Методика оценки рисков безопасности аутентификации пользователя при применении ЭП

Рускрипто 25-27 марта 2014 г.

Алексей Сабанов

Зам. генерального директора

ЗАО «Аладдин Р.Д.»

План доклада

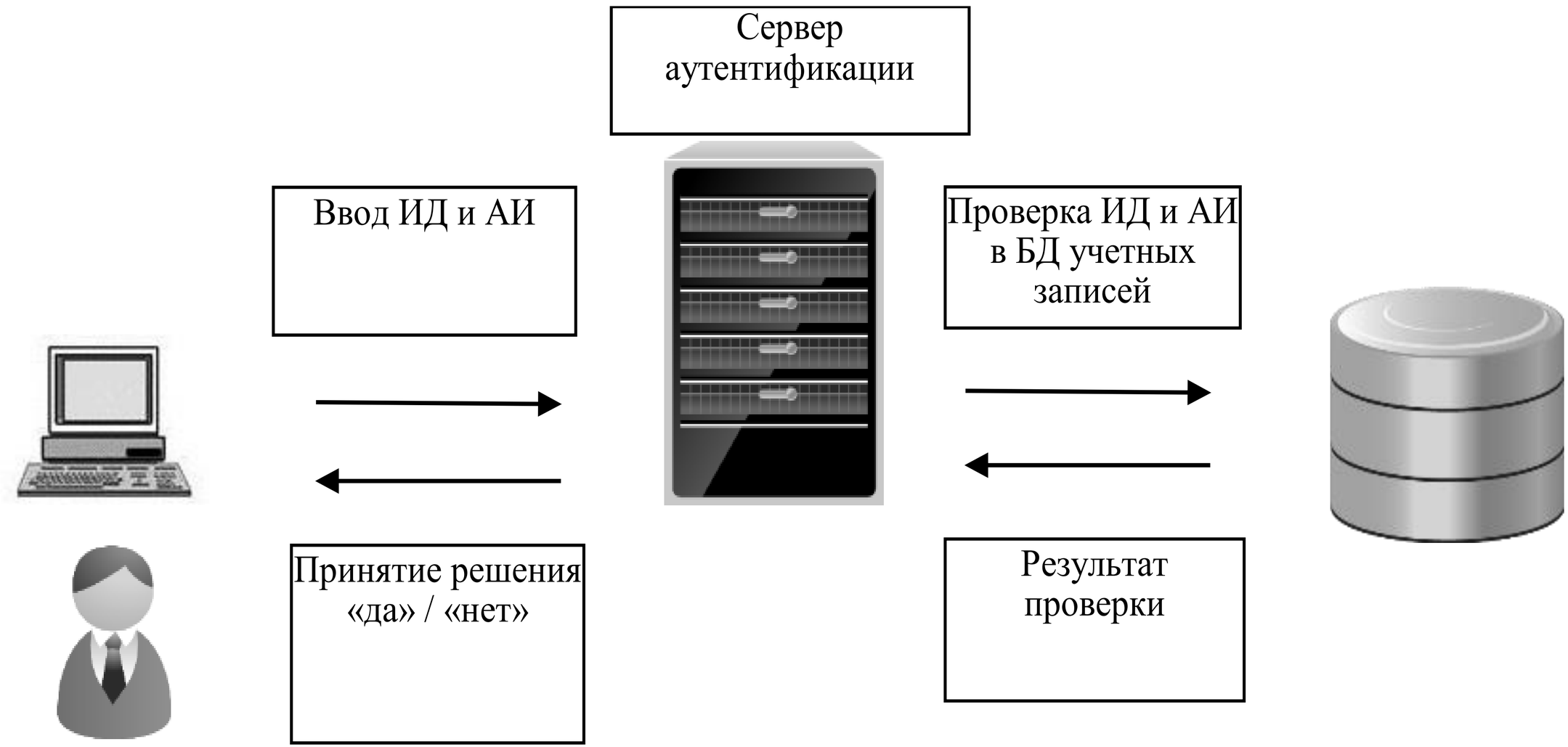
- Связь аутентификации и электронной подписи
- Методика оценка рисков
- Анализ угроз и уязвимостей аутентификации
- Анализ последствий и частоты
- Оценка рисков

