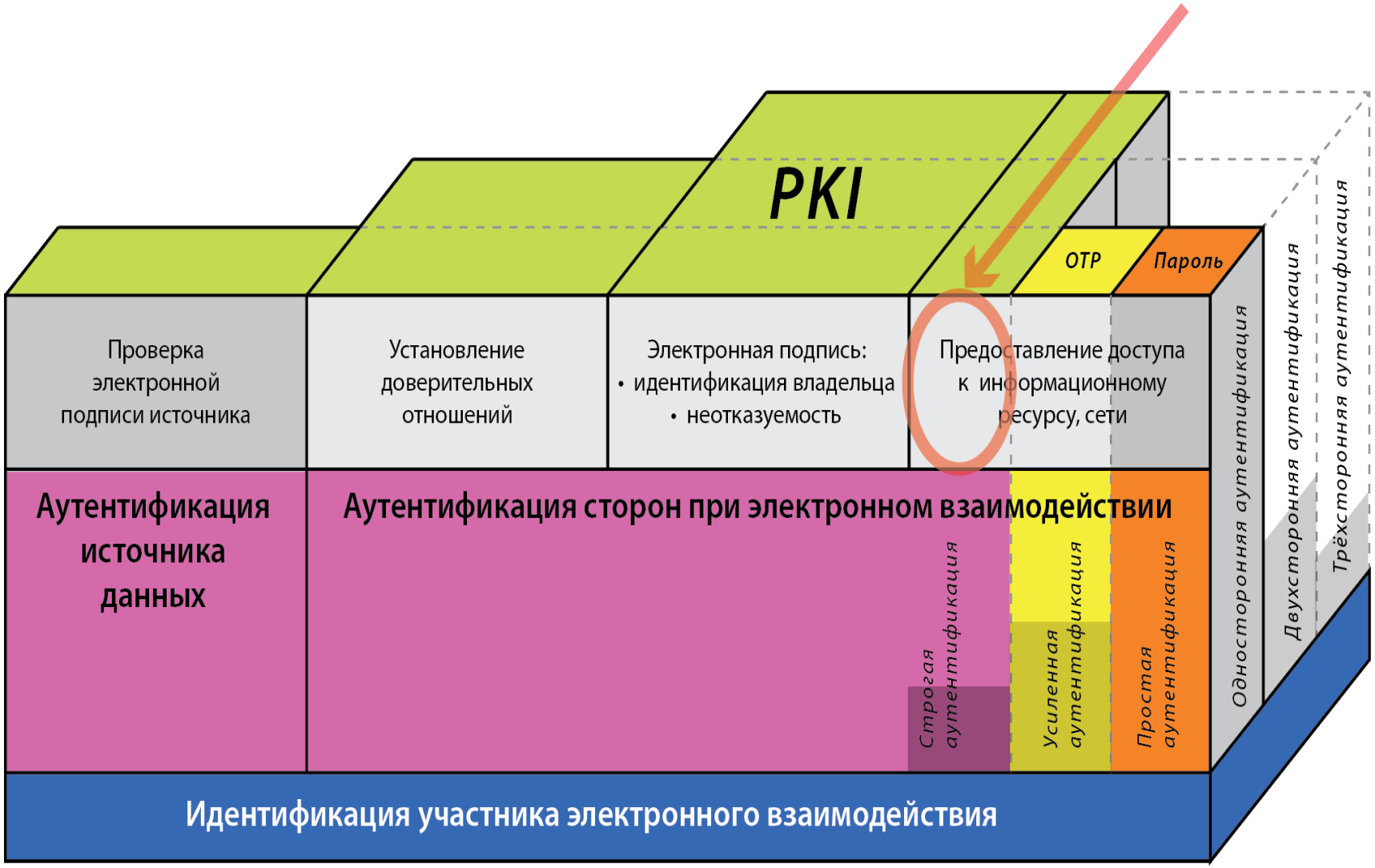
Стандартные методы оценки рисков



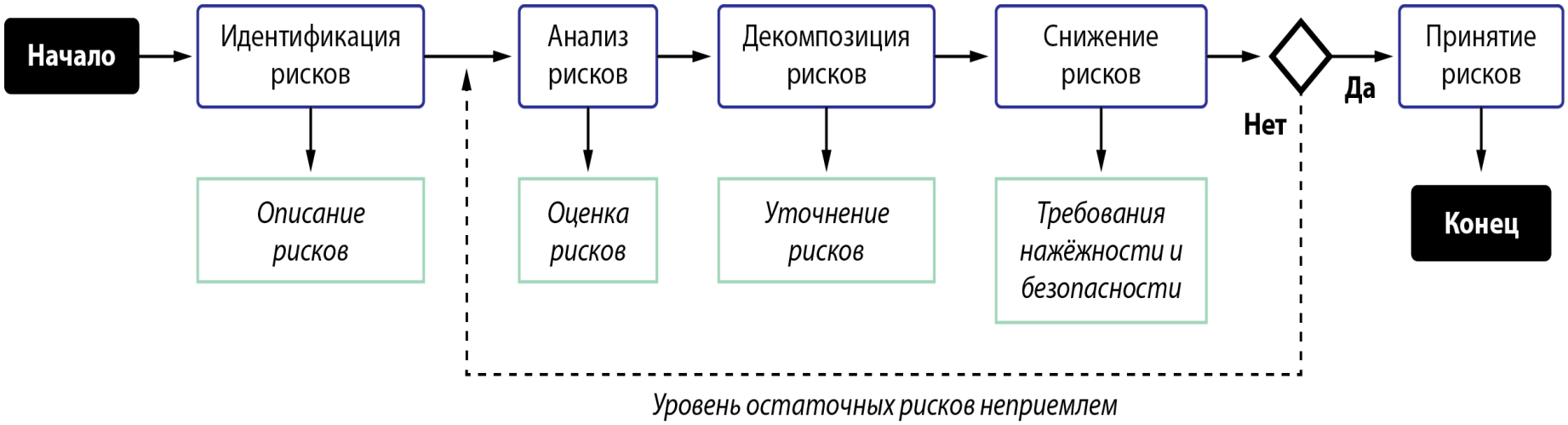
3 вида ЭП – 3 типа аутентификации

Учетная запись пользователя	**Секрет (аутентификатор)**	**Тип аутентификации**
логин	пароль	простая
Логин или поля X.509 (УЦ не аккредитован)	одноразовый пароль (технология OTP) или Закрытый ключ	усиленная
заданные поля X.509, сформированного **аккредитованным** удостоверяющим центром для доступа пользователя	закрытый ключ (в терминах №1-ФЗ)	строгая

