ДиалогНаука

Особенности реализации требований СТО БР ИББС по защите персональных данных

Корольков Сергей
Технический директор
ЗАО «ДиалогНаука»

ДиалогНаука

План презентации

- Текущая ситуация при внедрении СТО БР ИББС
- Особенности реализации требований по 152-ФЗ
- Проблемы и потребности
- О компании

ДиалогНаука

План презентации

Часть 1

Текущая ситуация

ДиалогНаука

Текущая ситуация

Банки, принявшие СТО БР ИББС в качестве внутреннего стандарта, сталкиваются с необходимостью:

- Внедрения требований СТО в части ПДн
- Внедрения СКЗИ прошедших оценку соответствия по уровню КС2
- Учета рекомендаций СТО БР ИББС в части выделения и назначения ролей
- Учета возможных поправок «законопроекта Резника» в 152-ФЗ:
  - в части требований к обработке ПДн
  - в части требований по защите
- Достижения некого уровня выполнения требований по ПДн и уведомления БР

План презентации

Часть 2

Особенности реализации требований

Реализация требований в части ПДн

Для реализации требований надо выполнить ключевые требования:

- Сформировать ролевой доступ
- Провести классификацию активов, включая ИСПДн
- Провести документирование банковских информационных технологических процессов обработки ПДн
- Разработать, согласовать и внедрить ОРД
- Внедрить СЗИ и СКЗИ
- Провести оценку соответствия

Формирование ролевого доступа

Анализ проекта РС БР ИББС 2.5-20xx «Выделение и назначение ролей» показал, что:

- Процедуры формирования ролей представляются избыточно сложными
- Решаема ли вообще задача построения такого перечня полномочий?
- Каков срок его создания? Каков срок актуальности?
- Вовлечение в процесс бизнес-подразделений на этапах «описания» приведет к увеличению сроков, наличию излишних полномочий
- Функциональная роль почти не отличается от должностных обязанностей
- Не учитываются уже те наработки, которые есть в банке

«Будьте проще и люди потянуться к вам»

Формирование ролевого доступа

На практике в банках, встречаются следующие ситуации:

- Ролей нет вообще, ни формально, ни в виде наборов полномочий в АБС
- Ролей нет частично. Роли не сформированы на основании формальной процедуры. В итоге есть наборы сформированные ИТ подразделениями на собственное усмотрение.
- Роли есть частично. В основных АБС сформированы роли вполне корректно, но не формально

