Уральский форум за 15 минут

Фигня! За 15 минут не уложиться ☺

Алексей Лукацкий
Бизнес-консультант по безопасности

16 февраля 2018

Disclaimer

Презентация описывает взгляд автора на программу 10-го Уральского форума по информационной безопасности финансовой сферы

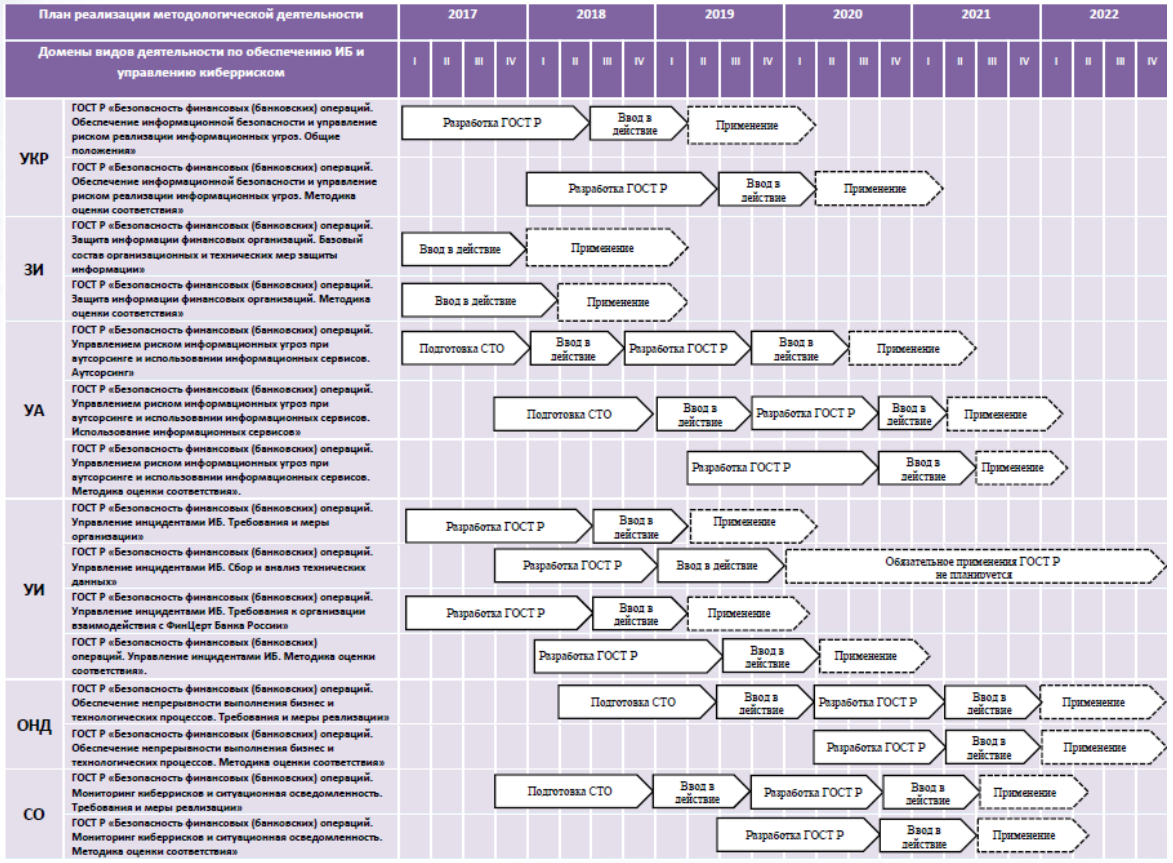
Данная презентация описывает личную точку зрения автора и может не совпадать с точкой зрения его работодателя или иных официальных лиц, с которыми автора связывают или не связывают какие-либо отношения!

cisco

Основные направления технологического развития Банка России

Стандартизация и направления регулирования ИБ

Дорожная карта стандартизации по ИБ Банка России



- **Домен УКР** – «управление киберриском»
- **Домен ЗИ** – «защита информации»
- **Домен СО** – «мониторинг киберрисков и ситуационная осведомленность»
- **Домен ОНД** – «обеспечение непрерывности выполнения бизнес и технологических процессов финансовых организаций в случае реализации информационных угроз»
- **Домен УА** – «управлением киберриском при аутсорсинге и использовании сторонних информационных услуг (сервисов)»
- **Домен УИ** – «управление инцидентами ИБ»

