Нормативно-правовое обеспечение деятельности в рамках создания государственной информационной инфраструктуры электронного правительства в РФ. Проблемы и пути решения

Алексей Сабанов, к.т.н.,

генеральный директор НП «СОИБ»

Зам. ген. директора ЗАО «Аладдин Р.Д.»

Классификация видов аутентификации

Сайт Правительства США

(ICAM) program has focused on addressing challenges, pressing issues, and design requirements for digital idSince its creation in fall 2008, the Identity, Credential, and Access Management entity, 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).

Директивные документы

- Директива 1999/93/EC "Об общих условиях использования электронных подписей" (1999 г.) – унификация правил использования ЭП и формулировка условий, необходимых для признания юридической равнозначности собственноручной и ЭП
  - Рекомендовано использование SSCD-устройств
- 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.
- Проект Регламента ЕС об электронной идентификации и доверенных службах на внутреннем рынке, 2012
  - Регламент будет обязателен для стран ЕС с весны 2014г.
  - Использование SSCD-устройств вводится в обязательном порядке

Международные рекомендации

- ISO/IEC 10181-1, ITU-T Rec. X.810 Теоретические основы обеспечения безопасности, 2004.
- SO/IEC 10181-2, ITU-T Rec. x.811 Теоретические основы аутентификации, 2004.
- OECD Recommendation on Electronic Authentication, 2007.
  - 3 уровня рисков – 3 уровня достоверности аутентификации, рекомендованы SSCD
- Framework for Secure Signature Devices Cross-border Recognition (CROBIES). Финальный отчет Европейской комиссии, 2010.
- ETSI draft SR 000 000 v0.0.2 Rationalized Framework for Electronic Signature Standardization August 2011
- ETSI TS 1, 103173, …(ряд драфтов документов – всего 9 шт.)
- OECD. Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy – Guidance for Government Policy Makers/ OECD Digital Economy Papers, No 196, OECD Publishing at p.3, 2011.

Стандарты аутентификации

- **FIPS 196**, "Entity authentication using public key cryptography," Federal Information Processing Standards Publication 196, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1997. (Аутентификация субъекта на основе криптографии открытых ключей).
- **ISO/IEC 9798-1: 1997**, Information technology – Security techniques- Entity authentication - Part 1: General. (Аутентификация субъекта. Часть 1).
- **ISO/IEC 9798-3: 1997**, Information technology – Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques. (Аутентификация субъекта. Часть 3. Механизмы, использующие технологии цифровой подписи).
- **FIPS PUB 201-1** Personal Identity Verification (PIV) of Federal Employees and Contractors. March 2006, **FIPS PUB 201-2. March 2011.**

Специальные публикации NIST

- **NIST SP-800-30** Руководство по управлению рисками ИБ. Июль, 2002.
- **NIST SP-800-33** Технические модели, лежащие в основе безопасности информационных технологий. Дек., 2001.
- **NIST SP-800-35** Руководство по управлению сервисами ИБ. Окт., 2003.
- **NIST SP-800-37** Управление рисками ИБ в федеральных организациях. Фев., 2010.
- **NIST SP-800-63** Рекомендации по электронной аутентификации. Апр., 2006.
- **NIST SP-800-103** Онтология электронных удостоверений. Окт., 2006.
- **NIST SP-800-118** Руководство по управлению паролями. Апр., 2009.
- **NIST SP-800-53A** Руководство по управлению ИБ в ГИС. Июнь, 2010.

CEN Workgroup Agreements

CWA 14167-1/4 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures. July 2003 (CWA 14167-1) – May 2004 (CWA 14167-4).

CWA 14168 Secure Signature - Creation Devices “EAL 4+” July 2001.

CWA 14169 Secure Signature - Creation Devices “EAL 4+” March 2004.

CWA 14170 Security Requirements for Signature Creation Applications. May 2004.

CWA 14172-1/8 EESSI Conformity Assessment Guidance. March 2004.

