Об актуальных направлениях развития системы национальных и отраслевых стандартов ИБ для российских финансовых организаций

Голованов В.Б., отв. Секретарь ПК1 ТК122, ИнфоТеКС

Наши ориентиры (ТК122)

«Весь бизнес представляет собой вопрос доверия. Доверие может развиться только в том случае, когда участники сделки ощущают надежность и безопасность. Таким образом, безопасность, с точки зрения бизнеса, должна рассматриваться как способствующий бизнесу фактор, а не как его цена.»

«Доверие информационной безопасности для руководящих работников», 7 октября 2003 г.
Консультативный комитет **ОЭСР** по предпринимательству и промышленности **(BIAC)**,
Международная торговая палата **(ICC)**

ТК 122 «Стандарты финансовых операций». Создание

ПРИКАЗ

30 декабря 2010 г. № 5527

г. Москва

О создании технического комитета по стандартизации «Стандарты финансовых операций»

В целях реализации Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», повышения эффективности работ по национальной, региональной и международной стандартизации в области

ПРИКАЗ

19 октября 2011 г. № 5481

г. Москва

О реализации пункта 3 приказа Федерального агентства по техническому регулированию и метрологии от 30 декабря 2010 года № 5527 « О создании технического комитета по стандартизации «Стандарты финансовых операций»

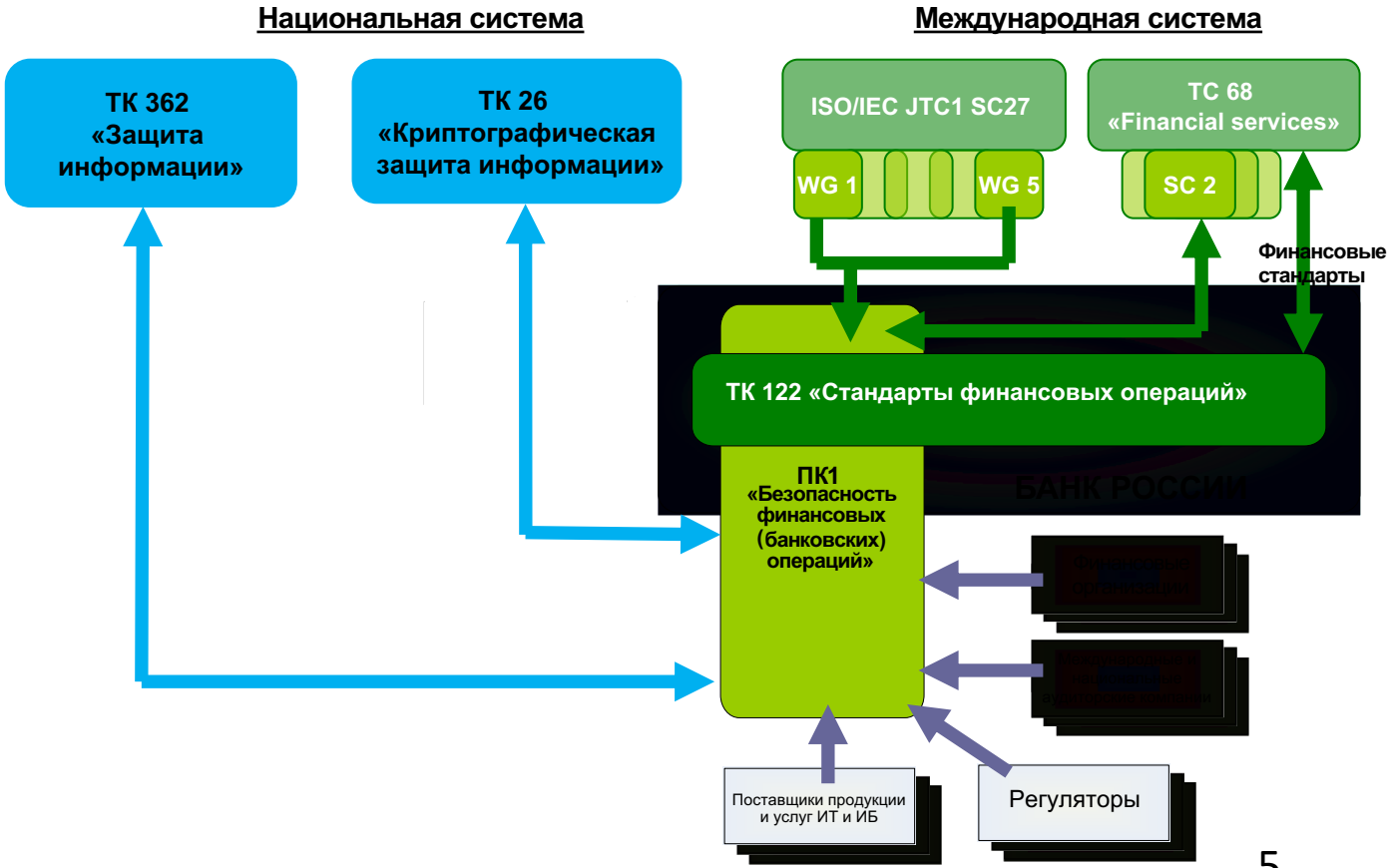
В целях реализации Федерального закона "О техническом регулировании", повышения эффективности работ по национальной, региональной, межгосударственной и международной стандартизации в области финансовых

п р и к а з ы в а ю :

1. Создать технический комитет по стандартизации «Стандарты финансовых операций» (далее ТК) на базе Центрального Банка Российской Федерации (Банка России) и закрепить за ним продукцию и услуги в соответствии с кодом ОКС 03.060.

