ДиалогНаука

Практические аспекты защиты персональных данных у операторов связи

Корольков Сергей, BSI ISMS Lead Auditor
Техический директор
ЗАО «ДиалогНаука»

План презентации

- Часть 1. Законодательство по вопросам защиты ПДн
- Часть 2. Вопросы защиты ПДн у операторов
- Часть 3. О компании ЗАО «ДиалогНаука»
- Часть 4. Обсуждение и вопросы

ДиалогНаука

План презентации

Часть 1

Законодательство по вопросам защиты ПДн

ДиалогНаука

Используемые сокращения

- ПДн – Персональные данные
- ИСПДн - информационная система персональных данных
- СЗПДн - система защиты персональных данных
- ОРД – организационно-распорядительная документация

ДиалОгНаука

Основные понятия ФЗ «О персональных данных»

- **Оператор** - государственный орган, муниципальный орган, **юридическое или физическое лицо**, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных
- **Обработка персональных данных** - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных

ДиалОгНаука

Законодательная и нормативная база в области ПДн

Федеральный закон «О персональных данных» № 152-ФЗ с поправками

- **Оператор обязан принимать организационные и технические меры**, для защиты ПДн от НСД, уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий
- **Правительство РФ устанавливает требования** к обеспечению безопасности ПДн при их обработке
- **Федеральные органы в области обеспечения безопасности ПДн** (Роскомнадзор, ФСБ России, ФСТЭК России) осуществляют контроль и надзор
- **Лица, виновные в нарушении требований несут** гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность

ДиалОгНаука

Документы, разработанные на основе ФЗ «О персональных данных»

- Постановление Правительства РФ от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности ПДн при их обработке в ИСПДн"
- Постановление Правительства РФ от 15 сентября 2008 г. N 687 Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации
- Приказ ФСТЭК, ФСБ, Мининформсвязи от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации ИСПДн»
- Приказ ФСТЭК от 5 февраля 2010 г. N 58 «Об утверждении Положения о методах и способах защиты информации в ИСПДн»

- **Отраслевой стандарт по защите персональных данных для операторов связи (НИР «ТРИТОН»)**

ДиалогНаука

Изменения в законодательной базе в области ПДн

Готовится большое количество изменений в ФЗ «О персональных данных»

- Вопросы сбора согласий на обработку
- Вопросы формирования требований к защите ПДн. Возможно будет легализованы отраслевые стандарты по защите ПДн
- Изменения в форму согласия на обработку

ДиалогНаука

Ключевые положения законодательства в области ПДн

- Необходимо выполнить уже действующие требования ФЗ-152
- Информационные системы персональных данных, созданные до 1 января 2010 года, должны быть приведены в соответствие с требованиями настоящего Федерального закона **не позднее 1 июля 2011 года**
- В ИСПДн К1 применяются СЗИ, соответствующие 4 уровню контроля отсутствия недекларированных возможностей
- В ИСПДн применяются СЗИ, прошедшие процедуру оценки соответствия. Сама процедура в отношении ИСПДн в настоящий момент не определена.
- Оценка соответствия ИСПДн не требуется, но рекомендуется

ДиалогНаука

Проверки Регуляторами

Плановые и внеплановые проверки проводятся в форме **документарной** или **выездной** проверки

Плановые:

- Плановые проверки проводятся на основании ежегодного плана проведения плановых проверок на текущий календарный год
- Плановые проверки проводятся в отношении Операторов, включенных в Реестр операторов, осуществляющих обработку персональных данных (далее – Реестр), а также в отношении Операторов, не включенных в Реестр, но осуществляющих обработку персональных данных

Внеплановые:

- Истечение срока исполнения Оператором ранее выданного предписания об устранении выявленного нарушения
- Поступление в или ее территориальные органы обращений и заявлений
- Нарушение прав и законных интересов граждан действиями (бездействием) Операторов при обработке их персональных данных.
- Нарушение Операторами требований законодательства РФ в области персональных данных