Направления стандартизации Банка России

- **Стандарты по защите информации**
  - ГОСТ 57580.1
  - ГОСТ 57580.2
- **Стандарты по ОИБ и управлению рисками**
  - Общие положения
  - Оценка соответствия
  - Аудит ИБ
- **Аутсорсинг и использование информационных сервисов**
  - Аутсорсинг
  - Использование информационных сервисов
  - Оценка соответствия
- **Стандарты по управлению инцидентами**
  - Требования и меры организации
  - Сбор и анализ технических данных
  - Взаимодействие с ФинЦЕРТ (СТО 1.5)
- **Стандарт по непрерывности**
  - Требования и меры реализации
  - Оценка соответствия
- **Мониторинг киберрисков и ситуационная осведомленность**
  - Требования и меры реализации
  - Оценка соответствия

Источник: план работы ПК1 ТК122

Резервирование капитала для покрытия рисков ИБ

cisco

Управление киберрисками

- Киберриски – это часть операционных рисков
- В кредитной организации должна быть создана база данных о событиях операционного риска и убытках, понесенных вследствие реализации операционного риска
- Назначение базы данных – контроль над уровнем фактически понесенных (прямых) убытков кредитной организации
- ДБР в 2018-м году планирует установить требования к отдельной классификации событий риска ИБ в составе БД операционных рисков

Управление киберрисками

Кредитная организация обязана будет резервировать капитал на покрытие операционных рисков, включая и киберриски

- Кредитная организация:

  Определяет на плановый годовой период количественные и качественные показатели склонности к риску ОР, в том числе к риску ИБ(риск-аппетиты ОР и ИБ)
  Устанавливает целевые уровни этих показателей: сигнальный (приемлемый) уровень и контрольный (лимитный) уровень

- Качественные требования будут формулироваться в рамках ВПОДК в Указании Банка России №3624-У ссылками на отраслевые стандарты ИБ (например, ГОСТР 57580.1-2017) с учетом качественных требований Базеля II к ВПОДК
- Банк самостоятельно определяет уровни и утверждает их на Совете Директоров.
- Уровни должны быть обоснованы и должны соотноситься с величиной минимального регуляторного капитала в рамках Положения No 346-П

Иные проекты НА и НПА

Иные нормативные и нормативно-правовые акты

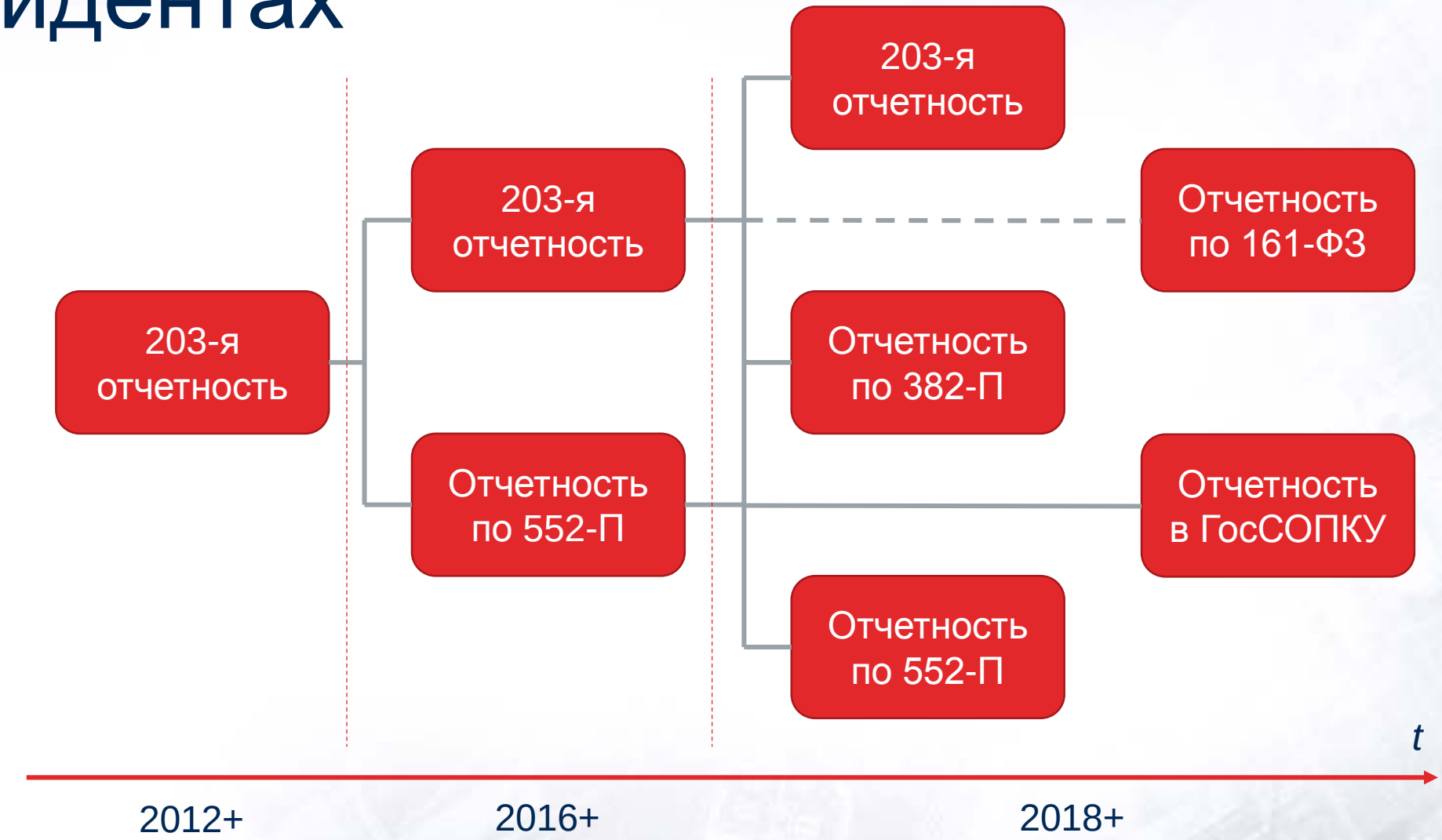
- Новая редакция 382-П – 1 июля 2018 года
  - Контроль защищенности платежных приложений
  - Внешний аудит
  - Оценка соответствия платежных приложений
  - Оперативное уведомление об инцидентах (в течение дня)
  - Разделение контуров
- Перспективная редакция 382-П – 2019 год
  - Обязательность применения ГОСТ Р 57580.1
  - Оценка соответствия по ГОСТ Р 57580.1 (57580.2)
- Новая форма отчетности 203