ДиалогНаука

Формирование ролевого доступа

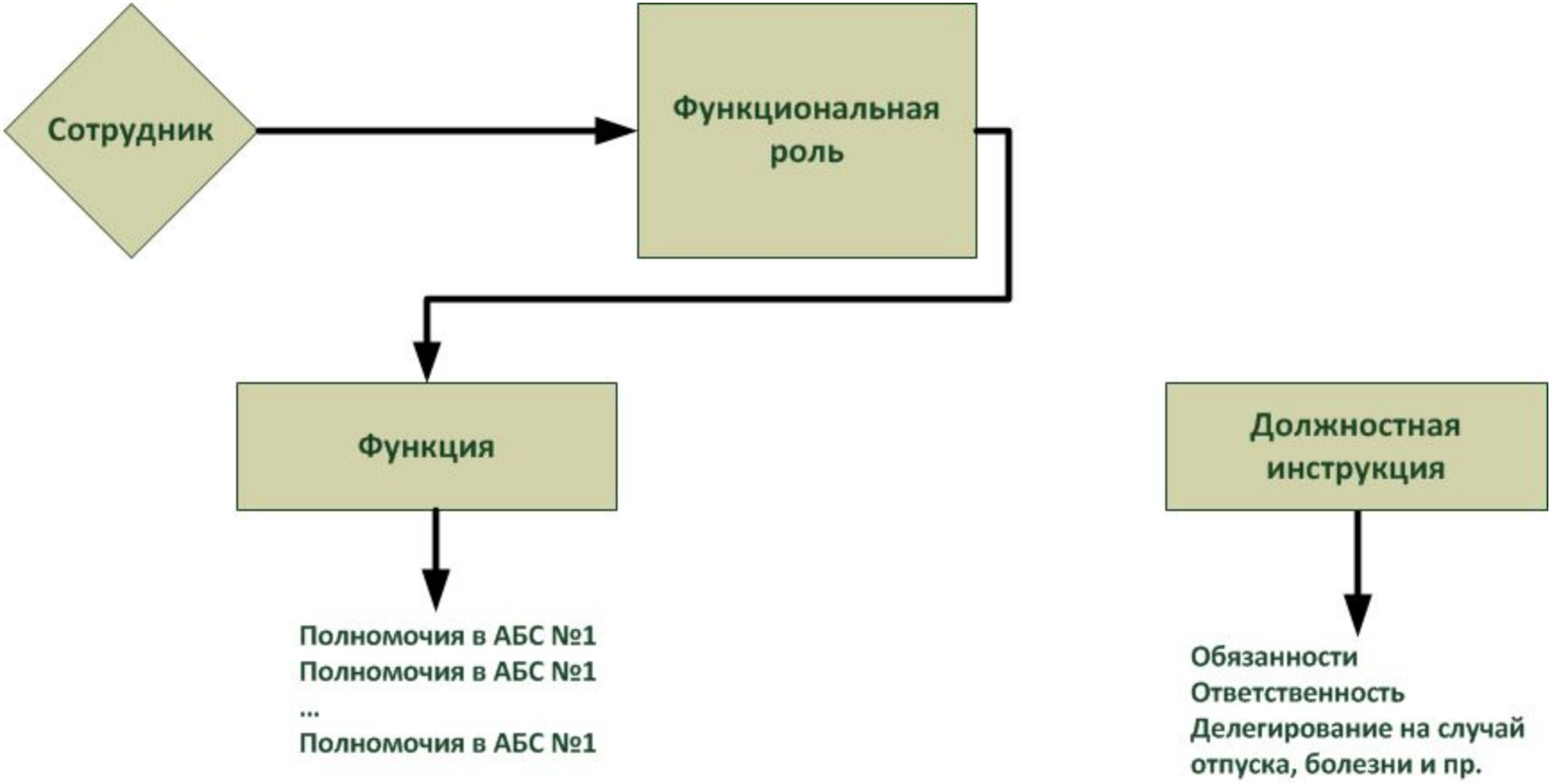
Наш подход по составлению ролей основан на следующих принципах:

- Сформировать роли на основании того, что банк уже имеет. Это не противоречит требованию СТО БР ИББС о фиксации ролей
- Формировать роли в виде базового набора полномочий и дополнительного набора полномочий получаемого в частном порядке
- Провести анализ на предмет несовместимых полномочий
- Бизнес-подразделения привлекать только на этапе согласования несовместимых полномочий и итоговых сформированных ролей
- Осуществить привязку к организационно-штатной структуре