ДиалОгНаука

Запрашиваемые документы

- учредительные документы Оператора;
- копия уведомления об обработке персональных данных;
- положение о порядке обработки персональных данных;
- положение о подразделении, осуществляющем функции по организации защиты персональных данных;
- должностные регламенты лиц, имеющих доступ и (или) осуществляющих обработку персональных данных;
- план мероприятий по защите персональных данных;
- план внутренних проверок состояния защиты ПДн;
- приказ о назначении ответственных лиц по работе с ПДн;
- типовые формы документов, предполагающие или допускающие содержание персональных данных;

ДиалОгНаука

Запрашиваемые документы

- журналы, реестры, книги, содержащие ПДн, необходимые для однократного пропуска субъекта ПДн на территорию, на которой находится Оператор;
- договоры с субъектами ПДн, лицензии на виды деятельности, в рамках которых осуществляется обработка персональных данных;
- выписки из ЕГРЮЛ, содержащие актуальные данные на момент проведения проверки;
- приказы об утверждении мест хранения материальных носителей персональных данных;
- письменное согласие субъектов на обработку их ПДн;
- распечатки электронных шаблонов полей, содержащие ПДн;

ДиалОгНаука

Запрашиваемые документы

- справки о постановке на балансовый учет ПЭВМ, на которых осуществляется обработка ПДн;
- заключения экспертизы ФСБ России, ФСТЭК России об оценке соответствия СЗИ, предназначенных для обеспечения безопасности ПДн при их обработке;
- приказ о создании комиссии и акты проведения классификации ИСПДн;
- журналы (книги) учета обращений граждан (субъектов персональных данных);
- акт об уничтожении персональных данных субъекта(ов) ПДн (в случае достижения цели обработки);
- иные документы, отражающие исполнение Оператором требований законодательства РФ в области ПДн

ДиалОгНаука

Ответственность

- **Меры по приостановлению или прекращению обработки ПДн**, осуществляемой с нарушением требований ФЗ «О персональных данных»
- **Направление в органы прокуратуры, другие правоохранительные органы материалов** для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн
- **Конфискация несертифицированных средств защиты информации** (в т.ч. основного оборудования и программного обеспечения ИС, т.к. персональные данные обрабатываются непосредственно в ИС, а средства защиты интегрированы в стандартное оборудование и программное обеспечение ИС)
- **Конфискация используемых средств шифрования**
- **Привлечение к административной и уголовной ответственности** лиц, виновных в нарушении соответствующих статей уголовного и административного кодекса

ДиалогНаука

Что должен сделать оператор

- Зарегистрироваться в реестре операторов
- Классифицировать ИСПДн
- Выполнить требования по обработке ПДн
- Выполнить требования по обработке ПДн без использования средств автоматизации
- Принять организационные и технические меры по защите ПДн
- Привести ИСПДн в соответствие требованиям по безопасности информации по не позже 1 июля 2011 года

ДиалогНаука

План презентации

Часть 2

Вопросы защиты ПДн у операторов связи

ДиалОгНаука

ИСПДн у операторов связи

- Операторы связи, как правило, обладают следующими ИСПДн:
  - Кадровый учет и бухгалтерия
  - Биллинговые системы
  - CRM
  - Личные кабинеты
  - Заявки на подключения на web сайте
  - Контакт-центры

ДиалОгНаука

Биллинговые системы

- Как правильно классифицировать биллинговую систему
- «Трехглавый приказ» не дает точно ответа о том, какая категория ПДн обрабатывается в биллинговых системах
- Рекомендуем использовать отраслевой стандарт для снижения класса ИСПДн

ДиалОгНаука

Личные кабинеты пользователей

- Формально личные кабинеты должны быть обезличены
- или должна обеспечиваться защита с использованием сертифицированных СКЗИ
  - На рабочей станции пользователя должно быть установлено СКЗИ

ДиалОгНаука

Заявки на подключения

- В настоящий момент, процесс сбора заявок на подключение, заполняемых на сайтах операторов, противоречат требованиям ФЗ-152
- Согласие на обработку персональных данных должно быть получено в письменном виде