cisco

Иные нормативные и нормативно-правовые акты

- Проект федерального закона № 296412-7 «О внесении изменений в отдельные законодательные акты Российской Федерации (в части противодействия хищению денежных средств)»
  - введение антифрод-систем кредитных организаций
  - возврат несанкционированно переведенных денежных средств юридическим лицам
  - введение обмена информацией о компьютерных атаках с использованием сервисов ФинЦЕРТ
  - расширение полномочий Банка России по регулированию обеспечения защиты информации на финансовом рынке

Развитие форм отчетности об инцидентах



Иные нормативные и нормативно-правовые акты

- Проект федерального закона «О внесении изменений в статью 151 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

  блокировка по решению Банка России фишинговых сайтов

  блокировка по решению Бланка России сайтов, предоставляющих финансовые услуги без соответствующей лицензии Банка России

- Проект федерального закона «О внесении изменений в Федеральный закон «О банках и банковской деятельности»

  Исключение режима не распространения банковской тайны на случаи обмена информации о совершении (попытках совершения) перевода денежных средств без согласия клиента с использованием информационных сервисов ФинЦерт Банка России

Иные нормативные и нормативно-правовые акты

- Проект федерального закона «О внесении изменений в Федеральный закон от 7 июля 2003 года № 126-ФЗ «О связи» (в части защиты прав и законных интересов пользователей услуг)»

  подтверждение принадлежности абонентского номера конкретного клиента кредитной организаций в единой информационной системе

- Проект Указания Банка России «Об определении перечня угроз безопасности биометрических персональных данных, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации»

Критическая информационная инфраструктура

cisco

Финансовые организации и КИИ

- Все финансовые организации являются субъектами КИИ
- Все информационные системы являются объектами КИИ, но не все являются значимыми

Что надо делать для выполнения закона?

- Категорирование
- Обеспечение ИБ
- Присоединение к ГосСОПКЕ

cisco

У кого могут быть значимые объекты?

1	2	3	4	5
	III. Экономическая значимость			
3.1	Возможно возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемое в снижении уровня дохода (с учетом НДС, акцизов и иных обязательных платежей) по всем видам деятельности (Д), в процентах от прогнозируемого объема годового дохода по всем видам деятельности	5<Д<=10	10<Д<=15	Д>15
3.2	Возможно возникновение ущерба бюджетам Российской Федерации, оцениваемое: а) в снижении доходов федерального бюджета (ФБ), в процентах от прогнозируемого годового дохода бюджета; б) в снижении доходов бюджета субъекта Российской Федерации (РБ), в процентах от прогнозируемого годового дохода бюджета; в) в снижении доходов бюджетов государственных внебюджетных фондов (БФ), в процентах от прогнозируемого годового дохода бюджета	0,001<ФБ<=0,05; 0,001<РБ<=0,05; 0,01<БФ<=0,5	0,05<ФБ<=0,1; 0,05<РБ<=0,1; 0,5<БФ<=1	ФБ>0,1; РБ>0,1; БФ>1

1	2	3	4	5
3.3	Возможно прекращение или нарушение проведения клиентами операций по банковским счетам/без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций ($Н_{КО}$), в млн. единиц (расчет осуществляется по итогам года, а для создаваемых объектов на основе прогнозных значений)	3,0< $Н_{КО}$ <=70,0	70,0< $Н_{КО}$ <=120,0	120,0< $Н_{КО}$

