СЛОЖНОСТИ И ОШИБКИ ПРИ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ

Илья Романов
CISA, CISM, PMP
Руководитель Отдела консалтинга
АО «ДиалогНаука»

ДиалогНаука

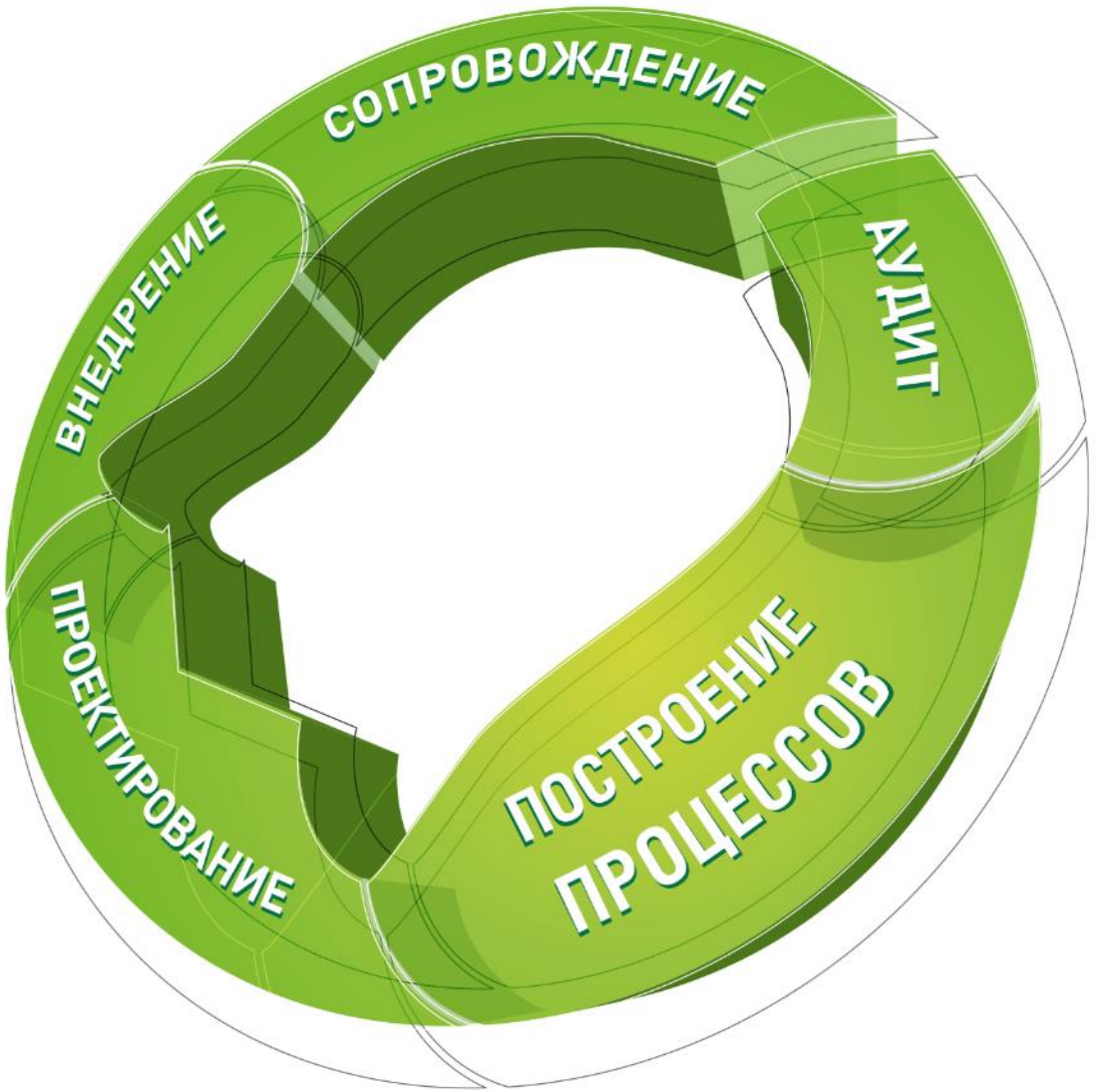
О компании

ДиалогНаука

- Создана в 1992 году СП «Диалог» и Вычислительным центром РАН.
- Первые продукты – ревизор ADinf, антивирусы Aidstest и Dr. WEB.
- В настоящее время – системный интегратор в области информационной безопасности.