ДиалОгНаука

Голосовая обработка ПДн

При ведении голосовой обработки ПДн необходимо принимать ряд организационно-технических мероприятий:

- Размещение помещения контакт-центра внутри офиса
- Проведение замеров утечек по акустическому каналу и установка средств зашумления, если например окна центра выходят на улицу

ДиалогНаука

Пакет ОРД

№	Название	Содержание	Пояснения
1.	Приказ «О создании рабочей группы по приведению информационных систем персональных данных в соответствие с требованиями Федерального Закона «О персональных данных»	Назначает рабочую группу по организации работ по обеспечению безопасности персональных данных, ее обязанности, полномочия, сроки.	Необходимо принять приказ в Организации
		Приложение 1. Состав рабочей группы	Рекомендуется включать в состав рабочей группы представителей заинтересованных подразделений компании участвующих в обработке ПДн.
		Приложение 2. План мероприятий по защите персональных данных	Необходимо разработать и сформировать план работ в соответствии со спецификой вашей организации. В таблице приведены некоторые этапы плана в качестве примера. В план работ должны входить как минимум проведение работ по разработке документов составляющих настоящий пакет.
2.	Приказ «О создании комиссии по классификации информационных систем персональных данных»	Назначает Комиссию по классификации информационных систем персональных данных, ее обязанности, полномочия, сроки.	Необходимо принять приказ в Организации
		Приложение 1. Состав Комиссии	Рекомендуется включать в состав рабочей группы представителей заинтересованных подразделений компании участвующих в обработке ПДн.
3.	Приказ «Об утверждении актов классификации информационных систем персональных данных»	Утверждает и вводит в действие акты классификации информационных систем персональных данных.	Необходимо указать названия всех ИСПДн и принять приказ в Организации.
		Приложения: Акты классификации	Необходимо заполнить для каждой ИСПДн Организации шаблон Акта классификации руководствуясь Приказом ФСТЭК/ФСБ/Мининформсвязи от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных». Акт шаблона является примерным и может быть изменен в соответствии с характеристиками Организации.
4.	Приказ «Об утверждении частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных»	Утверждает и вводит в действие «Частную модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».	Необходимо принять приказ в Организации.
		Приложение 1. «Частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».	Необходимо для каждой специальной ИСПДн организации (если ИСПДн обладают одинаковыми характеристиками, то целесообразно разрабатывать одну общую модель) разработать частную модель угроз. Частная модель угроз безопасности ПДн может разрабатываться Оператором, а может и организацией, обладающей лицензией ФСТЭК на деятельность по технической защите информации. В обоих случаях Частные модели угроз подлежат утверждению. Разработка модели угроз производится в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их

ДиалогНаука

Типовой пакет ОРД

№	Название	Содержание	Пояснения
			обработке в информационных системах персональных данных и Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных утвержденных ФСТЭК (см. папку «Методические документы»). Приведенные в шаблоне Модели угроз названия ИСПДн, характеристики ИСПДн, угрозы, возможные пути реализации угроз, применяемые контрмеры приведены для примера и подлежат обязательной актуализации в соответствии с характеристиками конкретной информационной системы.
		Приложение 2. «Модель нарушителя».	В случае использования в ИСПДн средств криптографической защиты, необходимо разработать Модель нарушителя. Модель нарушителя может разрабатываться Оператором, а может и организацией, обладающей лицензией ФСТЭК на деятельность по технической защите информации. В обоих случаях Модели нарушителя подлежат утверждению. Разработка Модели нарушителя производится в соответствии с методическими документами ФСБ. Приведенные в шаблоне Модели нарушителя названия ИСПДн, характеристики ИСПДн, угрозы, возможные пути реализации угроз, применяемые контрмеры категории нарушителей приведены для примера и подлежат обязательной актуализации в соответствии с характеристиками конкретной Организации.
5.	Приказ «О введении в действие перечня обрабатываемых персональных данных, перечня информационных систем персональных данных и перечня подразделений и сотрудников, допущенных к работе с персональными данными».	Утверждает и вводит в действие Перечень обрабатываемых персональных данных, Перечень информационных систем персональных, Перечень подразделений и должностей, допущенных к работе с персональными данными	Необходимо принять приказ в Организации.
		Приложение 1. Перечень обрабатываемых персональных данных.	Необходимо сформировать перечень обрабатываемых в Организации персональных данных в соответствии с предлагаемым шаблоном.
		Приложение 2. Перечень информационных систем персональных.	Необходимо сформировать перечень ИСПДн Организации в соответствии с предлагаемым шаблоном. Характеристики ИСПДн могут быть выбраны другие, более точно определяющие ее.
		Приложение 3. Перечень подразделений и должностных лиц, допущенных к работе с персональными данными.	Необходимо сформировать перечень подразделений и должностей, которым необходим доступ к персональным данным для выполнения должностных обязанностей
6.	Приказ «Об организации работ по обеспечению безопасности	Утверждает и вводит в действие внутренние документы по организации работ и обеспечению безопасности	Необходимо принять приказ в Организации