- 31 финансовая организация с участием государства
- 1 банк как стратегическое предприятие и стратегическое АО
- 11 системно значимых кредитных организаций
- 4 системно значимые инфраструктурные организации финансового рынка
- 9 операторов услуг платежной инфраструктуры системно и (или) социально значимых (но не национально значимых) платежных систем

По состоянию на 14 февраля 2018 года

Финансовые организации с участием государства

- Банк России
- Сбербанк
- Внешэкономбанк
- Национальный Клиринговый Центр
- ВТБ
- Россельхозбанк
- Газпромбанк
- Глобэкс (как дочка ВЭБ)
- Связь-Банк (как дочка ВЭБ)
- МСП Банк (как дочка Федеральной корпорация по развитию малого и среднего предпринимательства)
- Российский капитал (как дочка АИЖК)
- ВБРР
- Почта Банк (как дочка ВТБ и Почты России)
- РНКБ (как дочка Росимущества)
- Еврофинанс Моснарбанк (как дочка ГПБ и ВТБ)
- Крайинвестбанк
- Дальневосточный Банк
- Акибанк
- Алмазэргиэнбанк
- Московское Ипотечное Агентство
- Росэксимбанк
- БМ-Банк
- Русь
- Хакасский Муниципальный Банк
- Банк Казани
- Почтобанк (не путать с Почта Банк)
- Новикомбанк
- НСПК
- Открытие
- Бинбанк
- Ростбанк
- Уралприватбанк

Оценка автора

Системно значимые кредитные организации

- АО ЮниКредит Банк
- Банк ГПБ
- Банк ВТБ
- АО «АЛЬФА-БАНК»
- ПАО Сбербанк
- ПАО «Московский Кредитный Банк»
- ПАО Банк «ФК Открытие»
- ПАО РОСБАНК
- ПАО «Промсвязьбанк»
- АО «Райффайзенбанк»
- АО «Россельхозбанк»

Оценка автора

Системно значимые инфраструктурные организации финансового рынка

- Центральный депозитарий
- Расчетный депозитарий
- Репозитарий
- Центральный контрагент

Оценка автора

Операторы услуг платежной инфраструктуры системно и (или) социально значимых ПС

- Русславбанк и ВТБ (для CONTACT)
- НСПК, Банк России (для Visa)
- Платежный центр, Золотая корона (для Золотой короны)
- Национальный расчетный депозитарий (для НРД)
- Лидер (для ПС Лидер)
- НСПК, Банк России (для MasterCard)
- ВТБ (для ПС ВТБ)
- Сбербанк (для ПС Сбербанка)
- Рапида, ВТБ (для Рапиды)

Оценка автора

Что означает присоединение к ГосСОПКЕ?

- Информирование об инцидентах на значимых объектах КИИ вашего центра ГосСОПКИ
- Содействие сотрудникам ФСБ в деятельности по реагированию на инциденты
- Выполнять требования по установке и эксплуатации средств ГосСОПКИ на объектах КИИ (если устанавливаются)

cisco

ФинЦЕРТ и ГосСОПКА

- Организация и координация обмена информацией между ФинЦЕРТ и правоохранительными органами, кредитными и некредитными финансовыми организациями
- Анализ данных о компьютерных атаках в кредитных и некредитных финансовых организациях и подготовка аналитических материалов
- ФинЦЕРТ не является ни ведомственным, ни корпоративным центром ГосСОПКА и финансовые организации должны самостоятельно направлять данные об инцидентах в ГосСОПКУ
- Ведутся работы по наделению ФинЦЕРТ полномочиями центра ГосСОПКИ

Обратите внимание!

Требования по безопасности ФСТЭК предъявляются только к значимым объектам КИИ

Незначимые объекты могут продолжать относиться к ИСПДн, АБС и т.п.

cisco

Обратите внимание!

Действующие документы по ИБ ФСТЭК, Банка России, ФСБ, Минкомсвязи продолжают действовать!