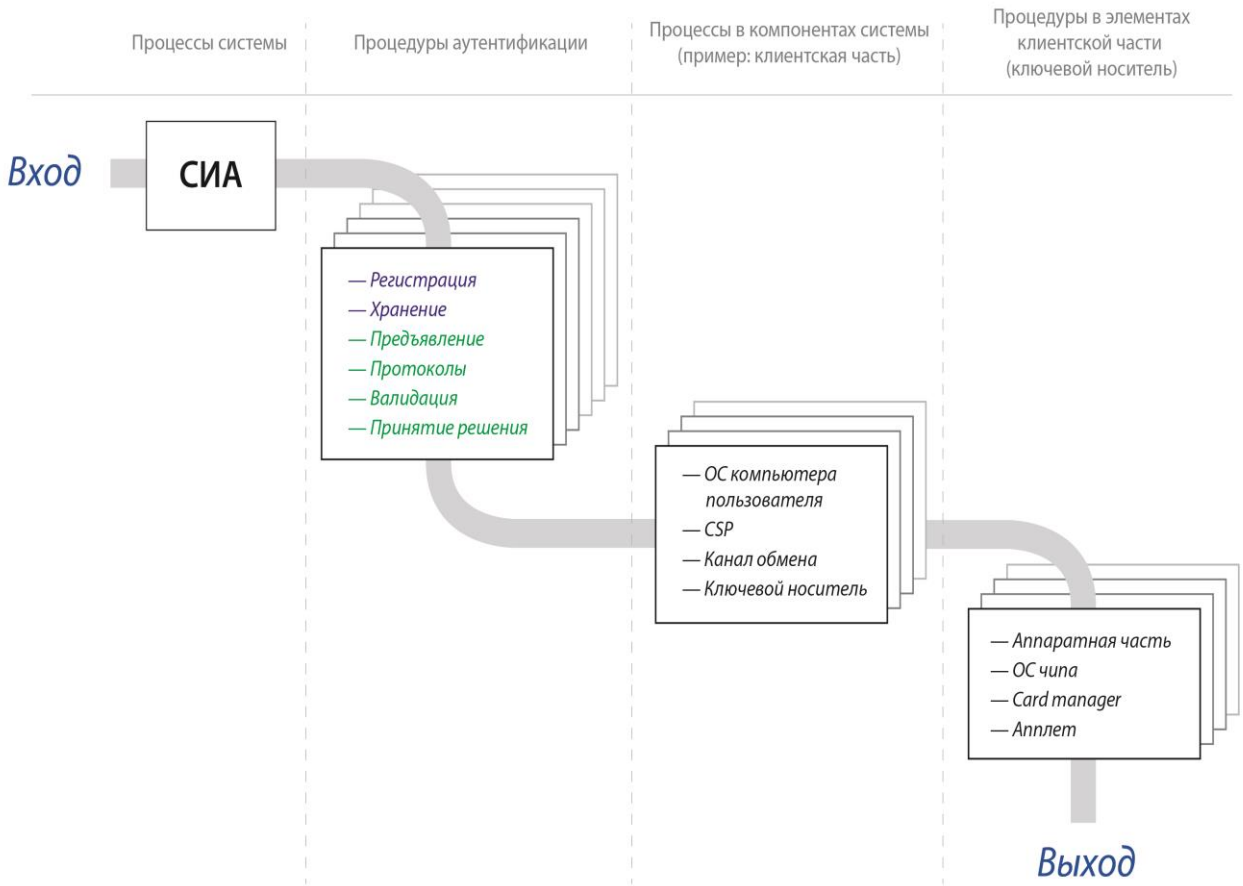
Связь аутентификации и ЭП



Алгоритм оценки рисков



Уровни анализа



Процедуры аутентификации

- Регистрация;
- Хранение;
- Предъявление идентификаторов;
- Предъявление аутентификатора;
- Протокол обмена;
- Валидация;
- Принятие решения;
- Передача управления в блок авторизации.

Пример процедур: регистрация

Субъект (аппликант) обращается в ЦР с целью стать пользователем ИС. Заявитель *предъявляет* в ЦР свои Credentials (ЭУ или бумажные действующие удостоверения личности, содержащие присвоенные ему *идентификаторы*).

ЦР *проверяет* предъявленные бумажные или ЭУ на предмет совпадения *принадлежности* предъявленных документов данному субъекту и их *действительности* (валидация).

На основании выполненной проверки ЦР *создает* учетную запись для данного субъекта в базе данных ЦР для доступа к информационным ресурсам (ресурсу).

На основе записи для субъекта ЦР *издает/регистрирует* секрет (аутентификатор), ассоциированный с конкретным субъектом.

Процедура *делегирования* прав доступа (фактически делегирование доверия к изданным аутентификатору и ЭУ) другой (или другим) ИС на основе доверительных отношений. При переходе к облачным вычислениям эта процедура становится весьма актуальной.

Последней процедурой регистрации является *выдача* изданных ЦР-ом аутентификатора и ЭУ на руки субъекту.