Типовой пакет ОРД

№	Название	Содержание	Пояснения
	персональных данных»	персональных данных.	
		Приложение 1 к Приказу. Положение об обработке персональных данных.	Основополагающий документ, определяющий основные принципы, цели, задачи, порядок автоматизированной и неавтоматизированной обработки персональных данных работников, клиентов и контрагентов, роли и ответственность должностных лиц. В положении приведены категории персональных данных, названия подразделений для примера. Требования положения должны быть актуализированы в соответствии с технологиями обработки ПДн, в том числе неавтоматизированной обработки
		Приложение 2 к Приказу. Положение об организации и обеспечении защиты персональных данных.	Документ, определяющий основные подходы, принципы, цели, задачи, порядок к обеспечению безопасности при автоматизированной и неавтоматизированной обработке персональных данных работников, клиентов и контрагентов, роли и ответственность должностных лиц.
		Приложение 3 к Приказу. Положение о подразделении, осуществляющем функции по организации и обеспечению защиты персональных данных	Типовое положение о подразделении определяет цели, задачи, права и обязанности подразделения, на которое возлагается защита персональных данных в Компании. Названия, организационная структура отдела, функции отдела приведены в Положении для примера и требуют актуализации для каждой конкретной Организации. Организация может дополнить предлагаемый документ положениями в соответствии со своими потребностями.
		Приложение 4 к Приказу. Типовая форма дополнительного соглашения по изменению трудового договора с сотрудниками.	Содержит дополнения в разделы типовых трудовых договоров о соблюдении конфиденциальности персональных данных, а также дополнительные соглашения к трудовым договорам с работниками Организации. Организация может дополнить предлагаемый документ положениями в соответствии с трудовым договором, заключенным с конкретным работником и в соответствии со своими потребностями.
		Приложение 5 к Приказу. Дополнения в должностные инструкции лиц участвующих в обработке персональных данных.	Содержит изменения и дополнения в разделы должностных инструкций ответственных лиц и сотрудников в части обеспечения безопасности персональных данных. Текст данного дополнения необходимо внести в должностные инструкции всех сотрудников Организации, имеющих доступ к ПДн.
		Приложение 6 к Приказу. Инструкции работнику по обеспечению безопасности при работе с персональными данными	Типовая инструкция работнику по работе с ПДн. Инструкция содержит общие требования и правила по работе с информационными системами персональных данных, права, обязанности и ответственность пользователей. В зависимости от классов ИСПДн требования, приведенные в инструкции, могут различаться. В зависимости от классов ИСПДн, их количества и количества пользователей, допущенных к каждой ИСПДн возможно выпуск одной общей инструкции по работе в ИСПДн или инструкции для каждой