Удаленная идентификация

Удаленная идентификация клиентов

Удаленная идентификация клиентов финансовых организаций – подтверждение соответствия информации, предоставленной клиентом (ФИО, паспорт, биометрические данные, иное), ранее не обращавшимся за услугами, информации, содержащейся в доверенном государственном информационном ресурсе, осуществляемое с использованием дистанционных каналов взаимодействия

ЦЕЛИ

- Повышение качества финансовых услуг за счет усиления конкуренции на финансовом рынке
- Повышение доступности финансовых услуг для потребителей в труднодоступных регионах
- Увеличение скорости предоставления услуг за счет перехода на полное электронное взаимодействии

ЗАДАЧИ

- Создание единого пространства доверия идентификации и аутентификации
- Интероперабельность информационных систем участников взаимодействия
- Безопасность и надёжность механизма удаленной идентификации
- Актуальность и достоверность идентификационной информации
- Гибкость и своевременность реализации необходимых изменений

cisco

Первичная идентификация

Удаленная идентификация при получении услуг в месте, отличном от первичной идентификации

В дальнейшем может быть предусмотрено проведение удаленной идентификации физических лиц в НФО

Обновление идентификационной информации

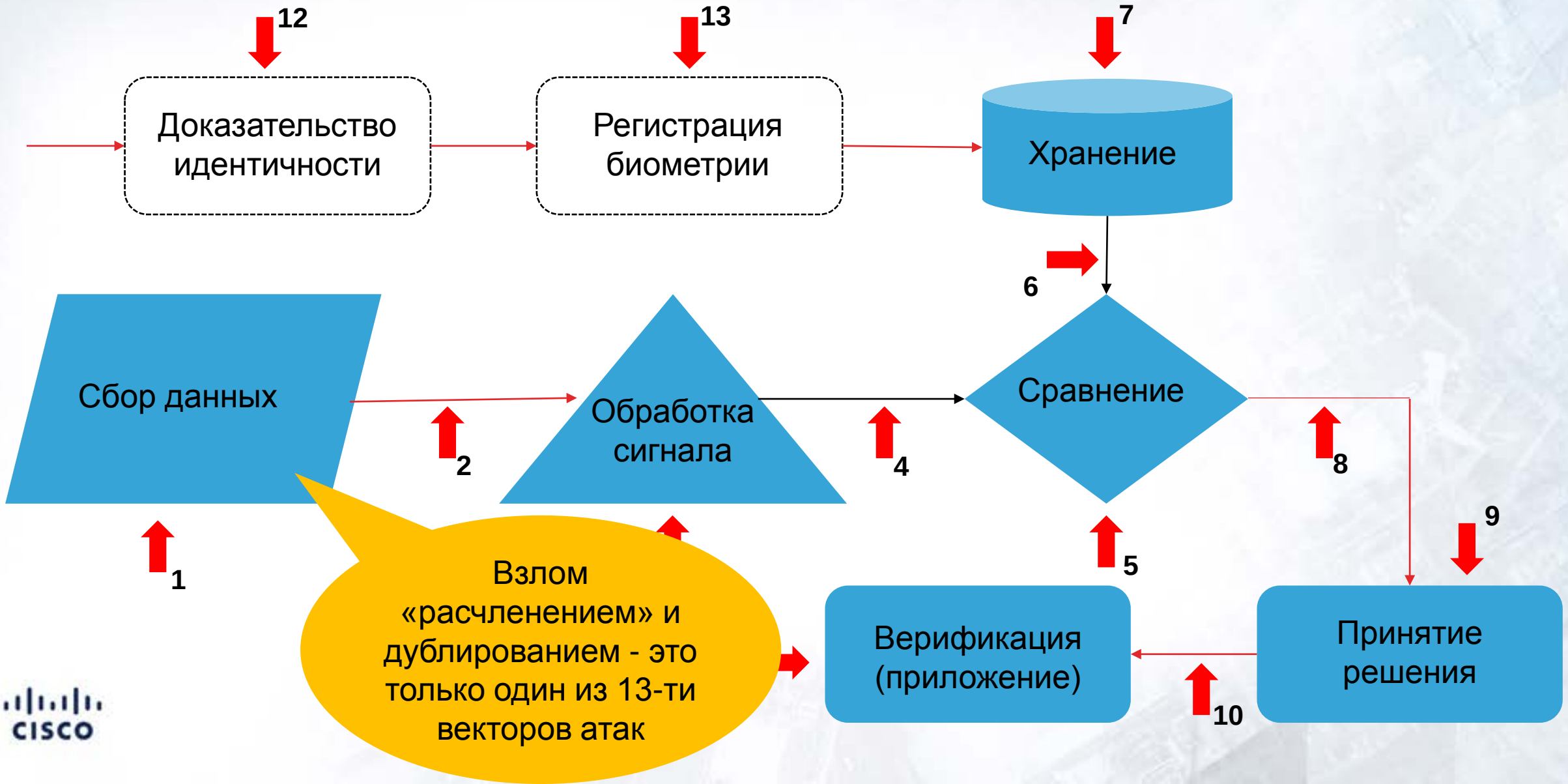
cisco

Перспективы ЕСИА: взгляд Минкомсвязи

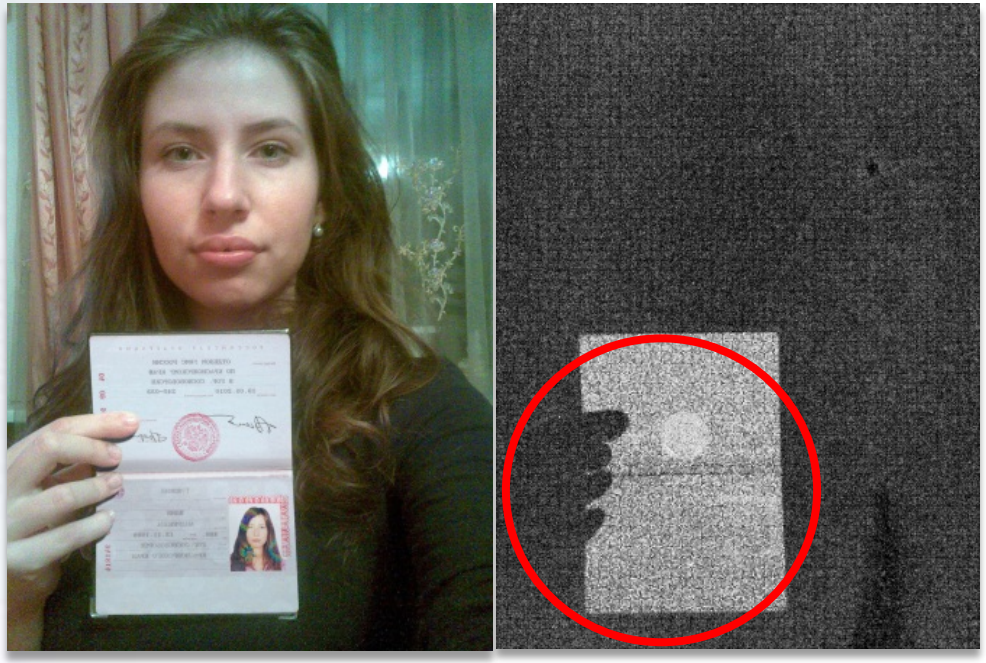
- Биометрическая идентификация/ аутентификация
- Облачная квалифицированная электронная подпись
- Реестр персданных и система дачи согласий на доступ к ним
- Юридически значимые уведомления

CISCO

Кто-нибудь учитывает модель угроз?



Практические аспекты небезопасности биометрии



Посмотрите материалы мастер-класса Oz Forensics и Информзащиты про использование нейросетей для обхода биометрии

- Мало кто говорит о защите центрального хранилища биометрических ПДн, площадь атаки на которое будет только расти в связи с подключением большого количества участников (это вам не база биометрических паспортов)