Определения

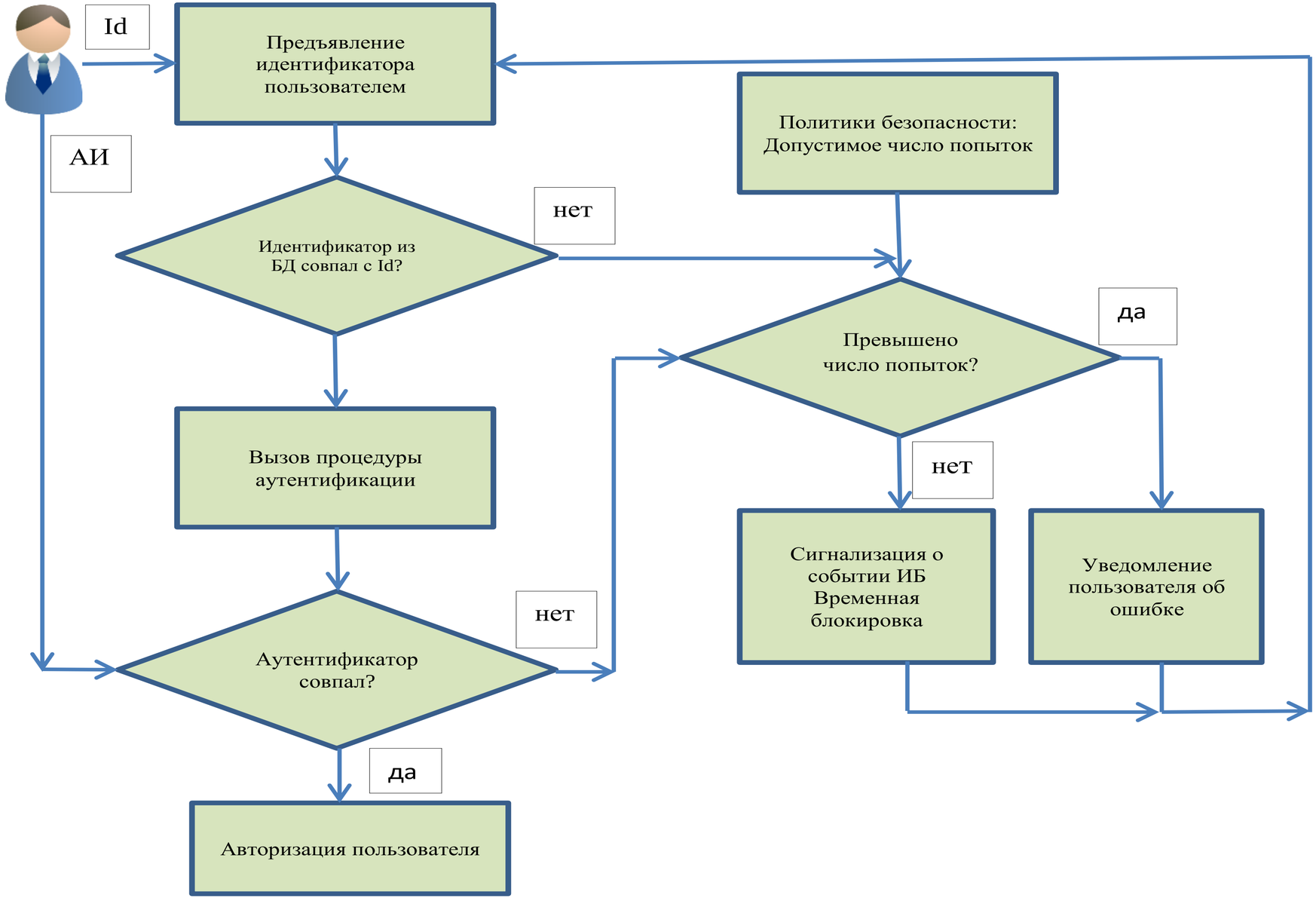
Идентификация – это сравнение идентификатора, вводимого участником информационного взаимодействия в любую из информационных систем, указанных в пункте 4 Требований (ПП-977от 28.11.2011г.), с идентификатором этого участника, содержащимся в соответствующем базовом государственном информационном ресурсе, определяемом Правительством Российской Федерации

Аутентификация – это процессы подтверждения подлинности предъявленных заявителем идентификаторов (идентификатора) и проверка принадлежности аутентификатора (секрета, который знают обе стороны взаимодействия или о существовании которого знают обе стороны взаимодействия)