Анализ угроз первого уровня

Источник угроз	**Вид угрозы**	**Уровень угрозы**
внешний нарушитель	без злого умысла	средний
внешний нарушитель	злонамеренная	высокий
внутренний нарушитель	ошибки	средний
внутренний нарушитель	инсайдер	высокий
техногенные угрозы	аварии	низкий
техногенные угрозы	отказы	средний
техногенные угрозы	сбои	средний
стихийные угрозы	пожары	низкий
стихийные угрозы	наводнения	низкий
стихийные угрозы	землетрясения	низкий
стихийные угрозы	др. форс-мажорные	низкий

Угрозы и уязвимости процедур

Блоки	Процесс	Уязвимости	Угрозы
1	**Регистрация**	**С**	**С**
1.1	Субъект ***предъявляет*** свои идентификаторы (удостоверения или ЭУ)	Н	С
1.2	ЦР ***проверяет*** предъявленные субъектом идентификаторы	С	В
1.3	ЦР ***создает*** учетную запись субъекта	Н	Н
1.4	ЦР ***регистрирует/создает*** секрет (аутентификатор) и ***издает*** ЭУ	Н	С
1.5	ЦР ***делегирует*** права доступа субъекта к другим ИС	Н	Н
1.6	ЦР ***выдает*** секрет и ЭУ на руки субъекту	Н	Н
2	**Подтверждение подлинности**	**С**	**С**
2.1	Субъект ***хранит*** секрет и ЭУ	С	В
2.2	Субъект ***предъявляет*** секрет и ЭУ доверяющей стороне (ДС)	С	С
3	**Валидация**	**Н**	**Н**
3.1	ДС ***проверяет*** цепочку сертификатов, срок и область действия ЭУ	Н	Н
4	**Принятие решения**	**Н**	**Н**
4.1	ДС ***принимает решение*** о результате аутентификации	Н	Н

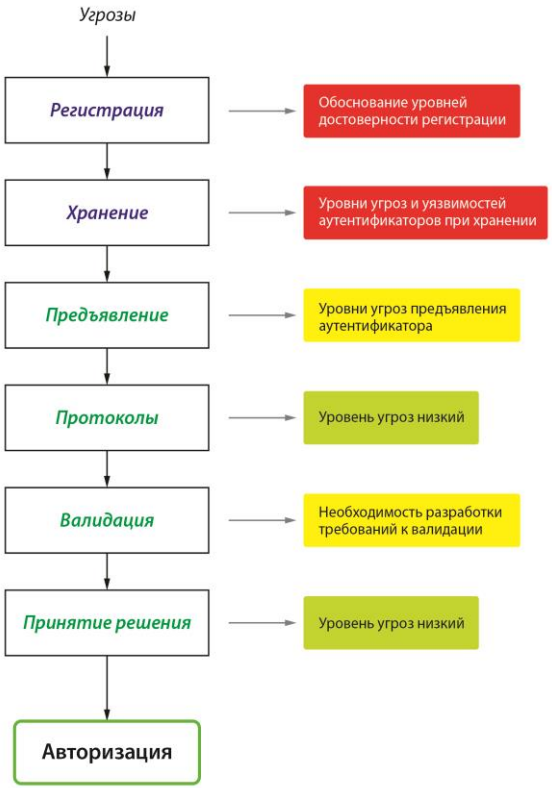
Угрозы и уязвимости предъявления АИ

Вид аутентификатора	**Уровень уязвимости**	**Уязвимость предъявления**	**Уровень угрозы**
Пароль	Высокий	Предъявляется в открытом виде	Высокий
Одноразовый пароль	Высокий	Предъявляется и передается по сети в открытом виде	Средний
Закрытый ключ в применяется в оперативной памяти компьютера	Средний	Закрытый ключ нуждается в средствах защиты, например, средствами ОС	Низкий
Процедура подписи производится внутри специально спроектированного чипа устройства SSCD (QSCD)	Низкий	Неизвлекаемость закрытого ключа гарантирована	Низкий

