Надежность идентификации и аутентификации

Алексей Сабанов, к.т.н.,
Генеральный директор НП СОИБ
Зам.ген. директора «Аладдин Р.Д.»
27 ноября 2013г.

Важность аутентификации в мире

- “is a key element for the delivery of any e-services.”
  - European Commission COM(2008) 798 final (28 Nov. 2008)

- “is a critical component of . . . national and global economic, governmental and social activities [which] rely more and more on the Internet.”
  - OECD, The Role of Digital Identity Management in the Internet Economy (June 2009)

- “is a one of the most important security service of e-commerce and e-government”

  APEC Guidance for E-commerce (December 2005)

Связь понятий надежности и безопасности

IDENTITY, CREDENTIAL, & ACCESS MANAGEMENT

- Since its creation in fall 2008, the Identity, Credential, and Access Management (ICAM) program has focused on addressing challenges, pressing issues, and design requirements for digital identity, credential, and access management and defining and promoting consistency across approaches for implementing ICAM programs as reflected in the FICAM Roadmap & Implementation Guidance (FICAM Roadmap). The FICAM Roadmap was developed to outline a common framework for ICAM within the Federal Government and to provide supporting implementation guidance for federal agencies as they plan and execute a segment architecture for ICAM management programs. Much of the work accomplished under the FICAM program is driven by the Identity, Credential, and Access Management Subcommittee (ICAMSC).

Документы

- 04.2006 - NIST Special Publication 800-63 Version 1.0.2 Electronic Authentication Guideline | Download
- Backend Attribute Exchange (BAE) Governance | Download
- Backend Attribute Exchange (BAE) Overview | Download
- Federal ICAM Identity Scheme Adoption Process | Download
- Federal ICAM Privacy Guidance for Trust Framework Assessors and Auditors | Download
- Federal ICAM Trust Framework Provider Adoption Process for Levels of Assurance 1, 2, Non-PKI 3 | Download
- Federated Physical Access Control System (PACS) Guidance | Download
- FICAM Roadmap and Implementation Guidance | Download
- Fingerprint Exception Handling Guidelines | Download
- GSA Memorandum Acquisitions of Products and Services for Implementation of HSPD-12 | Download
- GSA Memorandum Federal Child Care Center Workers Facility Access Credentialing | Download
- GSA Technical Supplement in support of OMB issued memorandum M-05-05 | Download
- Identity, Credential, and Access Management (ICAM) Roadmap Snapshot | Download
- Modernizing Federal Logical Access Control Systems (LACS) Brochure | Download
- Modernizing Federal Physical Access Control Systems (PACS) Brochure | Download
- NIST SP800-63 E-Authentication Guideline | Download
- OMB M-04-04 E-Authentication Guidance for Federal Agencies | Download
- OMB Memorandum dated October 6, 2011 Requirements for Accepting Externally-Issued Identity Credentials | Download
- OMB Memorandum M-05-05 Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services | Download
- Password/PIN Entropy Tool | Download
- SAML Identifier and Protocol Profiles for BAE | Download
- SAML Metadata Profile for BAE | Download
- Security Assertion Markup Language (SAML) Web Browser Single Sign-on (SSO) Profile | Download
- Trust Framework Provider Assessment Package Application | Download
- Источник: http://www.idmanagement.gov/identity-credential-access-management

Выполнение Директивы 12 Президента

- **HSPD-12 PURCHASING**
- Through HSPD-12 Purchasing, Government approved products and services are made available to federal agencies through GSA Schedules. The resources available on the GSA Schedules have pre-approved vendors and pre-registered rates.
- **SCHEDULE 70 & SINS**
- IT Schedule 70 is an acquisition vehicle under the Multiple Award Schedule (MAS) program that gives agencies direct access to commercial experts who are able to address the needs of the government IT Community through a series of Special Item Numbers (SINs). These SINs cover most of the general purpose commercial IT hardware, software, and services and should be used by agencies as needed to meet their mission objectives as well as ICAM initiatives.
- Special Item Number Series 132 6x is reserved for product lines needed to authenticate an individual for purposes of physical and logical access control, electronic signature, performance of e-Business transactions and delivery of Government services. Pursuant to Section 211 of the E-Gov Act of 2002, Cooperative Purchasing provides authorized State and local government entities access to information technology items offered through GSA's Schedule 70 and the Corporate contracts for associated special item numbers.
- **QUALIFICATION REQUIREMENTS**
- Qualification Requirements and Evaluation Procedures for Special Item Number 132 6x Series:
- Special Item No. 132 60 A-F Access Certificates for Electronic Services (ACES) Program.
- Special Item No. 132 61 Public Key Infrastructure (PKI) Shared Service Provider Program.
- Special Item No. 132 62 HSPD-12 Product and Service Components.
- **SIN 132-62**
- The Special Item Number (SIN) 132-62 has been established for products and services to implement the requirements of HSPD-12, FIPS 201, and associated NIST special publications. Vendors providing offers on SIN 132-62 must meet the qualification requirements for the category of product and service being offered. Vendors should follow evaluation procedures outlined in the CONOPS document when submitting qualification packages to: Daryl Hendricks, (703) 306-6367, daryl.hendricks@gsa.gov.
- **QUALIFICATION RESOURCES**
- Qualification requirements are established for the following HSPD-12 system components and categories on SIN 132-62:
- PIV Enrollment and Registration Services and Products.
- PIV Systems Infrastructure Services and Products.
- PIV Card Management and Production Services and Products.
- PIV Card Activation and Finalization Services and Products.
- PIV System Integration Services and Products.
- Additional forms needed for the qualification process:
- Evaluation Cover Sheet From Vendor submits as part of the application package.
- Failure Review Form Vendor submits when in disagreement

Нормативная база

- Declaration on Authentication for Electronic Commerce 7-9 October 1998
- CWA 14365 Guide of use of Electronic Signature. Jan.2003
- OMB Memorandum M-04-04 E-Authentication Guidance for Federal Agencies December 16, 2003 & OMB Circular A-130 2003
- Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors. August 27, 2004
- ISO/IEC 10181-2, ITU-T Rec/x.811 Теоретические основы аутентификации. 2004
- NIST Special Publication 800-63 April 2006 (РД по использованию е-аутентификации)
- OECD Recommendation on Electronic Authentication/2007
- FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors. March 2006, FIPS PUB 201-2. March 2011
- ETSI draft SR 000 000 v0.0.2 Rationalized Framework for Electronic Signature Standardization August 2011 & ETSI TS 1, 103173,…

Идентификация и аутентификация (ИА)

Процессный подход:

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

Процедуры ИА. Пример: 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.