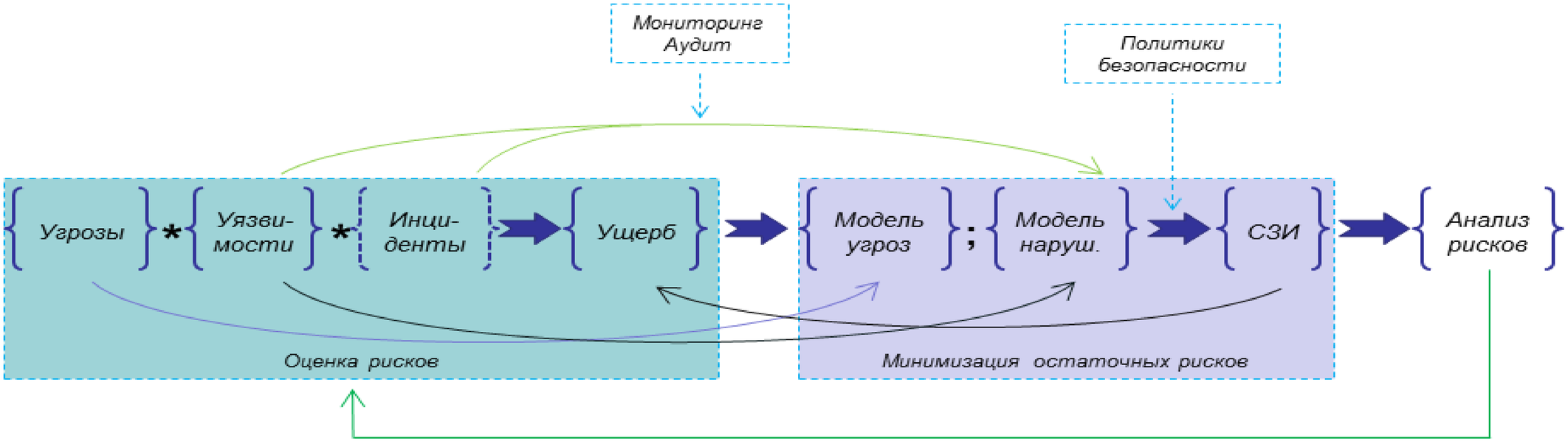
Схема проверки информации претендента



Блок - схема аутентификации



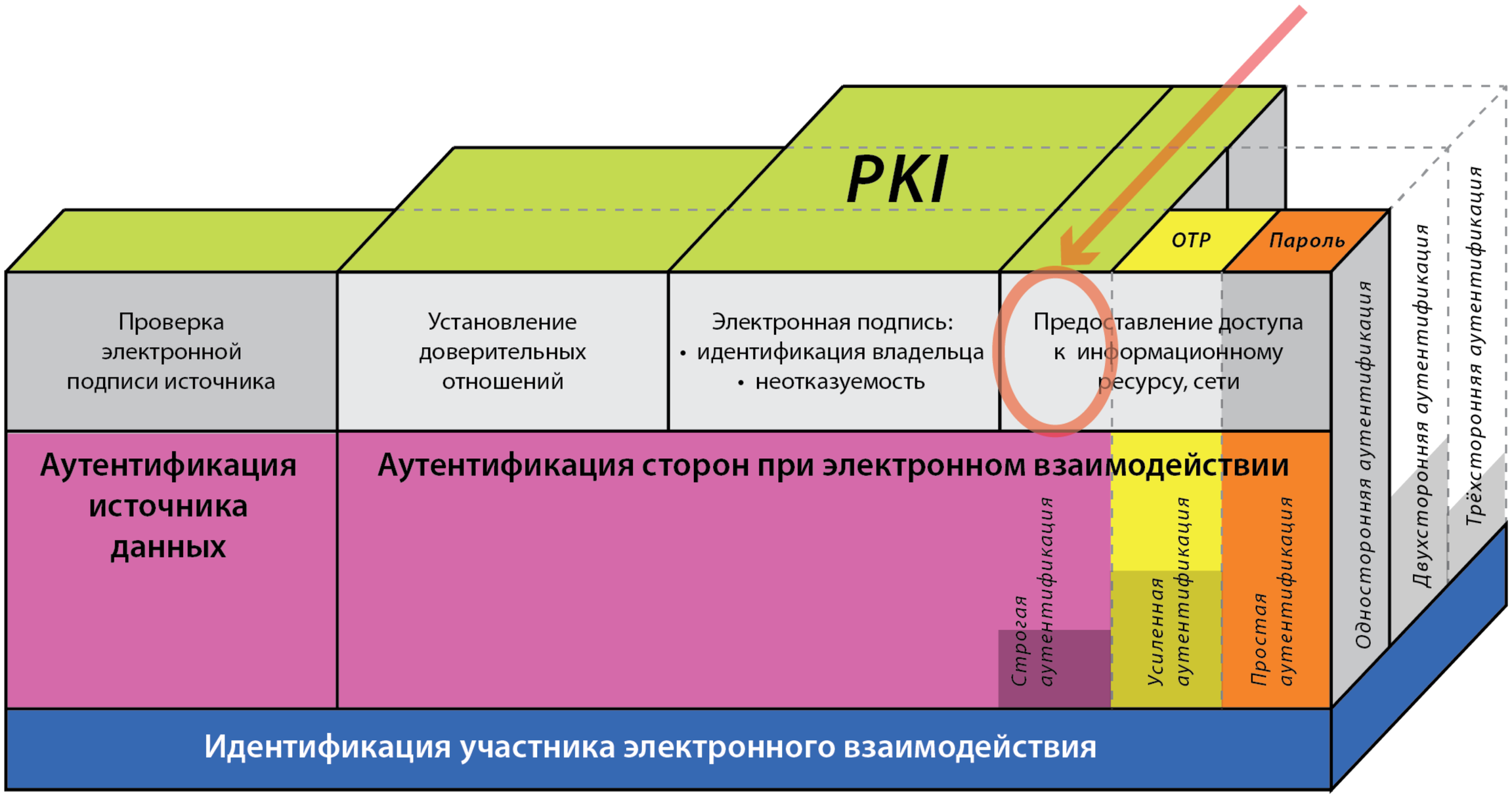
Стандартные методы оценки рисков