Уязвимости защиты ключа подписи

Способ формирования ключевого материала	Носитель ключевой информации	Уровень уязвимости	Уязвимость
Внешний CSP с последующим импортированием закрытого ключа на дискету	Дискета	Высокий;	Дискету легко скопировать
Внешний CSP с последующим импортированием закрытого ключа на носитель с памятью, защищенной PIN	Смарт-карта, USB-ключ	Средний	Для копирования надо знать или подобрать PIN-код
Формирование ключевого материала производится программно внутри памяти устройства, защищенной PIN-кодом	USB-ключ на основе бытового микроконтроллера	Средний	Закрытый ключ защищен только PIN –кодом и нуждается в дополнительных средствах защиты
Формирование ключевого материала производится аппаратно внутри специально спроектированного чипа устройства SSCD	SSCD (Secure Signature Creation Device)	Низкий	Неизвлекаемость закрытого ключа гарантирована международными и российскими сертификатами

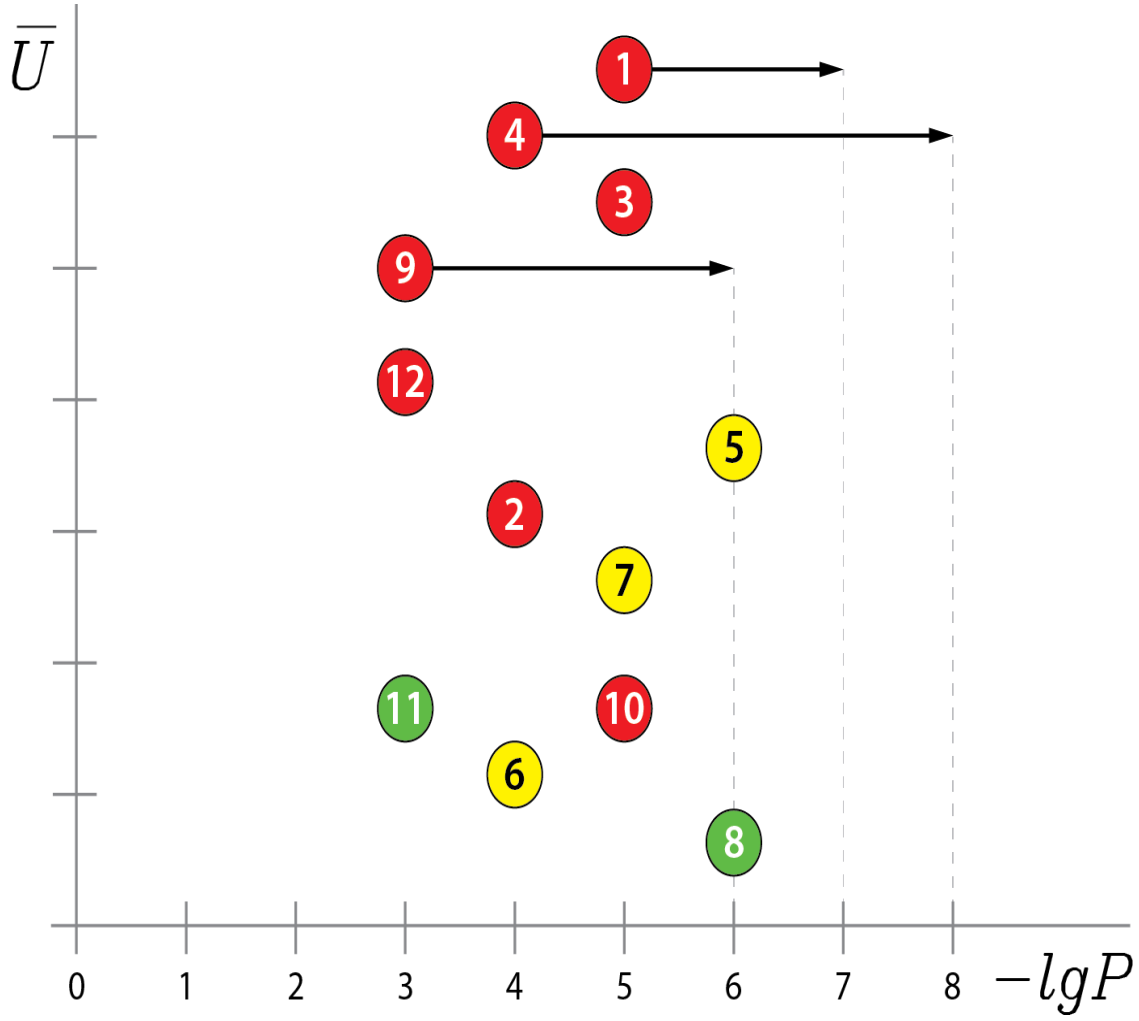
Итоги анализа угроз и уязвимостей



Идентификация опасных событий

PHE1	регистрация злоумышленника под видом легального польз.	$10^{-7} – 10^{-5}$
PHE2	использование уязвимостей СИА	$10^{-5} – 10^{-3}$
PHE3	помощь инсайдера	$10^{-6} – 10^{-4}$
PHE4	завладение злоумышленником АИ легального пользователя	$10^{-5} – 10^{-3}$
PHE5	атака "вход под принуждением"	$10^{-7} – 10^{-5}$
PHE6	ошибки или целенаправленные действия при смене АИ	$10^{-5} – 10^{-3}$
PHE7	ошибки валидации	$10^{-6} – 10^{-4}$
PHE8	ошибки в принятии решения "свой-чужой"	$10^{-7} – 10^{-5}$
PHE9	фишинг	$10^{-4} – 10^{-2}$
PHE10	spoofing - подмена доверенной стороны	$10^{-6} – 10^{-4}$
PHE11	риск добровольной передачи носителя ключа и АИ	$10^{-4} – 10^{-2}$
PHE12	воздействие вредоносного ПО	$10^{-4} – 10^{-2}$