Упрощенная схема аутентификации

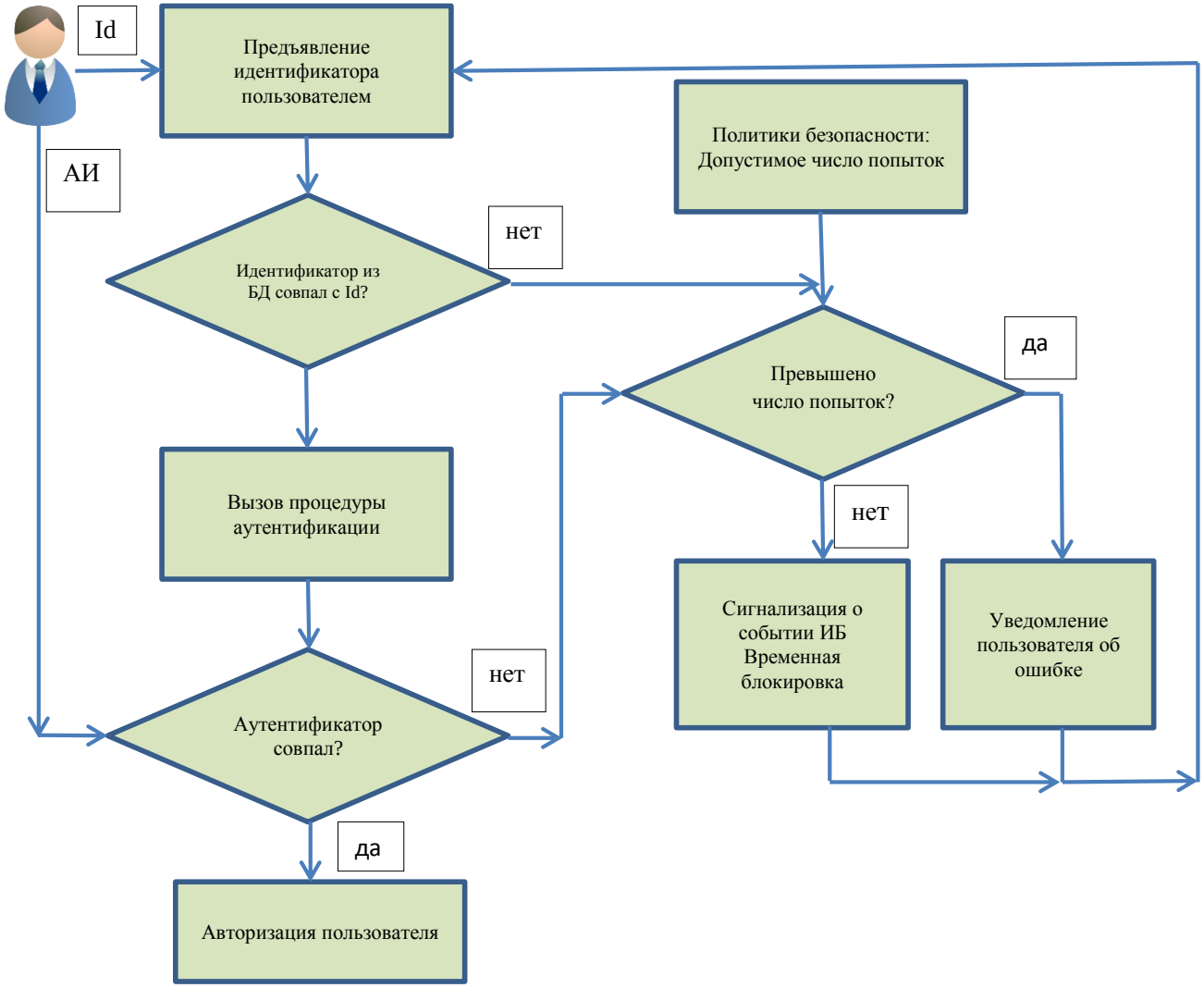
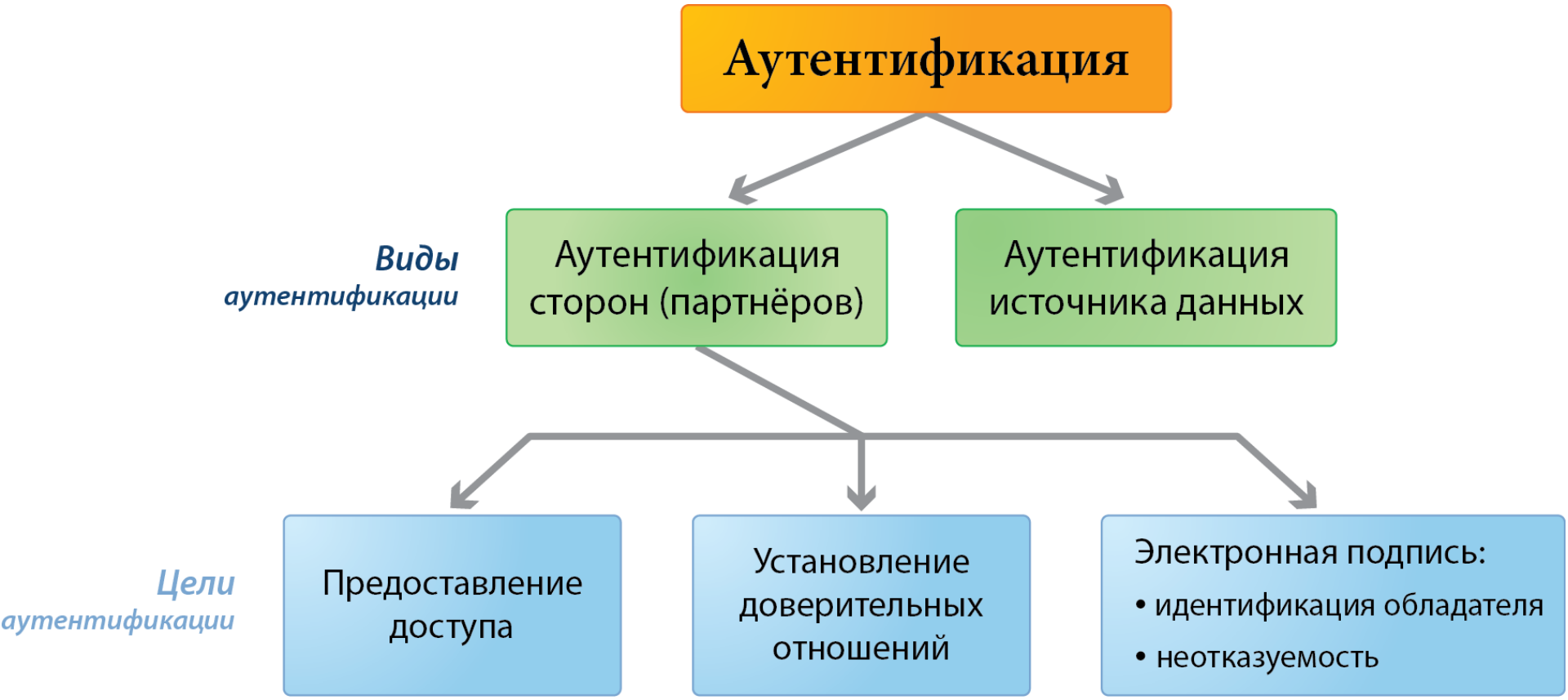