- Технологии меняются и дешевеют быстро, а внедрение биометрии на тысячи и десятки тысяч устройств (например, банкоматов) может занять длительное время
- Биометрия может иметь отношение к биометрическим ПДн, обработка которых требует письменного согласия субъекта ПДн
- Не каждый банковский офис в состоянии обеспечить эффективное снятие биометрического профиля клиента (качество освещения и качество звука)

ФинЦЕРТ

Центр компетенций по ИБ в кредитно-финансовой сфере на базе ФинЦЕРТ

- Определение потребностей рынка в совершенствовании вопросов киберустойчивости
- Организация и осуществление информационного обмена о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении финансовых операций по определенной технологии и в установленных форматах электронных сообщений
- Нормативное регулирование вопросов киберустойчивости финансовых организаций
- Ведение базы данных о выявленных инцидентов, связанных с нарушением киберустойчивости финансовых организаций
- Организация и координация работ по совершенствованию форм и методов взаимодействия финансовых организаций по вопросам обеспечения информационной безопасности и повышения их готовности к противостоянию информационным угрозам

Планы развития ФинЦЕРТ

- Использование ГОСТа ФСТЭК по описанию уязвимостей
- Создание системы противодействия хищениям денежных средств (Антифрод)
- Взаимодействие с КЦ национального домена сети Интернет
- Усиление технической экспертизы в части расследования инцидентов
- Система личных кабинетов на сайте ЦБ
- Участие в инспекционных проверках
- Получение большего числа уведомлений об инцидентах
- Автоматизация рассылки бюллетеней в машинно-читаемом формате

АСОИ ФинЦЕРТ (1-я очередь)

- Обмен с участниками через интегрированный защищенный портал и e-mail (получение информации в форматах XLS и JSON)

  Проект СТО 1.5 по форматам обмена данными на основе информации от ФинЦЕРТ и ГосСОПКИ