ТК 122 Стандарты, кооперация и конкуренция

Организация работ в рамках систем стандартизации



ТК 122 «Стандарты финансовых операций». ПК1 «Безопасность финансовых (банковских) операций».

Цели и направления работы (*С 2003 по 2011 год работы шли в составе ТК362 «Защита информации»*)

Обеспечение безопасности банковской деятельности и финансовых операций, включающее:

- **Разработку национальных стандартов** обеспечения безопасности финансовых (банковских) операций на основе документов в области стандартизации Банка России СТО/РС БР ИББС
- **Гармонизацию международных стандартов**, изданных в рамках юрисдикции ISO/TC 68/SC 2 «Security management and general banking operations». Продвижение отечественного опыта
- **Гармонизацию профессиональных стандартов** обеспечения информационной безопасности банковской и платежной индустрий (стандарты PCI Council/PCI DSS, рекомендации EPC/Европейский платежный совет и т.п.)

Стандарты Банка России, принятые в рамках планов работ ПК1 ТК122 (ранее ПК3 ТК362)

Стандарты Банка России

- **СТО БР БФБО-1.5-2018** «Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации»
- **СТО БР ИББС-1.4-2018** «Управление риском информационной безопасности при аутсорсинге»
- **СТО БР ИББС-1.3-2016** «Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств»
- **СТО БР ИББС-1.0-2014** «Обеспечение ИБ организаций БС РФ. Общие положения»
- **СТО БР ИББС-1.2-2014** «Обеспечение ИБ организаций БС РФ. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0 — 2014»
- **СТО БР ИББС-1.1-2007** «Аудит информационной безопасности»

Рекомендации по стандартизации Банка России

- **РС БР ИББС-2.9-2016** «Предотвращение утечек информации»
- **РС БР ИББС-2.8-2015** «Обеспечение информационной безопасности при использовании технологии виртуализации»
- **РС БР ИББС-2.7-2015** «Ресурсное обеспечение информационной безопасности»
- **РС БР ИББС-2.6-2014** «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем»
- **РС БР ИББС-2.5-2014** «Менеджмент инцидентов информационной безопасности»
- **РС БР ИББС-2.2-2009** «Методика оценки рисков нарушения информационной безопасности»
- **РС БР ИББС-2.1-2007** «Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0»
- **РС БР ИББС-2.0-2007** «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0»

Национальные стандарты, принятые в рамках планов работ ПК1 ТК122

- **ГОСТ Р 57580.1-2017** «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»
- **ГОСТ Р 57580.2-2018** «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»

В разработке:

- **ГОСТ Р ХХХХХ** Безопасность финансовых (банковских) операций. *Управление риском реализации информационных угроз. Общие положения*
- **ГОСТ Р ХХХХХ** Безопасность финансовых (банковских) операций. *Управление риском реализации информационных угроз. Методика оценки соответствия*
- **ГОСТ Р ХХХХХ** Безопасность финансовых (банковских) операций. *Обеспечение операционной надежности. Общие положения*
- **ГОСТ Р ХХХХХ** Безопасность финансовых (банковских) операций. *Обеспечение операционной надежности. Методика оценки соответствия*

ISO/TC 68/SC 2 Financial Services, Security. Фокус работ – прикладная криптография

Действующие международные стандарты обеспечения безопасности финансовых операций:

- **ISO 9564-1:2017** Financial services -- Personal Identification Number (PIN) management and security -- Part 1: Basic principles and requirements for PINs in card-based systems; **ISO 9564-2:2014** Part 2: Approved algorithms for PIN encipherment; **ISO 9564-4:2016** Part 4: Requirements for PIN handling in eCommerce for Payment Transactions
- **ISO 11568-1:2005** Banking -- Key management (retail) -- Part 1: Principles; **ISO 11568-2:2012** Part 2: Symmetric ciphers, their key management and life cycle; **ISO 11568-4:2007** Part 4: Asymmetric cryptosystems -- Key management and life cycle
- **ISO 13491-1:2016** Financial services -- Secure cryptographic devices (retail) -- Part 1: Concepts, requirements and evaluation methods; **ISO 13491-2:2017** Part 2: Security compliance checklists for devices used in financial transactions
- **ISO 13492:2007** Financial services -- Key management related data element -- Application and usage of ISO 8583 data elements 53 and 96
- **ISO/TR 14742:2010** Financial services -- Recommendations on cryptographic algorithms and their use
- **ISO 16609:2012** Financial services -- Requirements for message authentication using symmetric techniques
- **ISO/TR 19038:2005** Banking and related financial services -- Triple DEA -- Modes of operation -- Implementation guidelines
- **ISO 19092:2008** Financial services -- Biometrics -- Security framework
- **ISO 20038:2017** Banking and related financial services -- Key wrap using AES
- **ISO 21188:2018** Public key infrastructure for financial services -- Practices and policy framework
- **ISO/TR 21941:2017** Financial services -- Third-party payment service providers