Схема обмена информацией из ITU Rec.X.811

Классификация средств идентификации и аутентификации

с точки зрения применяемых технологий

Классификация аутентификации по видам и целям

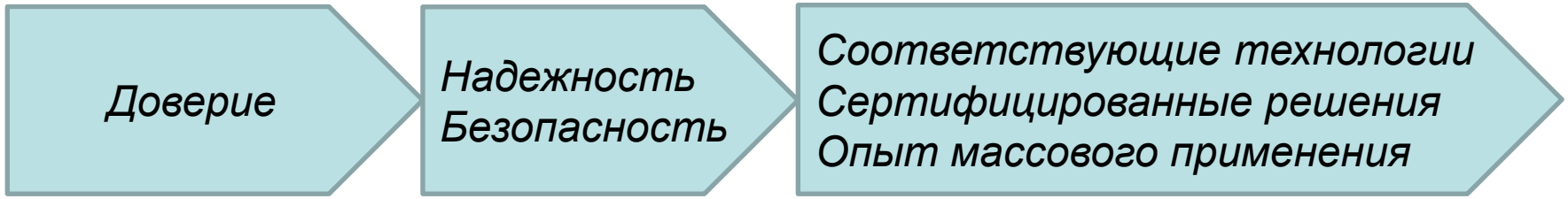


Три вида секрета, три типа аутентификации

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

Классификация аутентификации

Связь понятий



В конечном счете нас интересует качество ***доступа****, в том числе* ***качество аутентификации***

Методика анализа

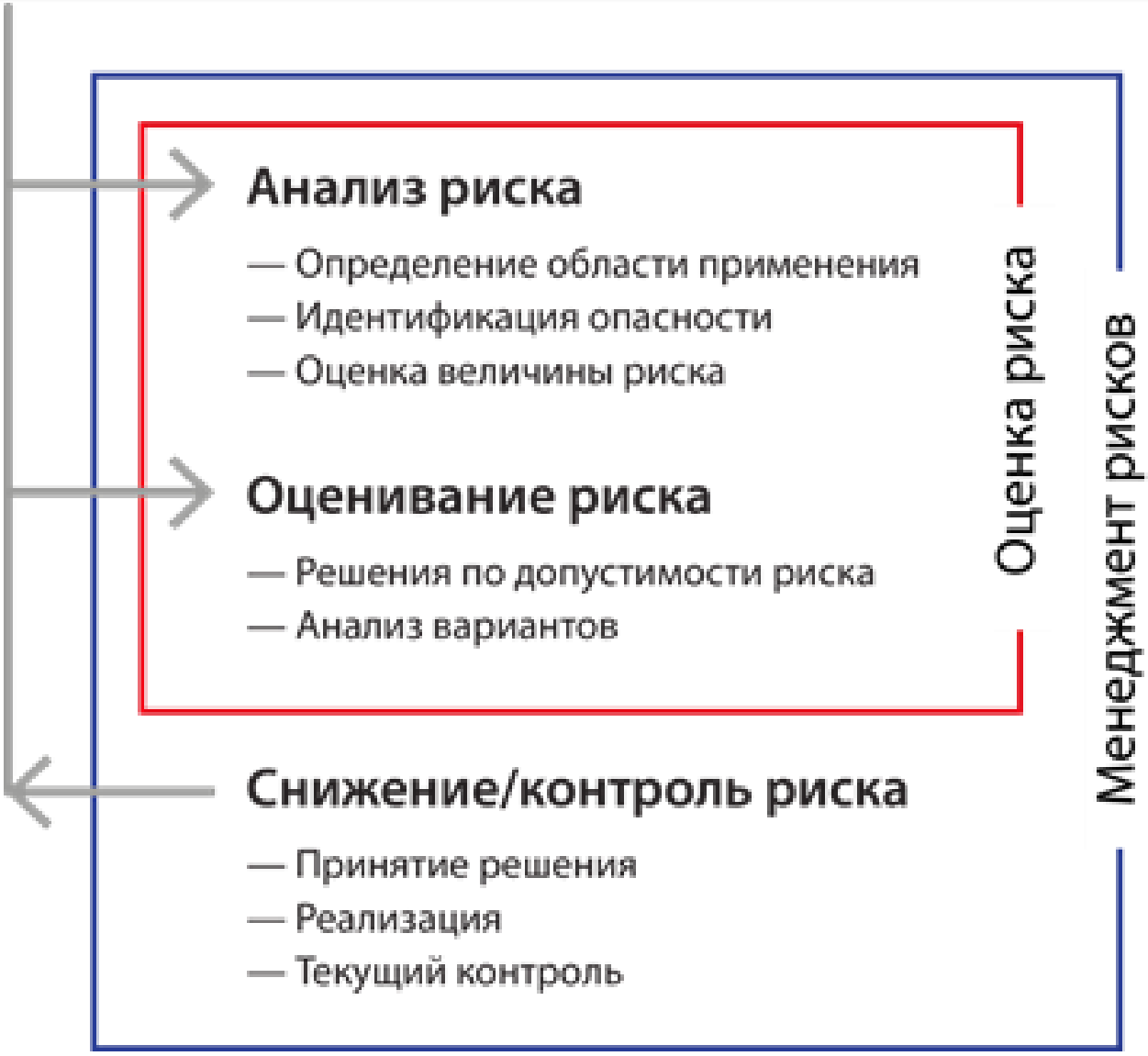
Классический подход оценки рисков:

1. Идентификация факторов опасности
2. Выявление угроз и уязвимостей
3. Оценка ущерба, вероятности его реализации и последствий
4. Оценка рисков, их снижение/контроль

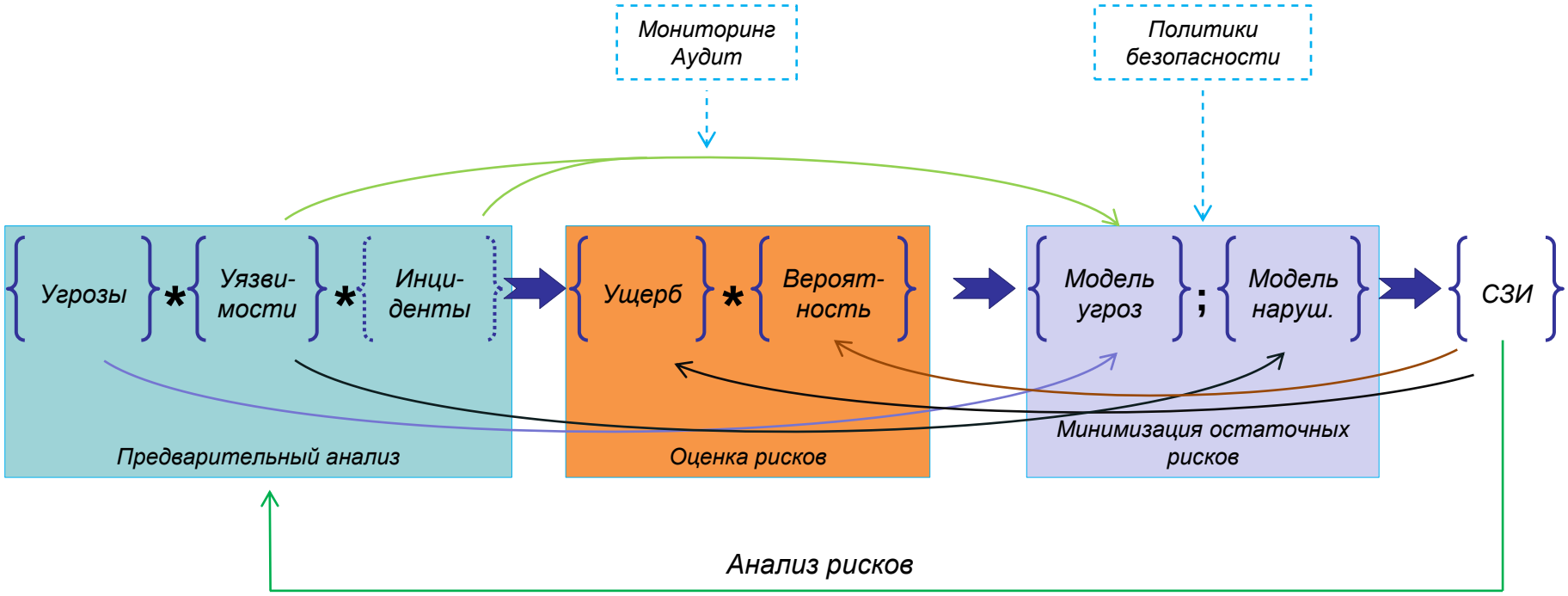
- Процессный подход
- Модели на основе применения Марковских процессов
- Оценка функциональной надежности и безопасности:

1. Матрица рисков
2. Метод построения дерева событий EMEA
3. Построение дерева отказов FTA аутентификации
4. Модели оценки вероятности безотказной работы
5. Методика оценки допустимого уровня рисков – связь с надежностью, качеством и безопасностью

Классический подход



Этапы работ по анализу рисков



Методы анализа рисков

- Качественные:
  - уровни рисков: низкий, средний, высокий;
  - ущерб невелик.
- Количественные:
  - предполагаемый ущерб значителен;
  - необходимость выбора наилучших средств защиты для минимизации ущерба или вероятности его реализации.
- Смешанные (гибридные)

Идентификация угроз

- Регистрация
  - «Маскарад» – имитация конкретного пользователя
  - Отрицание регистрации
- Токены (аутентификаторы: пароль, PIN-код, OTP,…)
  - Программные и физические ключевые носители может быть украдены или дублированы
  - Известное (PIN) может быть раскрыто злоумышленником
  - Обладаемое (отпечаток пальца) может быть скопировано
- Протоколы аутентификации
  - Подслушивание
  - Имитация (заявителя, проверяющей стороны, доверяющей стороны
  - Перехват сеанса аутентифицированного пользователя (обращение от имени пользователя к доверяющей стороне с целью получения конфиденциальной информации или ввода ложной информации)
  - Обращение от имени доверяющей стороны к проверяющей стороне с целью получения конфиденциальной информации или ввода ложной информации

Прочие угрозы

- Случайные и/или намеренные ошибки при издании Credentials, связывании, делегировании прав, создании учетных записей
- Злонамеренное ПО, направленное на компрометацию токенов (аутентификаторов)
- Вторжение в системы пользователей, CSP или проверяющих сторон с целью получения цифровых удостоверений или токенов
- Угрозы компрометации токенов со стороны инсайдеров
- Социальный инжиниринг с целью раскрытия пользователем PINa, подглядывание
- Атаки, при которых обманутый заявитель использует небезопасный протокол, думая, что использует безопасный, либо сам преодолевает средства защиты (например, принимая сертификаты серверов, не прошедших проверку)
- Явный отказ пользователей, сознательно скомпрометировавших свои токены