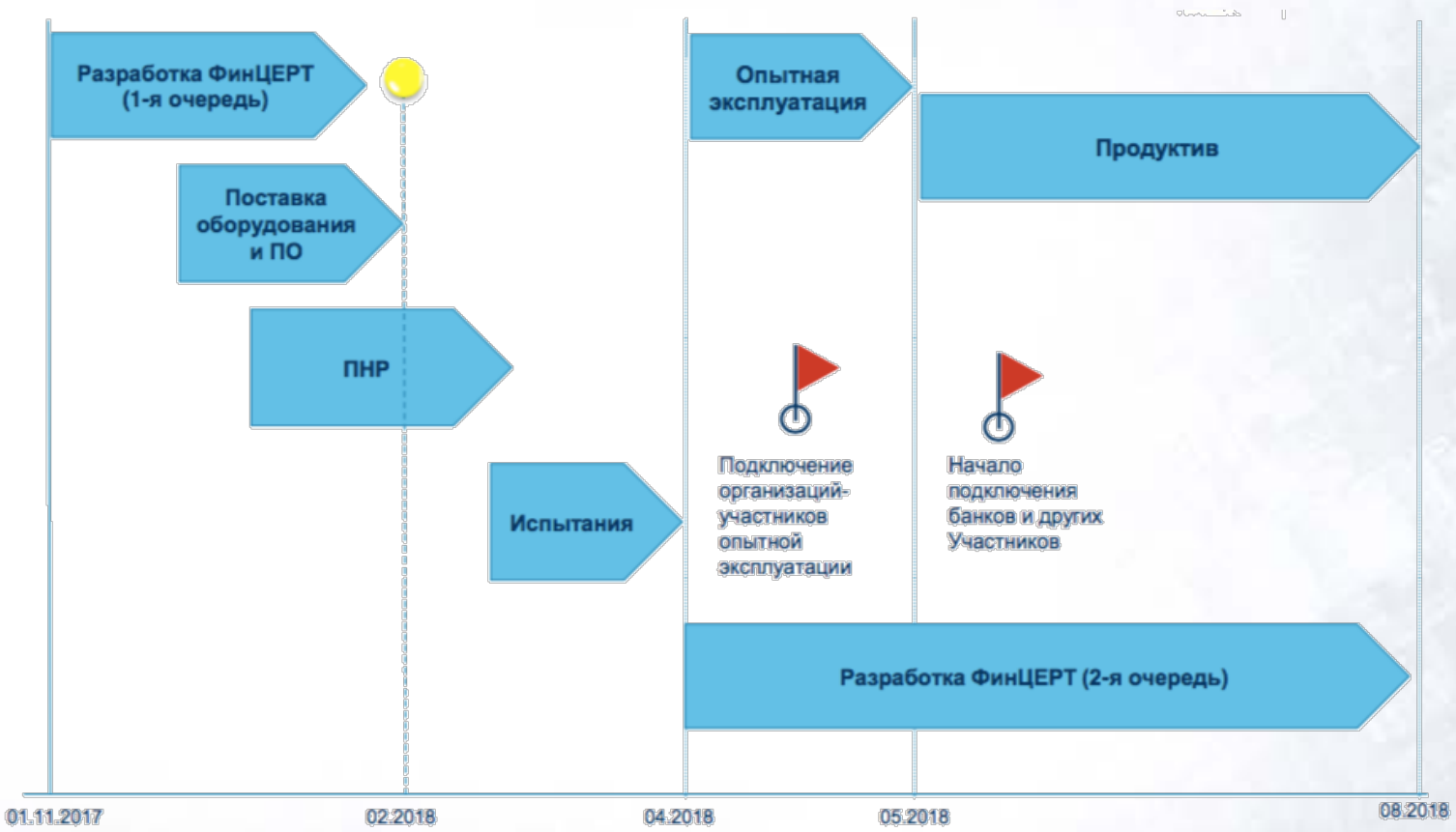
- Автоматизация ключевых процессов
- Автоматическое взаимодействие с ГосСОПКА
- Возможность взаимодействия с иностранными участниками

cisco

Автоматизация работы ФинЦЕРТ (2-я очередь)

- Автоматическое online-получение данных из SIEM-систем
- Автоматизация всех процессов деятельности
- Расширенные показатели назначения
- Online-анализ дампов трафика
- Максимально широкая экспертная база, автоматически пополняемая от российских и иностранных поставщиков
- Обеспечение неотказуемости (использование ЭП)
- Взаимодействие с иностранными участниками

Сроки внедрения АСОИ ФинЦЕРТ



Методологическая поддержка

Обзор несанкционированных переводов денежных средств за 2017 год

Обзор и схемы атак за 2017 год

БАНК РОССИИ
ФИНЦЕРТ

CISCO

Повышение квалификации

Совершенствование процесса повышения квалификации

+8 ПС **в области ИБ**

+1 new! ПС **по кибербезопасности**

+9 ФГОС для разных уровней подготовки **в области ИБ**

+2 new! ФГОС для разных уровней подготовки **в области ИБ для КФС**

Профессиональные стандарты

Дополнительные профессиональные программы

Образовательные стандарты

Система независимой аттестации специалистов

+1 new! типовая программа* профессиональной переподготовки специалистов **в области ИБ для КФС**

+1 new! типовая программа профессиональной переподготовки руководителей **в области ИБ для КФС**

Сертификаты международных независимых организаций (CISA, CISM, CISSP, COBIT, CGEIT, CRISC и другие)

+ new!