Преимущественно в оборудовании и протоколах по стандартам EMVCo, GlobalPlatform и пр.

ISO/TC 68/SC 2 Financial Services, Security
Фокус работ – прикладная криптография (продолжение)

Разрабатывающиеся/пересматриваемые международные стандарты обеспечения безопасности финансовых операций:

- **ISO/CD 9564-5** Banking -- Personal Identification Number (PIN) management and security -- Part 5: Methods for Generation, Change, and Verification of PINs and Associated Data
- **ISO/CD 11568** Financial services -- Key management (retail) -- Principles, symmetric ciphers and asymmetric cryptosystems, their key management and life cycle
- **ISO/PRF 13492** Financial services -- Key-management-related data element -- Application and usage of ISO 8583-1 data elements for encryption
- **ISO/AWI TR 14742** Financial services -- Recommendations on cryptographic algorithms and their use
- **ISO/AWI 16609** Financial services -- Requirements for message authentication using symmetric techniques
- **ISO/AWI 19092** Financial services -- Biometrics -- Security framework
- **ISO/CD 23195** Security objectives of information systems of third party payment services
- **ISO/AWI TS 23526** Security aspects for digital currencies

Преимущественно в оборудовании и протоколах по стандартам EMVCo, GlobalPlatform и пр.

Проект финансового рынка: Открытые данные. Сервисы безопасности доступа к открытым данным

Разработка проекта СТО БР ФАПИ.СЕК-1.6-202х на основе спецификаций (https://openid.net/wg/fapi/):

- Financial-grade API — Part 1: Read Only API Security Profile (Implementer's Draft);
- Financial-grade API — Part 2: Read & Write API Security Profile (Implementer's Draft);
- Financial-grade API — JWT Secured Authorization Response Mode for OAuth 2.0 (JARM) (Implementer's Draft).

Заказчик – Ассоциация ФИНТЕХ

Состав криптографических механизмов и протоколов для российской реализации подлежит **согласованию с уполномоченной организацией и на площадке ТК26**.

Проект: Открытые данные.
Сервисы безопасности доступа к открытым данным

Что подлежит согласованию с уполномоченным органом?

Основа гармонизируемых сервисов безопасности для прикладного программного интерфейса

OAuth 2.0:

- **RFC 6749** «The OAuth 2.0 Authorization Framework»;
- **RFC 6750** «The OAuth 2.0 Authorization Framework: Bearer Token Usage»;
- **RFC 6819** «OAuth 2.0 Threat Model and SecURIty Considerations»;
- **RFC 7591** «OAuth 2.0 Dynamic Client Registration Protocol»;
- **RFC 8414** «OAuth 2.0 Authorization Server Metadata»;
- **RFC 7662** «OAuth 2.0 Token Introspection»;
- **RFC 7636** «Proof Key for Code Exchange by OAuth Public Clients»

Проект: Открытые данные. Сервисы безопасности доступа к открытым данным

JSON Web:

- **RFC 7515** «JSON Web Signature (JWS)»;
- **RFC 7516** «JSON Web Encryption (JWE)»;
- **RFC 7517** «JSON Web Key (JWK)»;
- **RFC 7518** «JSON Web Algorithms (JWA)»;
- **RFC 7519** «JSON Web Token (JWT)»

Управление ключами:

- **RFC 6125** «Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer SecURIty (TLS)»

Расширения и дополнения от OpenID (http://OpenID.net/specs/***):***

- «OAuth 2.0 Multiple Response Type Encoding Practices»;
- «OAuth 2.0 Form Post Response Mode»;
- «OpenID Connect Session Management 1.0»

Небольшое общее резюме

1. В рамках вверенных полномочий под эгидой ТК122 разрабатываются и принимаются отраслевые и национальные стандарты, **предназначенные для защиты информации НЕкриптографическими методами**.

2. Развитие финансовых технологий **требует все более широкое использование криптографических механизмов**, что согласно действующих норм влечет надлежащее взаимодействие с уполномоченной службой.

3. В составе ТК26 образован Подкомитет № 3 «**Криптографические алгоритмы и механизмы в национальной платежной системе Российской Федерации**» - как результат обращения Банка России в свете создания и функционирования НСПК (карта «Мир») – 2015г.


infotecs
Спасибо!