Оценка угроз и уязвимостей

	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	В	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	В	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

Оценка технического риска по Вилсону

Риск, связанный с рассматриваемым фактором опасности	=	*Серьезность возможного ущерба, который может быть нанесен рассматриваемым фактором опасности*	+	*Вероятность нанесения этого ущерба: частоты и продолжительности воздействия; вероятности наступления опасного события, возможности избежать или ограничить ущерб*

Wilson R. Simple Area Source Algorithm for Risk Assessment Screening. Memorandum to P. Cirrone, 1990

1. Процессный подход

	процесс	критичные операции	Сервер (С) или клиент(К)
1.	**Регистрация**		
1.1.	субъект ***предъявляет*** свои идентификаторы (удостоверения или ЭУ)	ошибки ввода данных	К
1.2.	ЦР ***проверяет*** предъявленные субъектом идентификаторы	ошибки проверки идентификации	С
1.3.	ЦР ***создает*** учетную запись субъекта	ошибки ввода данных	С
1.4.	ЦР ***регистрирует/создает*** секрет (аутентификатор) и ***издает*** ЭУ	вероятность мала	С
1.5.	ЦР ***делегирует*** права доступа субъекта к другим ИС	вероятность мала	С
1.6.	ЦР ***выдает*** секрет и ЭУ на руки субъекту	вероятность мала	
2.	**Подтверждение подлинности**		
2.1.	Субъект ***хранит*** секрет и ЭУ	критичная операция	К
2.2.	Субъект ***предъявляет*** секрет и ЭУ доверяющей стороне (ДС)	вероятность мала	К
3.	**Валидация**		
3.1.	ДС ***проверяет*** цепочку сертификатов, срок и область действия ЭУ	вероятность мала	С
4.	**Принятие решения**		
4.1.	ДС ***принимает решение*** о результате аутентификации	вероятность мала	С

Многоуровневое моделирование ИА

- Верхнеуровневая модель: представление системы ИА в виде одного целого элемента. Метод исследования – на основе аппарата систем массового обслуживания (СМО);
- Модель второго уровня: моделирование процедур, составляющих процесс ИА. Методы: СМО, методы оценки рисков, аппарат оценки надежности;
- Модель третьего уровня: модель операций, составляющих процедуры. Методы: оценки рисков, аппарат оценки надежности.
- Модель четвертого уровня: модели устройств, ПО,… Методы: вероятностно-статистические, аппарат оценки надежности.

Предварительные оценки

	процессы	миним	макс.
1.	**Регистрация**		
1.1.	субъект ***предъявляет*** свои идентификаторы (удостоверения или ЭУ)		
1.2.	ЦР ***проверяет*** предъявленные субъектом идентификаторы	0,87	0,99
1.3.	ЦР ***создает*** учетную запись субъекта	0,99	0,995
1.4.	ЦР ***регистрирует/создает*** секрет (аутентификатор) и ***издает*** ЭУ	0,99	0,995
1.5.	ЦР ***делегирует*** права доступа субъекта к другим ИС	0,99	0,995
1.6.	ЦР ***выдает*** секрет и ЭУ на руки субъекту	0,9	0,995
2.	**Подтверждение подлинности**	1	1
2.1.	Субъект ***хранит*** секрет и ЭУ	0,43	0,995
2.2.	Субъект ***предъявляет*** секрет и ЭУ доверяющей стороне (ДС)	0,94	0,995
3.	**Валидация**	1	1
3.1.	ДС ***проверяет*** цепочку сертификатов ЭУ	0,8	0,9
3.2.	ДС ***проверяет*** срок действия ЭУ	0,99	0,995
3.3.	ДС ***проверяет*** действенность ЭУ	0,99	0,995
3.4.	ДС ***проверяет*** область действия	0,99	0,995
4.	**Принятие решения**	1	1
4.1.	ДС ***принимает решение*** о результате аутентифкации	0,99	0,995
	интегральный условный показатель надежности	0,236	0,8474