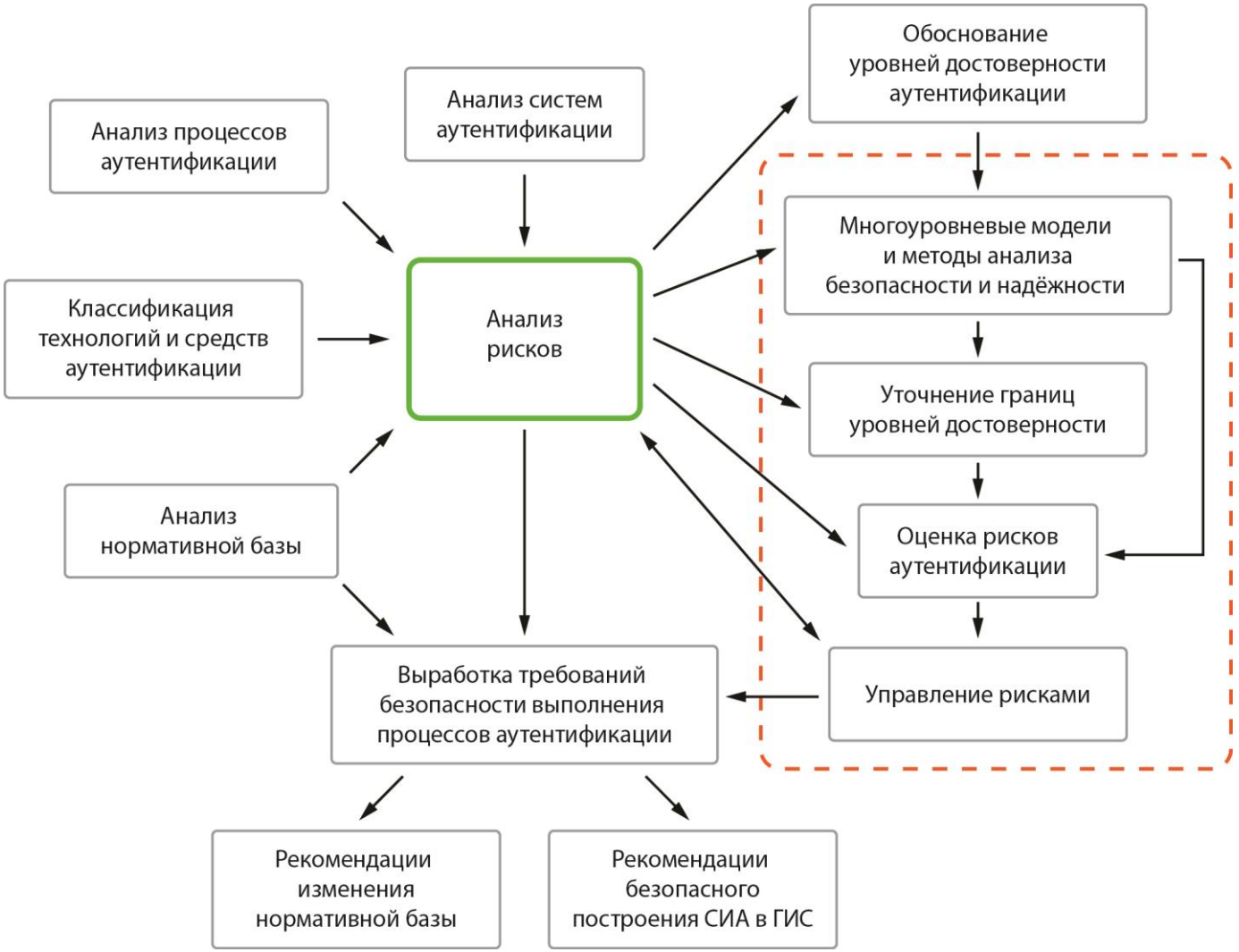
Пример управления рисками аутентификации



Ранжирование опасных событий

N	описание опасного события	частота (эксп.)
1	воздействие вредоносного ПО	$10^{-4} – 10^{-2}$
2	риск добровольной передачи носителя ключа и АИ	$10^{-4} – 10^{-2}$
3	фишинг	$10^{-4} – 10^{-2}$
4	ошибки или целенаправленные действия при смене АИ	$10^{-5} – 10^{-3}$
5	завладение злоумышленником АИ легального пользователя	$10^{-5} – 10^{-3}$
6	использование уязвимостей СИА	$10^{-5} – 10^{-3}$
7	ошибки валидации	$10^{-6} – 10^{-4}$
8	spoofing - подмена доверенной стороны	$10^{-6} – 10^{-4}$
9	помощь инсайдера	$10^{-6} – 10^{-4}$
10	регистрация злоумышленника под видом легального польз.	$10^{-7} – 10^{-5}$
11	атака "вход под принуждением"	$10^{-7} – 10^{-5}$
12	ошибки в принятиии решения "свой-чужой"	$10^{-7} – 10^{-5}$

Анализ рисков аутентификации



Некоторые результаты

Уровни достоверности (типы аутентификации)	доступность	целостность	конфиденциальность
Простая (пароль)	+	-	-
Усиленная (OTP)	+	-	-
Усиленная (несерт. X.509)	+	+	+
Строгая (X.509 выдан аккредитованным УЦ)	+	+	+

Рекомендации

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

Уровни 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

Проблемы идентификации

1. Отсутствие простых и понятных рекомендаций для работников, занимающихся идентификацией личности. Зачастую, идентификацией личности занимаются лица, не проходившие специальной подготовки. Они знают, что надо делать, но у них, как правило, нет четких инструкций, как делать. Действия, которые необходимо выполнить при проведении процедуры идентификации личности, описаны ниже в разделе «Предварительный проект типового Регламента идентификации личности уполномоченным сотрудником организации КФС».