CWA 14355 Guidelines for the implementation of Secure Signature-Creation Devices. March 2004.

CWA 14365-1/2 Guide of use of Electronic Signature. Jan.2003.

CWA 14890-1/2 Application Interface for smart cards used as Secure Signature Creation Devices. May 2004.

Государственные программы

- 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
- Trust Framework Provider Assessment Package Application | Download

Источник: http://www.idmanagement.gov/identity-credential-access-management

Проблема терминологии в РФ

Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности	Руководящий документ «Защита от НСД к информации. Термины и определения», Утверждено решением председателя Гостехкомиссии России от 30.03.1992 г.
Аутентификация отправителя данных	Подтверждение того, что отправитель полученных данных соответствует заявленному	«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г.
Аутентификация участников информационного взаимодействия (в ЕСИА)	Проверка принадлежности участнику информационного взаимодействия введенного им идентификатора, а также подтверждение подлинности идентификатора	Постановление Правительства РФ от 28.11.2011 г. № 977 "О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме"
Аутентификация сведений об участниках информационного взаимодействия (сведений об их информационных системах)	Проверка, в том числе с использованием квалифицированных сертификатов ключей проверки электронных подписей, принадлежности участнику информационного взаимодействия или его информационной системе введенного им идентификатора, а также подтверждения подлинности идентификатора;	Постановление Правительства РФ от 10.07.2013 г. № 584 «Правила использования федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме"»

Нормативные документы РФ

- Федеральный закон от 15.12.2002 № 65-ФЗ "О техническом регулировании";
- Федеральный закон от 06.04.2011№ 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 27.07.2006 № 149 "Об информации, информационных технологиях и защите информации";
- Федеральный закон от 27.07.2011 "Об организации предоставления государственных и муниципальных услуг";
- ПП РФ от 28 ноября 2011 г. № 977 "О федеральной государственной информационной системе "ЕСИА в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме« ;
- Распоряжение Правительства РФ от 19.09.2013 №1694-Р "Об утверждении Концепции введения в РФ удостоверения личности гражданина в виде пластиковой карты с электронным носителем информации"

Нормативные документы ФСТЭК России

- РД Гостехкомиссии. Несанкционированный доступ к информации»:
  - п 6.3. Обеспечивающие средства для СРД выполняют следующие функции: идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта";
- ……
- Приказ ФСТЭК от 11.02.2013 № 17 "Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных ИС" :
  - орг. и тех. меры должны обеспечивать ИА субъектов доступа к объектам доступа;
- Проект методического документа "Меры защиты информации в государственных ИС" - 2013: "3.1. Идентификация и аутентификация субъектов доступа и объектов доступа":
  - При доступе в ИС должна осуществляться однозначная ИА пользователя;
  - Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, био- или с помощью комбинации их…или др. средств.