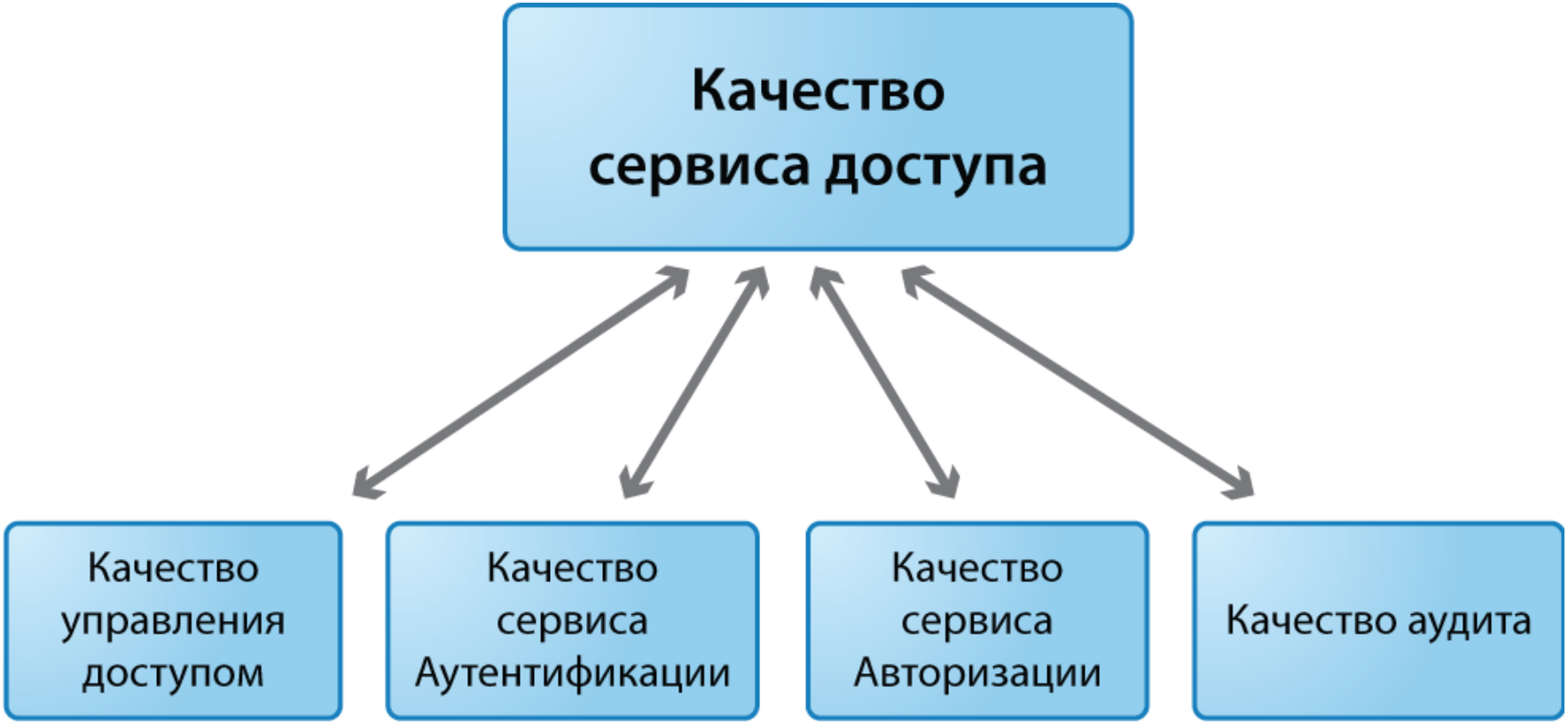
Качество сервиса аутентификации

- ГОСТ Р ИСО 9000-2008: качество (*quality*) - степень соответствия совокупности присущих характеристик некоторым требованиям.

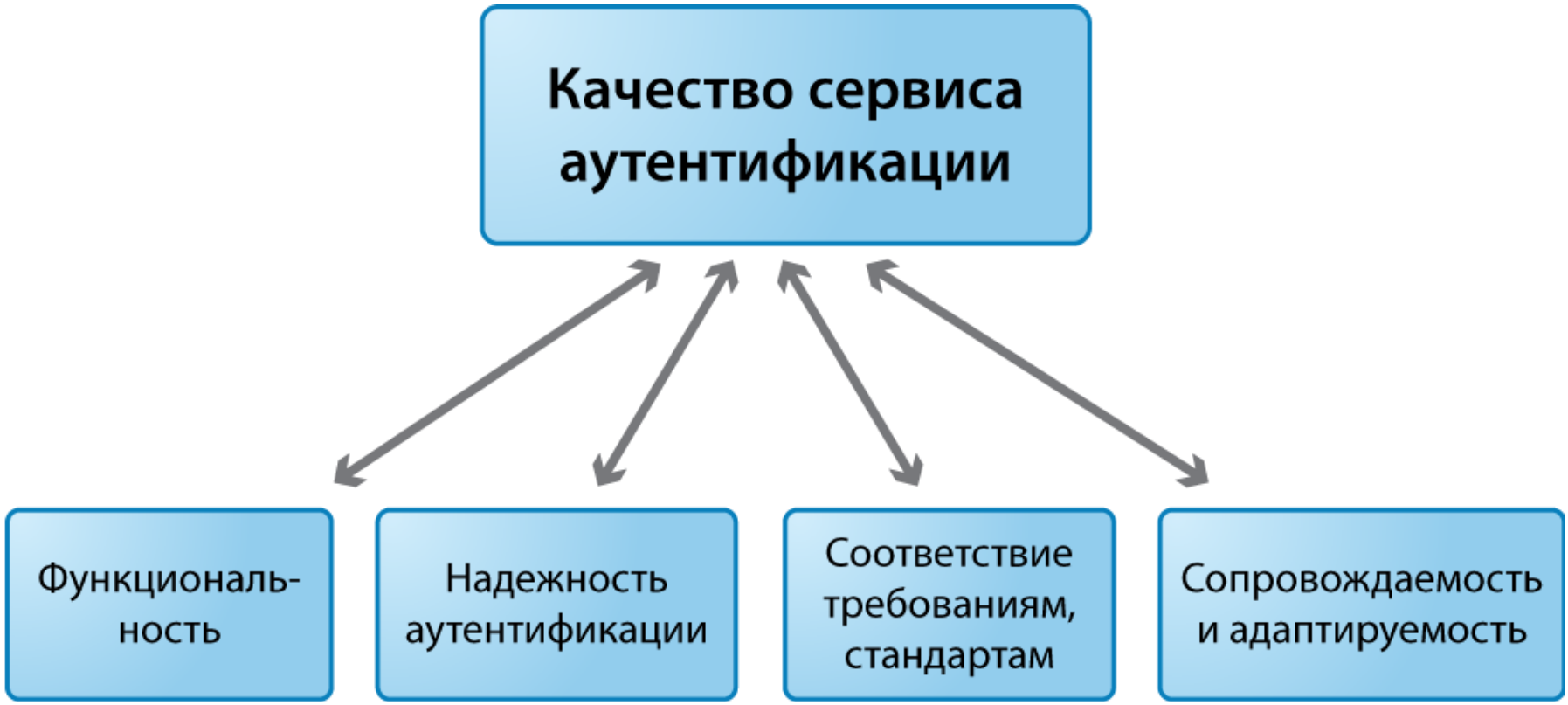
Семинар ТС56 МЭК (Лондон,2006г.)