2. Отсутствие возможности оперативной и достоверной проверки данных, предоставленных для идентификации.

3. Сложность проверки документа, удостоверяющего личность, на подлинность.

4. Отсутствие на рабочих местах функционала, позволяющего осуществить автоматизированную проверку соответствия фотографии в документе удостоверяющем личность с фотографией идентифицируемого лица (фото обратившегося, сканирование фото с паспорта, результат автоматизированной сверки в виде процента соответствия).

5. Низкий уровень персональной ответственности лица, осуществляющего идентификацию.

Способы идентификации

Внедрение программно-аппаратных комплексов, позволяющих производить проверку защитных признаков идентификатора (проверка защитных признаков идентификатора, например, паспорта – проверка в различных спектрах излучения, фотографирование идентифицируемого лица, с последующей автоматизированной сверкой полученной фотографии фотографией в паспорте);
Проверка биометрических данных заграничного паспорта;
Проверка нескольких идентификаторов (основной идентификатор - паспорт, дополнительные - водительское удостоверение, военный билет, заграничный паспорт и т.д.);
Проверка информации, указанной в предъявляемом идентификаторе посредством обращения к внешним источникам данных (реестры, регистры и т.д.);
Видеофиксация процедуры идентификации;
Проверка дееспособности идентифицируемого лица;
Внедрение принципа солидарной ответственности за проведение процедуры идентификации;
Выработка критериев качества идентификации (разработка процентной шкалы, позволяющей принимать решение о качестве идентификации).

Повышение ответственности

Доведение под роспись статей уголовного и иных кодексов, предусматривающих ответственность за не добросовестное исполнение служебных обязанностей, мошенничество. Разъяснение последствий нарушения установленной процедуры идентификации (объявление взыскания, лишение премии и т.д.);

Строгая регламентация действий, которые необходимо выполнить при проведении процедуры идентификации.

В зависимости от предоставленных документов и результатов проверки установить уровень доверия (например, низкий, средний и высокий) по утвержденным в зависимости от уровня рисков, например, финансовых операций.

Проект регламента

Запросить документ удостоверяющий личность.
Визуально проверить соответствие лица, изображенного на фотографии, с лицом обратившегося (при необходимости посмотреть на обратившегося несколько раз).
Проверить паспорт на сайте федеральной миграционной службы (Проверка по списку недействительных российских паспортов).
Проверить страницу с фотографией на предмет замены фотографии.
Попросить назвать данные, указанные в паспорте (например, адрес предыдущего места регистрации или уточнить дату и место рождения);
В случае возникновения сомнений, запросить еще один документ подтверждающий личность (водительское удостоверение, заграничный паспорт).
Зафиксировать в информационной системе паспортные данные и результат проверки паспорта.
Запросить иные документы при необходимости фиксации дополнительной информации об обратившемся.
Внести в информационную систему дополнительные сведения об обратившемся.
Сфотографировать обратившегося на веб-камеру.
Вывести на печать заявление, необходимое для получения соответствующей услуги.
Попросить обратившегося подписать заявление (фамилия имя отчество полностью собственноручно, подпись).
Сравнить подпись на заявлении с подписью в паспорте, результат сравнения зафиксировать в информационной системе.
Поставить на заявлении отметку о принятии, подпись.
Подписать сведения в информационной системе электронной подписью (электронная подпись должна находится на носителе с неизвлекаемыми ключами, для подписания необходимо два фактора, пин-код и скан отпечатка пальца).
Информирование руководителя подразделения о готовности к оказанию услуги, передача паспорта обратившегося руководителю подразделения.

Спасибо за внимание!