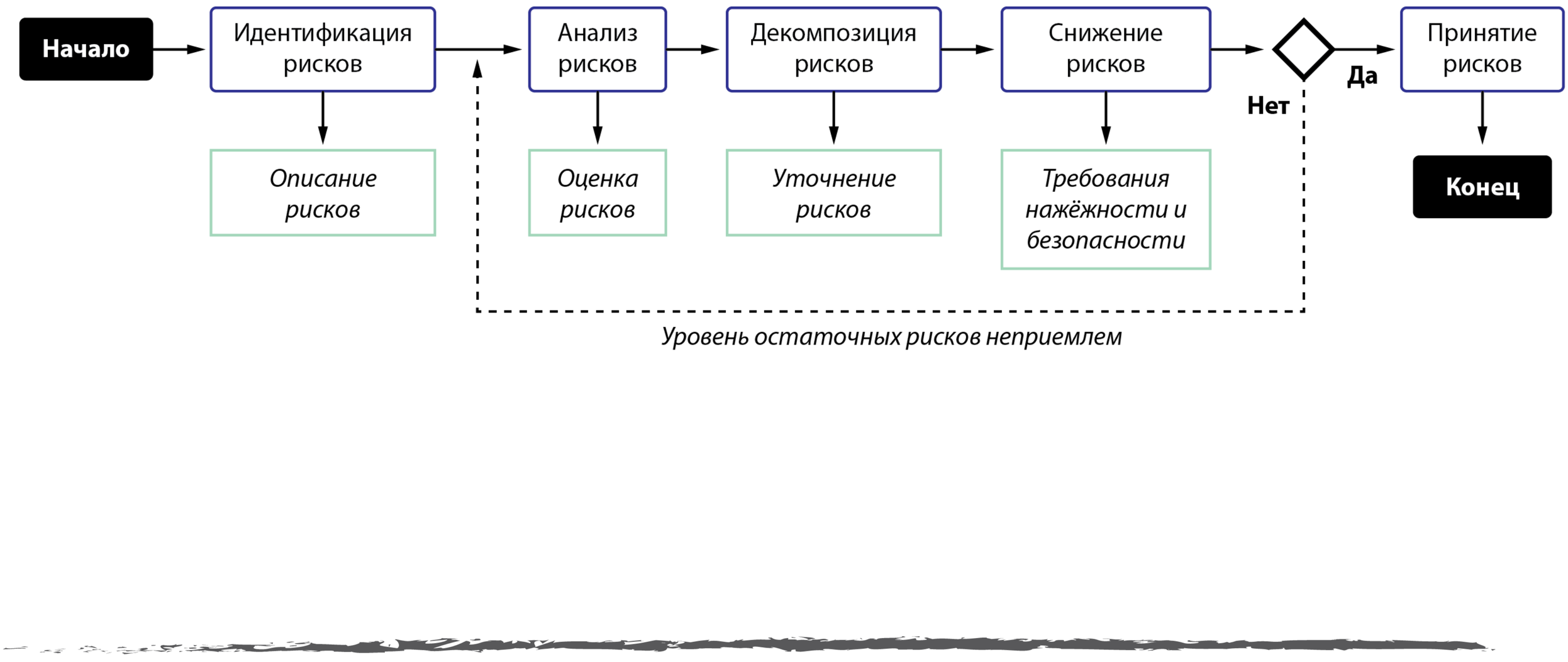
3 вида ЭП – 3 типа аутентификации

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

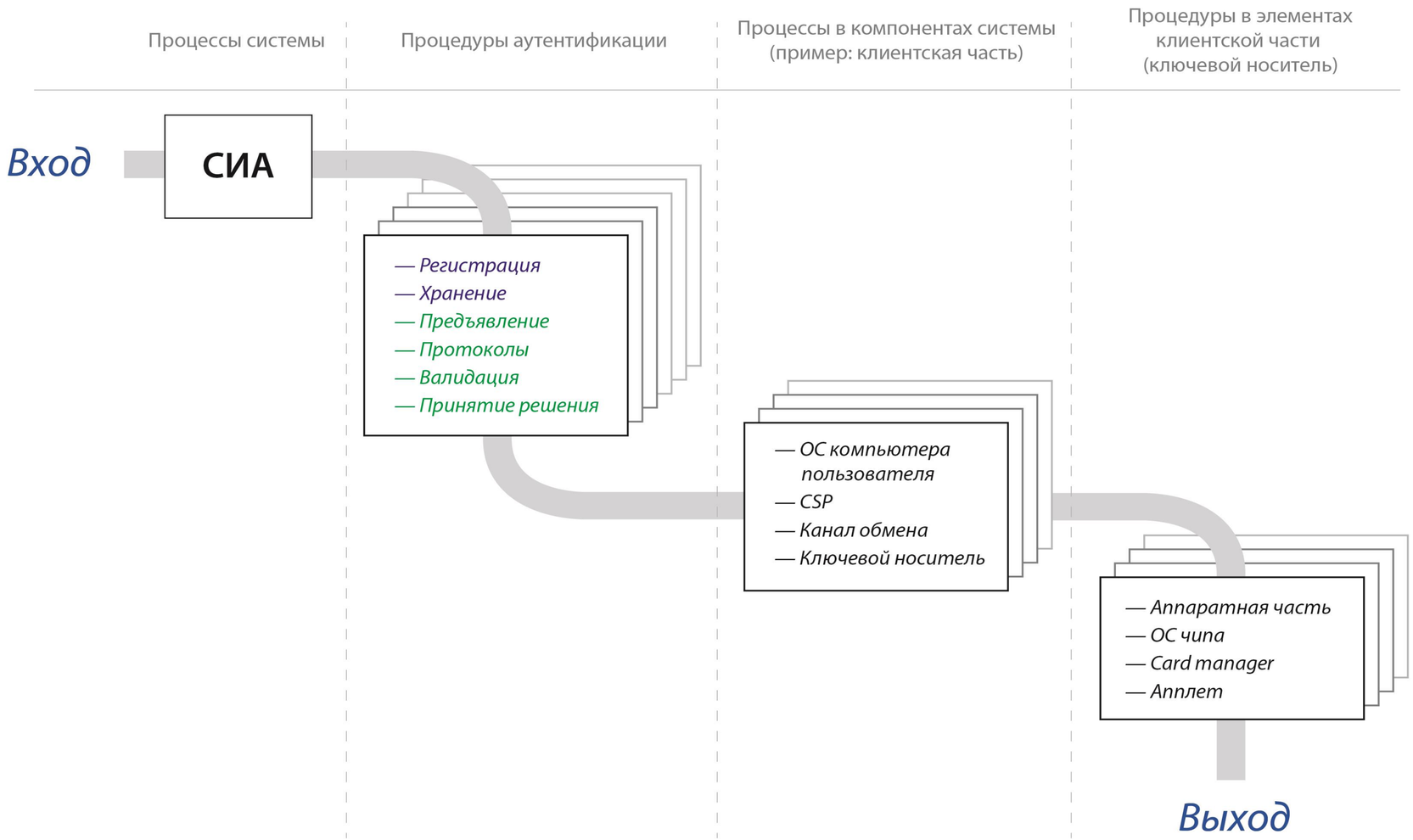
Связь аутентификации и ЭП



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	**Регистрациям**	**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