ГОСТ Р 53110-2008

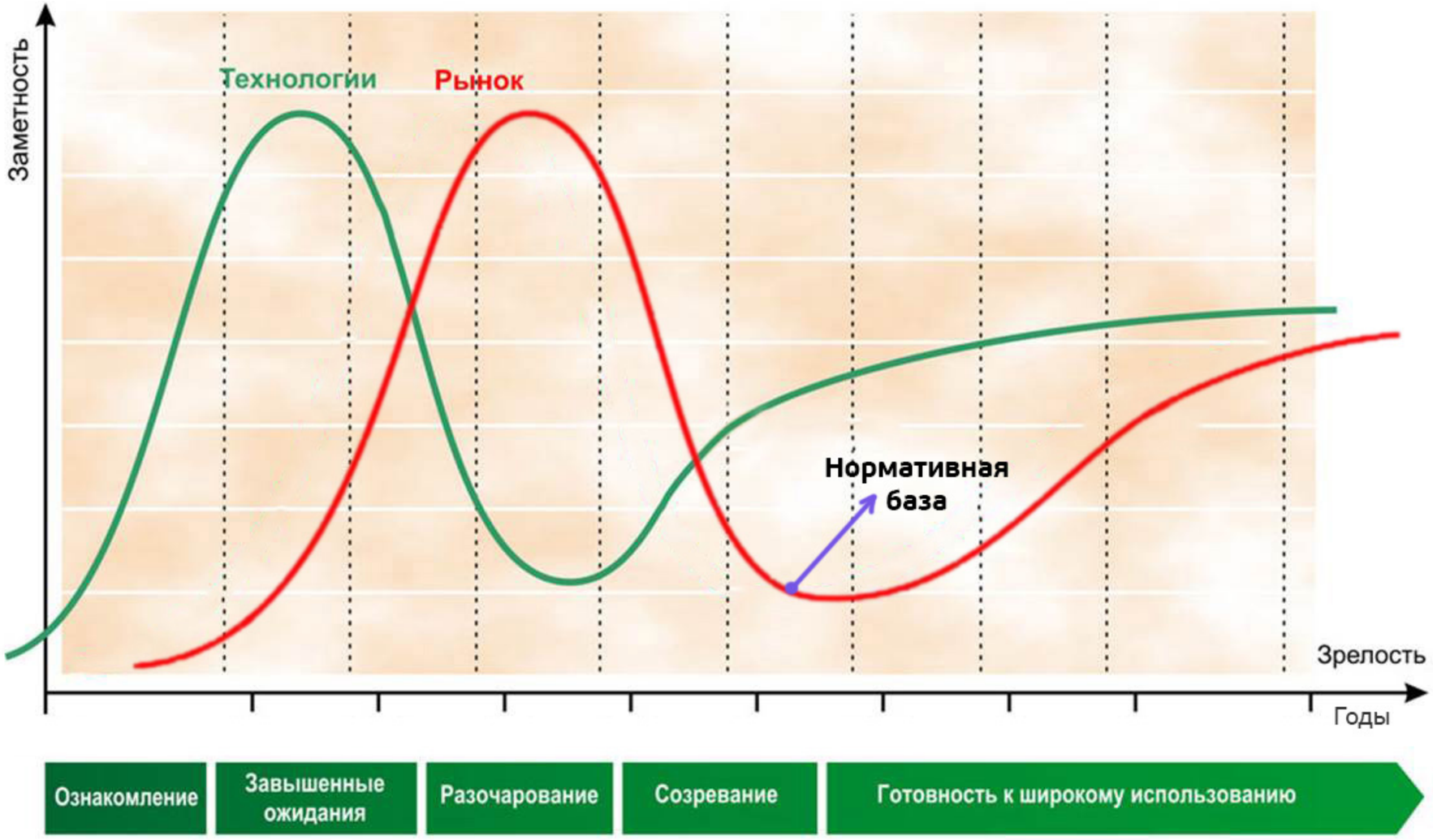
Система обеспечения информационной безопасности сети связи общего пользования

- Управление рисками по ГОСТ Р 53448;
- Подсистема «аутентификация и авторизация»:
  - Предназначена для централизованной аутентификации и авторизации субъектов к программно-аппаратным средствам связи и управления;
  - Может быть реализована встроенными механизмами аутентификации средств связи и информатизации для идентификации, аутентификации и авторизации.

Выводы

- Анализ зарубежного опыта:
  - исторически первые требования к аутентификации при доступе к информационным ресурсам разработаны в США.
  - Канада, Австралия и ряд других стран повторяют и лишь локализуют американские требования, которые являются наиболее проработанными.
  - В ЕС внимание уделено аутентификации для электронной подписи.
- Российская нормативная база существенно отстаёт от развитых стран. Необходимо сократить это отставание нормативного регулирования на основе анализа зарубежных разработок
- Самой большой проблемой существующей и планируемой к опубликованию российской нормативной базы является полная **независимость от технологий**.

Технологии и их внедрение



Спасибо за внимание!