ДиалогНаука

Типовой пакет ОРД

№	Название	Содержание	Пояснения
			ИСПДн
		Приложение 7 к Приказу. Инструкция администраторам безопасности информационных систем персональных данных.	Типовая инструкция содержит общие требования и правила по работе с информационными системами персональных данных, права, обязанности и ответственность администраторов безопасности. В зависимости от классов ИСПДн требования, приведенные в инструкции, могут различаться. В зависимости от классов ИСПДн, их количества и количества пользователей, допущенных к каждой ИСПДн возможно выпуск одной общей инструкции по работе в ИСПДн или инструкции для каждой ИСПДн.
		Приложение 8 к Приказу. Инструкция по действиям в случае компрометации ключевой информации.	Типовая инструкция по действию в случае компрометации ключевой информации. Определяет порядок действий при компрометации ключевой информации. В инструкции необходимо учесть требования и положения документации к конкретным используемым СКЗИ в Организации.
		Приложение 9 к Приказу. План внутренних проверок состояния защиты персональных данных.	Типовая форма плана проверок. Содержит перечень проверок с описанием области проверки, содержания проверки, сроков проведения проверок, ресурсов используемых при проверке, ответственных за проверку, результата проверки, мероприятий рекомендуемых для проведения по результатам проверки
		Приложение 10 к Приказу. Перечень мест хранения материальных носителей персональных данных, обрабатываемых без использования средств автоматизации.	Определяет перечень мест хранения материальных носителей персональных данных, обрабатываемых без использования средств автоматизации
7.	Форма Акта внедрения средств защиты информации	Форма Акта внедрения	Типовая форма акта содержит результаты установки и настройки средств защиты информации. В соответствии с потребностями Организации типовая форма должна быть изменена.
		Приложение 1. Настройки СЗИ	Типовая форма для отражения настроек СЗИ. В соответствии с потребностями Организации типовая форма должна быть изменена.
8.	Приказ «О назначении комиссии по проведению оценки соответствия информационных систем персональных данных требованиям безопасности»	Определяет состав комиссии по проведению оценки соответствия информационных систем персональных данных требованиям безопасности	Необходимо принять приказ в Организации в случае проведения самостоятельной оценки по результатам реализации системы защиты
		Приложение 1. Состав комиссии	Необходимо определить состав комиссии.
		Приложение 2. Заключение по результатам оценки соответствия информационной системы персональных данных требованиям по безопасности	Типовая форма Заключения по результатам оценки соответствия. В зависимости от класса ИСПДн, используемых технологий обработки ПД, применяемых СЗИ и СКЗИ, требований документации типовая форма должна быть доработана под конкретную ИСПДн. Приведен типовой набор технических требований для ИСПДн класса К1 (максимальный).

ДиалОгНаука

Техническое задание

- Рекомендуем составлять Техническое задание на создание системы защиты персональных данных
- Оценка соответствия, которая должна проводится по требованиям ПП 781, проводится на соответствие требованиям по обеспечению безопасности ПДн

План презентации

Часть 3

О компании ЗАО «ДиалогНаука»

ДиалогНаука

Членство в ассоциациях

- Межрегиональная общественная организация «Ассоциация защиты информации» (АЗИ)
- Ассоциации документальной электросвязи (АДЭ)
- Сообщество ABISS (Association of Banking Information Security Standards)
- Сертифицированный партнер BSI Management Systems
- Ассоциация IT компаний «Инфорус»

ABISS АДЭ АЗИ BSI

ДиалогНаука

Лицензии и аттестаты компании «ДиалогНаука»

- Лицензия ФСТЭК на деятельность по разработке и (или) производству средств защиты конфиденциальной информации
- **Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации.**
- Лицензия ФСБ на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем. Регистрационный номер 3237 П от 15 июня 2006 г
- **Лицензия ФСБ на осуществление технического обслуживания шифровальных (криптографических) средств**
- **Лицензия ФСБ на распространение шифровальных (криптографических) средств**
- Лицензия ФСБ на предоставления услуг в области шифрования информации
- **Аттестат аккредитации органа аттестации** в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 для проведения аттестации объектов информатизации