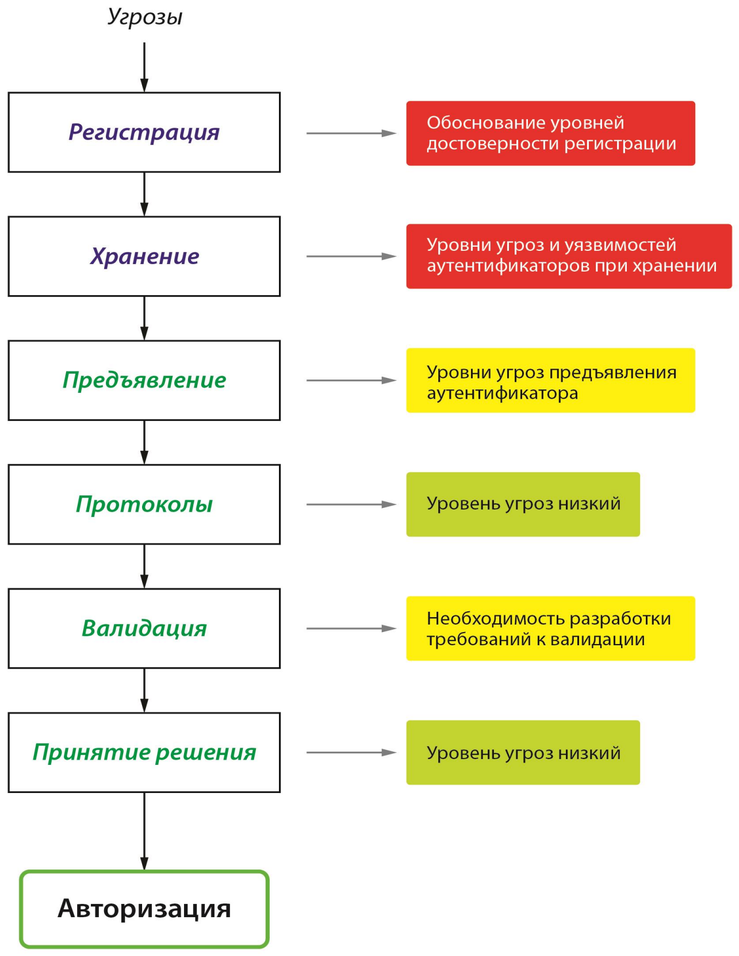
Угрозы и уязвимости предъявления АИ

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	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-кодом	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