Качество → соответствие стандартам → гарантии качества → страхование

Доступность услуг и облачных сервисов



Аутентификация – доверенный сервис

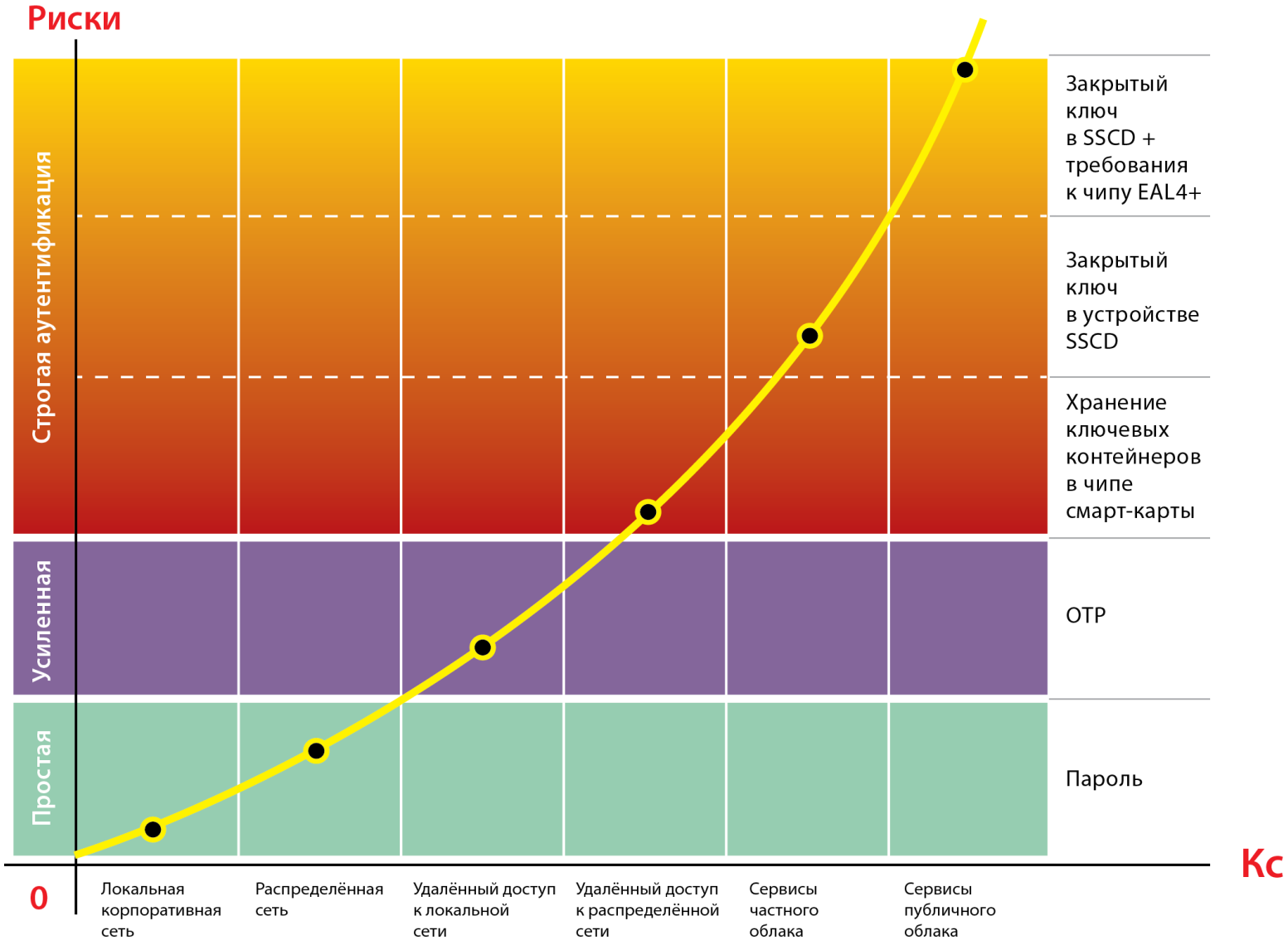


Развитие требований

Три уровня надежности ИА в РФ

- Низкий уровень надежности процессов ИА. Основной аутентификатор – пароль.
- Средний уровень надежности. Основной аутентификатор:
  - OTP;
  - цифровой сертификат X.509 доступа, выданный неаккредитованным удостоверяющим центром.
- Высокий уровень надежности аутентификации. Сертификат доступа от аккредитованного УЦ. Требования к аутентификатору:
  - Хранение контейнеров ключевого материала в защищенном PIN-кодом от копирования чипе;
  - Применение SSCD (Secure Signature Creation Device);
  - SSCD с повышенными требованиями: EAL4+