Формирование ролевого доступа

В соответствии с проектом

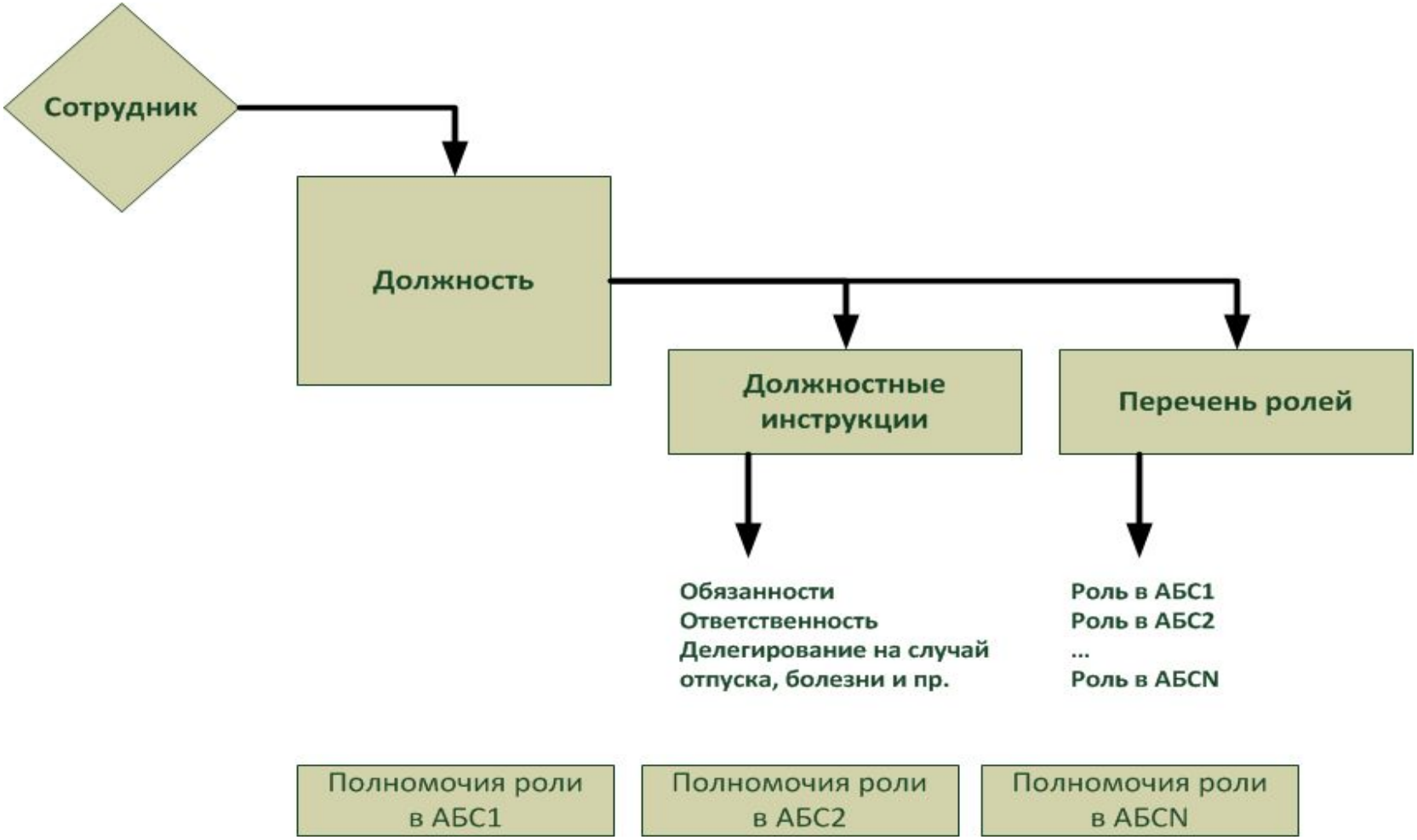
РС БР ИББС 2.5-20xx «Выделение и назначение ролей»



ДиалОгНаука

Формирование ролевого доступа

Предлагаемая схема формирования ролевого доступа



Формирование ролей

Предложения по совершенствованию РС БР ИББС 2.5-20xx «Выделение и назначение ролей»:

- Определить место и связь с должностными инструкциями и ролями
- Упростить количество процедур – чем проще набор требований, тем с большей вероятностью они будут реализованы
- Учитывать уже наработанный в банке опыт, а не составлять роли с нуля
- Более четко определить функции подразделений «технологов»

ДиалогНаука

Документирование деятельности

- Вопросы документирование банковских информационных технологических процессов обработки ПДн находятся не в компетенции подразделений ИБ и не всегда в компетенции Комитета по ИБ, что существенно затрудняет выполнение этого требования
- Не определена степень документирования процессов. Например, наличие нескольких верхнеуровневых документов может формально повышать оценку, а реально не влиять на безопасность ПДн и не только
- Вопросы документирования документирования процессов существенно влияют на оценки получаемые для уведомления регуляторов о соответствии

ДиалогНаука

Сертифицированные СКЗИ

Множество вопросов возникает по реализации требований по применению СКЗИ по уровню КС2 (п. 7.7.1).

- Для многих банков проекты по внедрению СКЗИ, прошедших оценку соответствия требованиям КС2, являются сложными ввиду:
  - Сложной структуры КСПД, в ней может использоваться проприетарные протоколы (например, IEGRP).
  - Наличия большого количества филиалов
  - Невозможности осуществления обслуживания в удаленных филиалах в соответствии с формулярами и правилами по использованию СКЗИ

ДиалогНаука

Сертифицированные СКЗИ

Сложности с реализацией отдельных требований Формуляров и Правил эксплуатации СКЗИ:

- Доставка сертификатов и ключей должна производиться администратором безопасности на съемном носителе, или иным доверенным способом, не нарушающим документ «… Руководство администратора безопасности…»
- Рядом с окнами помещений не должно быть пожарных лестниц и водосточных труб
- Обязательно наличие опечатываемого сейфа, оборудованного двумя внутренними замками, для хранения СКЗИ, тестовых ключей, эталонных CD дисков с ПО ПК, другой конфиденциальной информации. Для сейфа должно быть два ключа - основной ключ хранится у сотрудника, отвечающего за СКЗИ, а дубликат - в опечатанном его личной печатью пенале в сейфе Генерального директора.