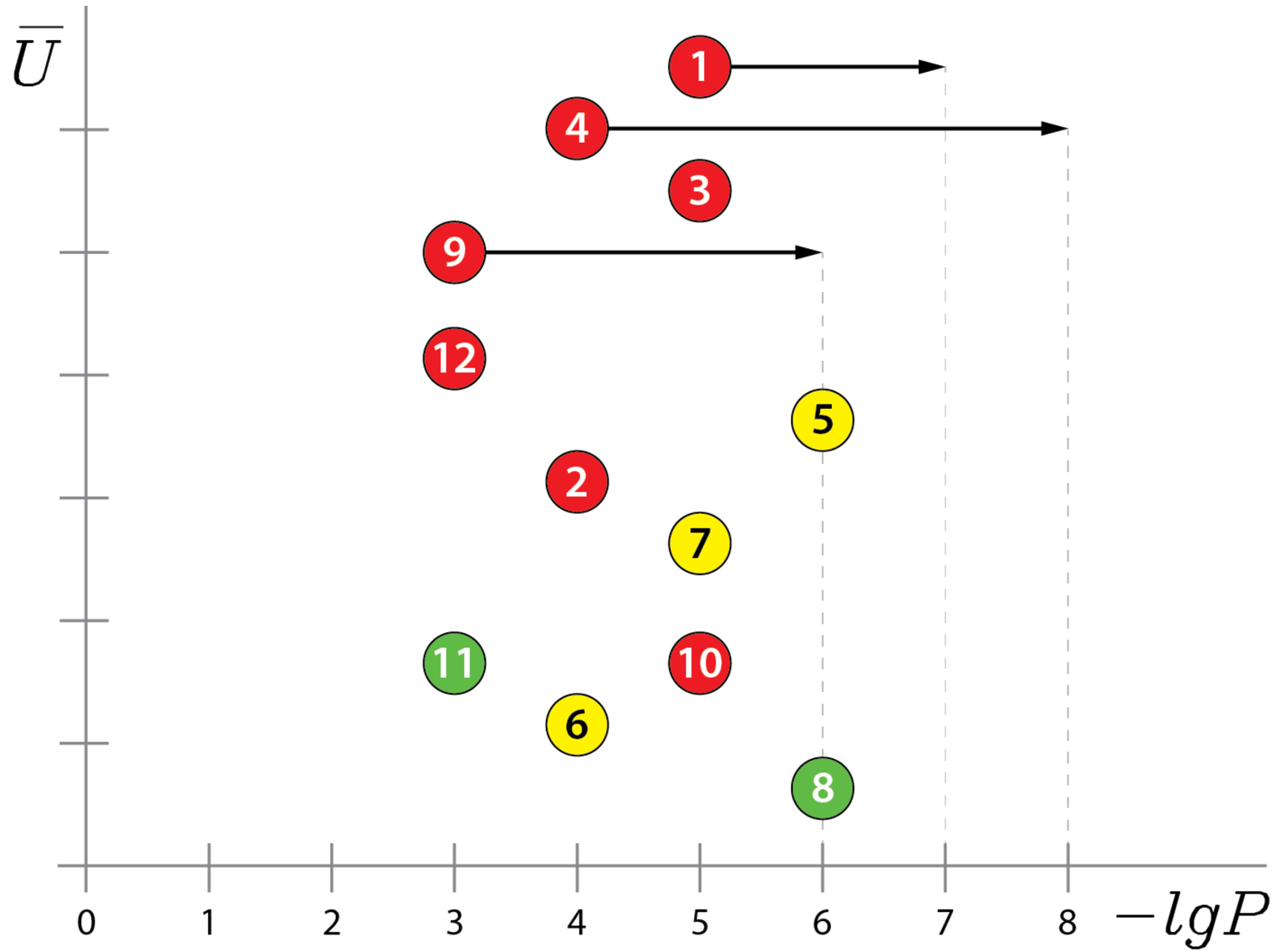
Итоги анализа угроз и уязвимостей



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	$10^{-4} – 10^{-2}$

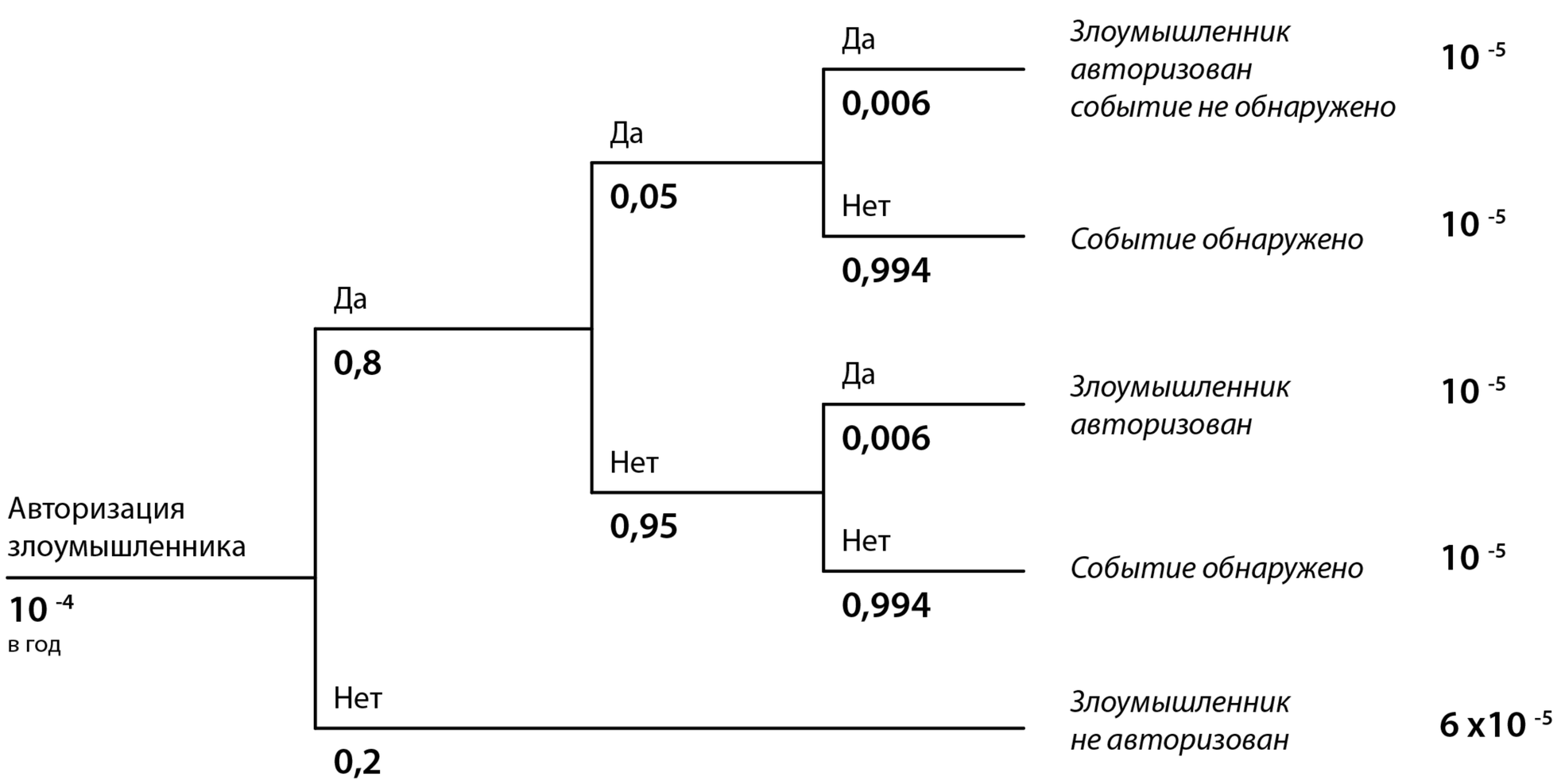
Пример управления рисками аутентификации