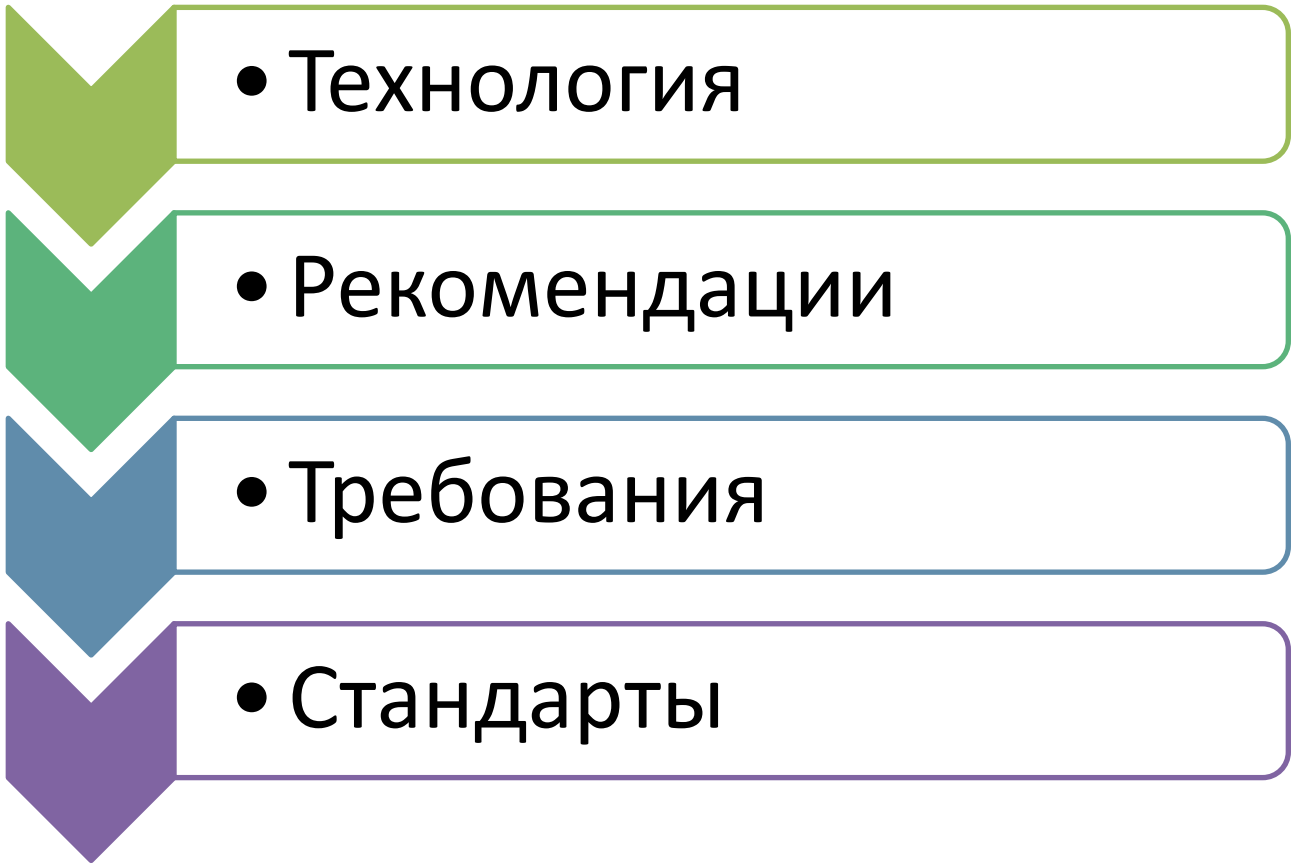
Качественные интегральные показатели



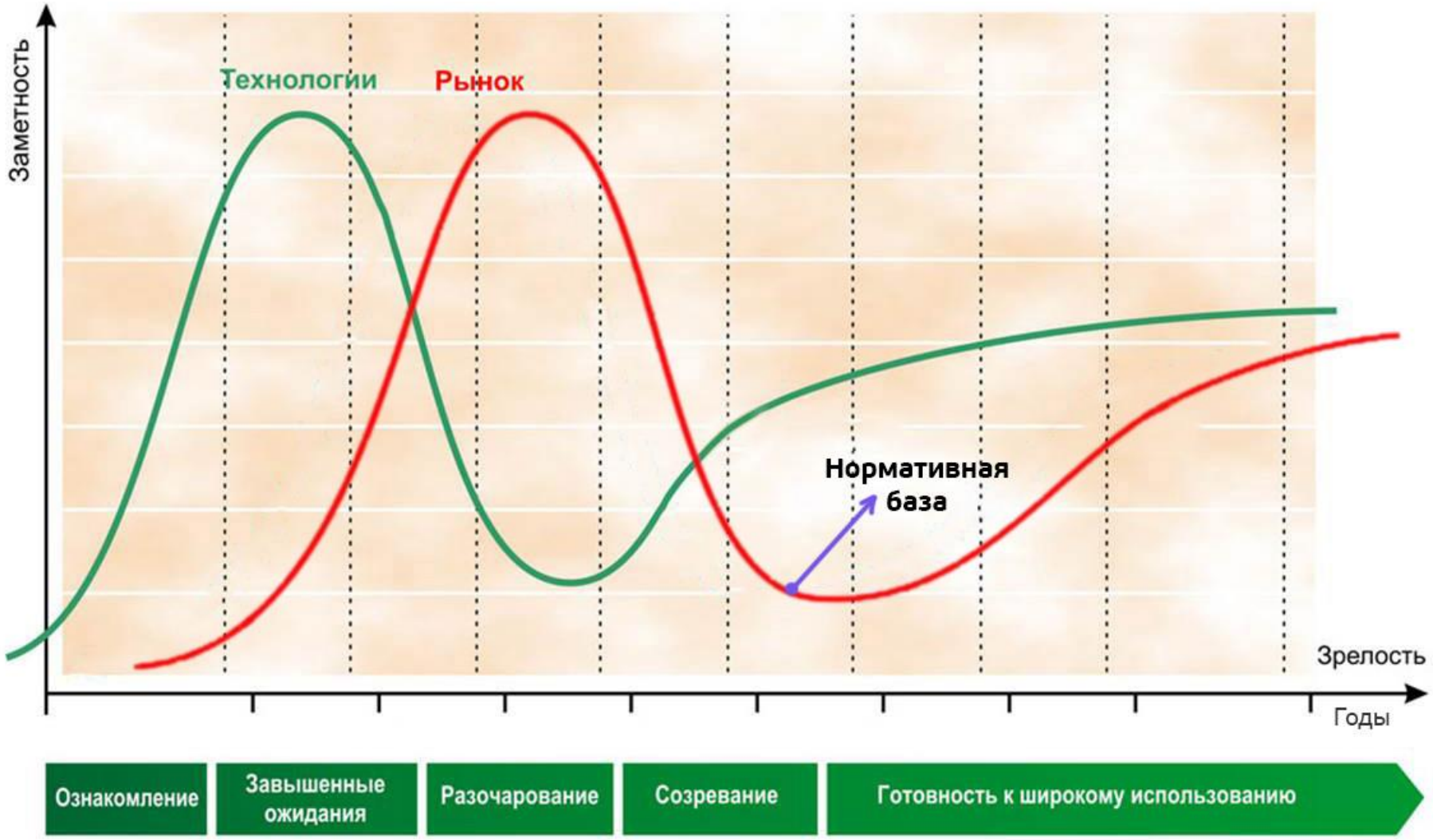
Выводы

- Анализ зарубежного опыта показывает, что исторически первыми требования к аутентификации для доступа разработаны в США. Канада, Австралия и ряд других стран повторяют и лишь локализуют требования США, которые являются наиболее проработанными.
- Российская нормативная база существенно отстает от развитых стран. Следовательно, необходимо интенсивно поработать, чтобы сократить отставание.
- Самой большой проблемой существующей и планируемой к опубликованию российской нормативной базы является полная независимость от технологий.
- Представленный подход может лечь в основу научной основы разработки нормативных требований к созданию надежных систем аутентификации.

Диалектика развития стандартов



Технологии и их внедрение



Аладдин РД

Спасибо за внимание!

a.sabanov@aladdin-rd.ru