ДиалОгНаука

Услуги ЗАО «ДиалогНаука» в области защиты ПДн

- **Обследование ИСПДн** компании на соответствие требованиям Федерального закона «О персональных данных»
- **Разработка системы защиты персональных данных**, обрабатываемых в информационных системах Заказчика
- **Поставка, установка и настройка средств защиты информации** для обеспечения безопасности персональных данных
- **Подготовка к оценке соответствия** информационных систем Заказчика по требованиям безопасности информации
- **Оценка соответствия** информационных систем персональных данных Заказчика по требованиям безопасности информации

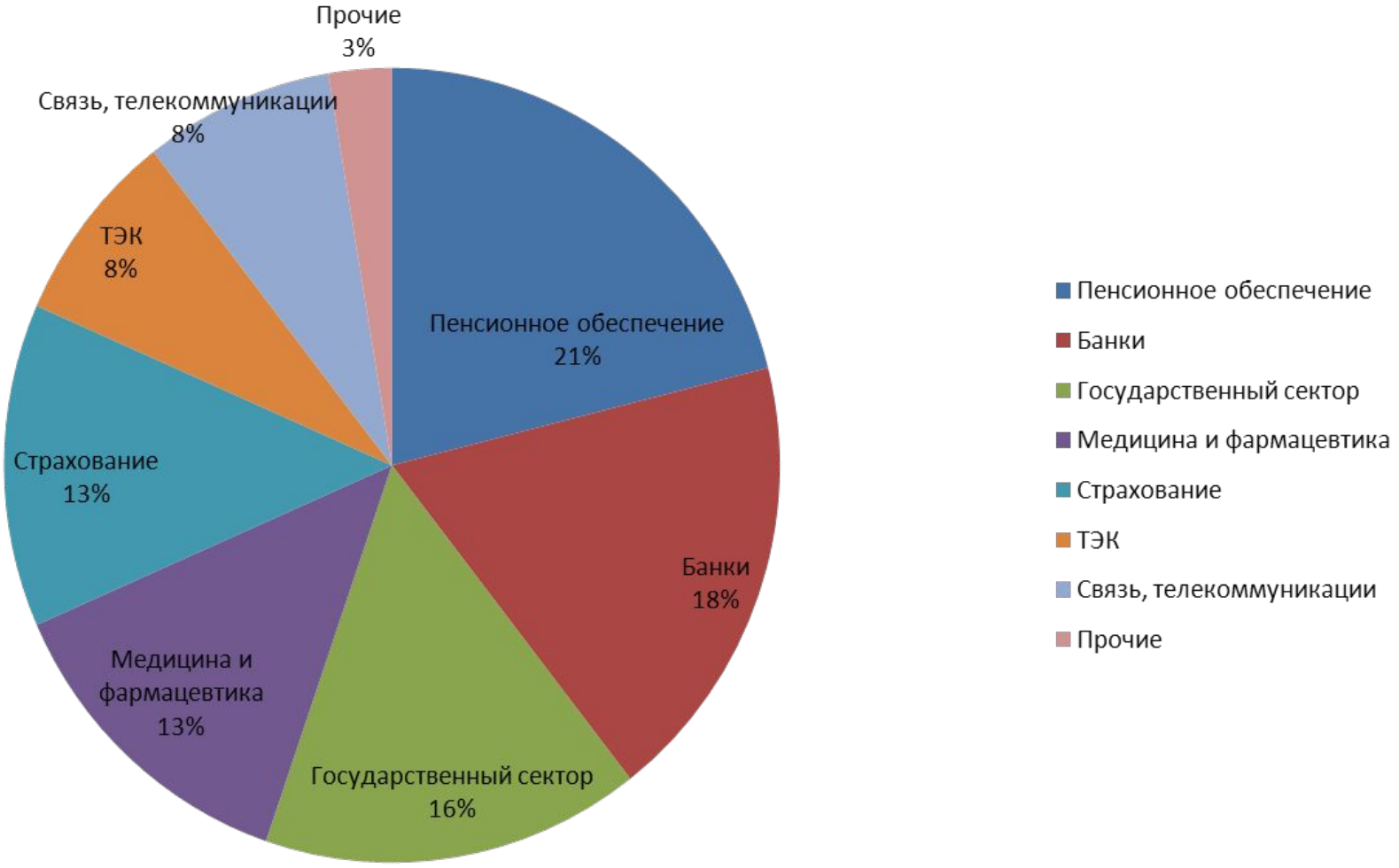
ДиалогНаука

Ключевые клиенты ЗАО «ДиалогНаука»