планируется разработка системы аттестации специалистов и руководителей подразделений ИБ

cisco

Разработка учебных программ

- Программа переподготовки специалиста ИБ на базе высшего образования
- Программа переподготовки руководителя ИБ на базе профильного высшего образования и (или) обучения по программе переподготовки «специалиста ИБ»
- Программа бакалавриата по профилю «Обеспечение информационной безопасности в организациях кредитно-финансовой сферы» в рамках общего направления «Информационная безопасность»
- Программа специализации «Информационная безопасность кредитно-финансовой сферы» в рамках специальности 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.04 «Информационно-аналитические системы безопасности»

Цифровая экономика

Цифровая экономика для финансовых организаций

- Российский сегмент Интернет хотят перевести на российскую криптографию, Web-сервера должны будут использовать TLS на базе ГОСТ 28147-89 в варианте «Кузнечик», а все браузеры должны реализовывать российскую криптографию
- Разработка процедуры обязательной оценки соответствия (сертификации) компонентов платежной инфраструктуры, используемых для переводов денежных средств в НПС

  Доклад ТК26 в рамках Уральского форума
- Рекомендуется перейти на отечественную криптографию в НПС

cisco

Новые рекомендации ТК26 для ФО

Р 1323565.1.013-2017 «Информационная технология. Криптографическая защита информации. Использование режимов алгоритма блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платёжных карт»

Утвержден Приказом №2116-ст от 28.12.2017 федерального агентства по техническому регулированию и метрологии с датой введения в действие 1 июня 2018 года.

Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации»

Утвержден Приказом №2068-ст от 22.12.2017 федерального агентства по техническому регулированию и метрологии с датой введения в действие 1 мая 2018 года.

Р 1323565.1.011-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN»

Утвержден Приказом №2019-ст от 19.12.2017 федерального агентства по техническому регулированию и метрологии с датой введения в действие 1 июня 2018 года.

cisco

Новые рекомендации ТК26 для ФО

Р 1323565.1.010-2017 «Информационная технология. Криптографическая защита информации. Использование функции диверсификации для формирования производных ключей платежного приложения»

Утвержден Приказом №2018-ст от 19.12.2017 федерального агентства по техническому регулированию и метрологии с датой введения в действие 1 июня 2018 года.

Р 1323565.1.009-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования при формировании прикладных криптограмм в платежных системах»

Утвержден Приказом №2017-ст от 19.12.2017 федерального агентства по техническому регулированию и метрологии с датой введения в действие 1 июня 2018 года.

Р 1323565.1.008-2017 «Информационная технология. Криптографическая защита информации. Использование режимов алгоритма блочного шифрования в защищенном обмене сообщениями между эмитентом и платежным приложением»

Утвержден Приказом №2016-ст от 19.12.2017 федерального агентства по техническому регулированию и метрологии с датой введения в действие 1 июня 2018 года.

Р 1323565.1.007-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN»

Утвержден Приказом №2015-ст от 19.12.2017 федерального агентства по техническому регулированию и метрологии с датой введения в действие 1 июня 2018 года.

cisco

Цифровая экономика для финансовых организаций

- Нормативное закрепление обязанности операторов персональных данных иметь финансовую гарантию ответственности или страховать свою ответственность (в случае утечек ПДн, или получения претензий) в соответствии с **классом информационной системы по обработке персональных данных** и уровнем защищенности ПДн (для высококритичных классов информационных систем)
- Страхование киберрисков

Предложения рынка ИБ

cisco

Активно предлагаемые на Уральском форуме решения ИБ

- Threat Intelligence и OSINT
- Антифрод в разных проявлениях
- Мониторинг ИБ (SOC)
- CASB
- Безопасность в облаке

  Блин, кто-нибудь ответит, можно банковскую тайну передавать облачному провайдеру, не имеющему лицензии ЦБ?
- Аутсорсинг

cisco

Что не удалось услышать?

cisco

Неозвученные темы

- Персональные данные

  Штрафы, большие данные, обезличивание, ФЗ-242, новое понятие ПДн

  РКН вообще не приехал ☹

- Позиция ФСТЭК и ФСБ по КИИ
- ФСБ и СКЗИ

  Новые требования по сертификации, 552-П и АРМ КБР, российская криптография и НПС/НСПК…

- PCI DSS

cisco

Спасибо!

alukatsk@cisco.com

CISCO