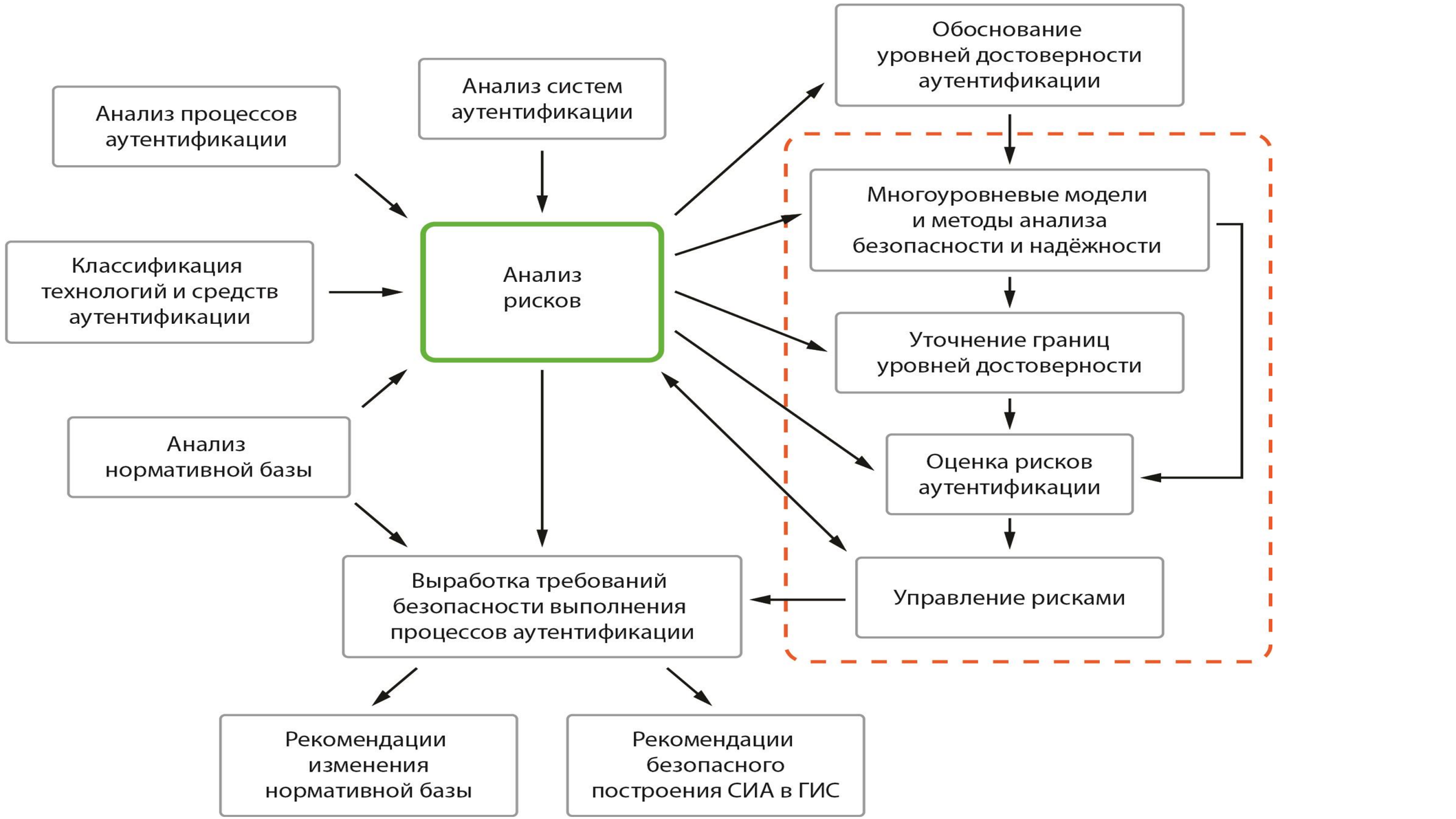
Ранжирование опасных событий

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"	$10^{-7} – 10^{-5}$

Пример анализа дерева событий



Анализ рисков аутентификации



Управление рисками

$VR = F_R\{C, P\} = \sum_i [F_R(C_i, P_i)]$

где VR – величина риска;

F_R - функционал, связывающий вероятность P возникновения события и математическое ожидание последствия (ущерба) C этого события;

P – вероятность (частота) возникновения события;

C – величина последствия возникновения события;

i – вид события. Сравнение с заданным уровнем риска.

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	+	+	+

Выводы

1. Вопросы безопасности и надежности процессов идентификации и аутентификации практически не регулируются, что не позволяет проводить оценку качества, безопасности и надежности сервисов идентификации и аутентификации.
2. Разработан метод исследования рисков аутентификации.
3. Наиболее критичными являются процессы регистрации, предъявления и хранения аутентификационной информации.
4. Необходимо введение уровней достоверности аутентификации.
5. Сформулированные выводы должны найти отражение в нормативной базе Российской Федерации по ИБ.

Спасибо за внимание!

Аладдин рд

a.sabanov@aladdin-rd.ru