ДиалОгНаука

Проекты по выполнению требований 152-ФЗ

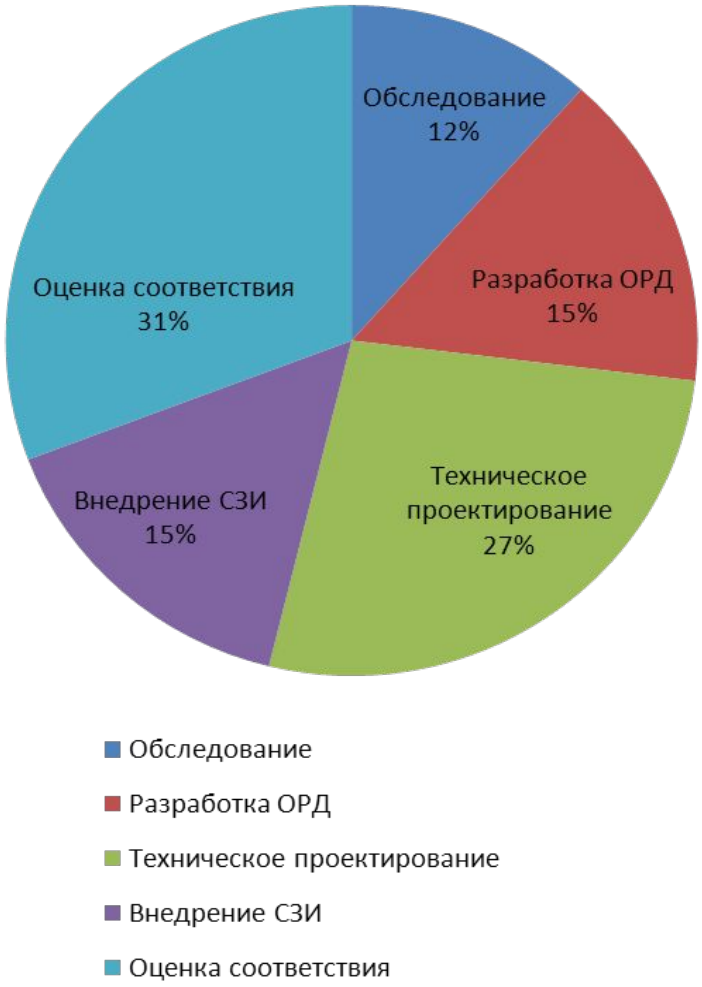
Заказчики услуг по персональным данным



ДиалогНаука

Проекты по выполнению требований 152-ФЗ

Распределение конечных стадий выполняемых проектов



88 процентов от общего количества Заказчиков утвердило организационно-распорядительную документацию и привели процессы обработки ПДн в соответствие требованиям

46 процентов проектов завершились внедрением полного комплекса средств защиты, соответствующих требованиям нормативных документов по защите

31 процент выбрали проведение итоговой оценки соответствия в виде добровольной аттестации ИСПДн

Только ***12 процентов*** от общего количества Заказчиков приостановили реализацию мер по защите ПДн после обследования (классификации ИСПДн)

План презентации

Часть 4

Обсуждение и вопросы

Контакты

Корольков Сергей, Технический директор ЗАО «ДиалогНаука»

Тел.: +7(495) 980-67-76 доб. 163, Факс: +7(495) 980-67-75

URL: http://www.DialogNauka.ru, E-mail: sergeysergey.sergey.korolkovsergey.korolkov@sergey.korolkov@dialognaukasergey.korolkov@dialognauka.sergey.korolkov@dialognauka.ru