ДиалогНаука

Сертифицированные СКЗИ

- Количество коммерческих работоспособных решений СКЗИ уровня КС2 измеряется единицами
- Влияние на итоговую оценку – 0.06
- Вероятность того, что в «законопроекте Резника» возможна определенная либерализация в вопросах требований по защите ПДн

На практике банки могут вовсе не внедрять СКЗИ прошедших оценку по уровню КС2

Мы рекомендуем сформировать и утвердить план, по которому СКЗИ будут внедряться в течении 2-3 лет

ДиалОгНаука

Коллекторские агентства

Коллекторские агентства и передача им персональных данных. Выход есть!

Гражданский кодекс позволяет передавать данные при:

- Соблюдении условий конфиденциальности
- Заключения агентского договора с коллектором (п. 1 ст. 1005 ГК РФ)
- или заключения договора цессии с коллектором (ст. 382 ГК РФ, ст. 384 ГК РФ, п. 2 ст. 385 ГК РФ)

При правильном заключении договора с коллекторами можно получить полностью легальный механизм!

План презентации

Часть 3

Проблемы и потребности Банков
в области информационной безопасности

ДиалогНаука

Непонимание

Исходя из опыта работы с банками по внедрению СТО БР ИББС нужно отметить:

- Банки небольшого размера в большинстве не понимают суть стандарта
- Многие банки среднего размера не могут корректно оценить последствия внедрения и затраты на «поддержку» СМИБ. Например, банк в котором во всем ИТ 4 человека считают, что вполне могут осилить внедрение за 3-4 месяца.
- Многие считают, что рекомендательный СТО БР ИББС на самом деле обязательный, или будет обязательным в течении нескольких лет
- Нет понимания процесса выполнения требований 152-ФЗ через СТО БР ИББС
- Не определен целевой уровень при реализации требований в части ПДн

ДиалОгНаука

Проблемы

- Online Prescoring. Этот процесс подразумевает получение персональных данных заемщика и его поручителей без согласия. В настоящий момент мы не знаем как обеспечить 100% легитимность процесса. СТО БР ИББС не помогает

- Согласия на обработку. Очень часто в соответствии с 152-ФЗ согласия не требуются. Тем не менее, часто, банк обрабатывает информацию не только с целью исполнения обязательств описанных в договоре. Вопрос получения согласий с 3-х лиц (например, поручителей) не затрагивается СТО.

- Уведомления об окончании обработки ПДн. Не затрагиваются в СТО.

ДиалОгНаука

План презентации

Часть 4

О Компании

ДиалогНаука

Основные направления деятельности

- Реализация требований 152-ФЗ, в том числе в рамках СТО БР ИББС
- Разработка систем управления информационной безопасностью в соответствии с ISO 27001, СТО БР ИББС

Сотрудники, привлекаемые для выполнения работ по проекту имеют:

- Сертификаты по СТО БР ИББС и опыт проведения проектов
- Сертификаты по созданию и аудиту СУИБ, построенных на базе стандартов семейства ISO/IEC 27000
- Опыт работы по проектам в области ПДн в банках
- Опыт работы в подразделениях ФСТЭК России
- Сертификаты о наличии вендорных статусов по лидирующим средствам защиты информации

«… в наше время верить никому нельзя, мне правда верить можно…»
(«Семнадцать мгновений весны, Мюллер, 9 серия»)

ДиалогНаука

Клиенты ЗАО «ДиалогНаука» из кредитно-финансового и страхового сектора

ДиалогНаука

Ключевые клиенты ЗАО «ДиалогНаука»

ДиалОгНаука

На стенде вас ждет

Компания представлена стендом, расположенным в холле конференц-зала

Вопросы

Спасибо за внимание!
Вопросы