Направления деятельности

- 152-ФЗ и GDPR
- Объекты КИИ (187-ФЗ)
- PCI DSS
- 382-П, 672-П, 683-П, 684-П
- ГОСТ 57580
- ISO 27001
- АСУ ТП
- Коммерческая тайна
- Сведения ДСП
- Защита ГИС



О компании «ДиалогНаука»: ключевые клиенты

Почему Вы – Оператор ПДн?

https://77.rkn.gov.ru/p30400/p32622/

КАК УЗНАТЬ, ЯВЛЯЕТЕСЬ ЛИ ВЫ ОПЕРАТОРОМ ПЕРСОНАЛЬНЫХ ДАННЫХ

и нужно ли подавать уведомление об обработке персональных данных в Роскомнадзор?

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Порядок проверки РКН

1. Запрос о предоставлении документов
   - «общие» вопросы
   - ОРД по вопросам обработки и защиты ПДн
   - типовые формы, анкеты, согласия, договоры
   - сведения об ИСПДн
   - сведения о сайтах и Интернет-сервисах

2. Обследование на месте (вы показываете самостоятельно):
   - информационные системы
   - документы

3. Точечные запросы
   - уточнения по реализации процессов
   - примеры, скриншоты и иные свидетельства реализации процессов
   - уточнение правовых оснований

Некорректное уведомление

Нарушение 1. Некорректное уведомление.

1.1. Учтены не все сведения:

- Обработка сведений о посетителях Интернет-сайтов
- Национальность (свидетельство о заключении брака)
- Причина увольнения (анкета кандидата)

1.2. Указаны не все меры по защите:

- Оценка вреда субъектам
- Ознакомление работников с законодательством и требованиями

Уведомление об обработке ПДн

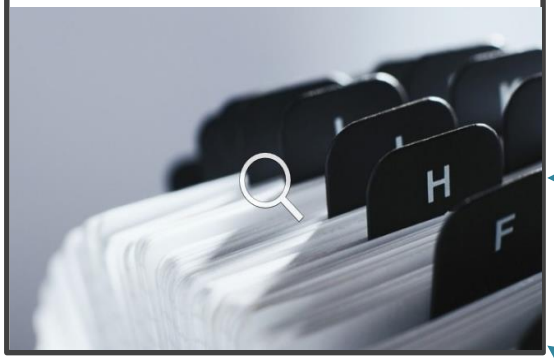
Отдел бухгалтерского учета

Отдел персонала

Отдел Информационных технологий

Юридический отдел

Персональные данные



Бизнес отделы

Финансовый

Администрация

Сторонние организации

Уведомление об обработке ПДн

Этап	Работы	Применяемые АО «ДиалогНаука» методы и подходы
1. Обследование	Процессы обработки ПДн, документация, типовые формы,…	• Интервью • Анкетирование • Анализ исходной документации • Анализ сайтов и информационных систем
	Информационные системы, средства защиты	
2. Разработка документации	Организационно-распорядительные документы, формы согласий, проект уведомления Роскомнадзора,…	• Учитывается имеющаяся документация Заказчика и применяемые средства защиты • Согласование документации и технических решений • Учет пожеланий, рассмотрение различных вариантов реализации
	Техническая документация на систему защиты – определение угроз, адаптация мер, техническое проектирование,…	
3. Внедрение средств защиты	Программы и протоколы испытаний, Акты внедрения,…	• При необходимости – корректировка, доработка документации
4. Оценка эффективности мер (1 раз в 3 года)	Аттестация, или оценка соответствия	• На основании лицензий ФСТЭК и ФСБ, в соответствии с нормативными документами регуляторов
Корректное уведомление об обработке ПДн (уведомление об изменениях)		
5. Сопровождение	Консультации, актуализация документации, сопровождение при проверках	• Очно • По телефону • По электронной почте

ПДн рекомендателей кандидатов

Нарушение 2. Обработка ПДн рекомендателей кандидатов.

…выявлен факт обработки персональных данных рекомендателей в объеме:

- ФИО,
- место работы и должность,
- телефон.

Правовым основанием обработки персональных данных рекомендателей в данном случае является согласие на обработку их персональных данных.

Нарушение сроков обработки (хранения)

Нарушение 3. **Нарушение сроков обработки (хранения).**

3.1. Анкета кандидата на работу (обработка по достижению целей)

3.2. Хранение в ИСПДн персональных данных работников, уволенных свыше 5 лет на момент проверки

Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн (ч. 7 ст. 5 ФЗ-152)

Нарушение требований к согласию

Нарушение 4. Нарушение требований к согласию в письменной форме

…при передаче персональных данных работников в адрес

- ПАО «Страховая Компания»
- ПАО «Туристическое Агентство»
- ПАО «Такси»

используется письменное согласие работников, несоответствующее требованиям ч. 4. ст. 9 ФЗ-151, что влечет за собой нарушение ст. 88 ТК РФ. **Представленное согласие работника содержит несколько целей обработки персональных данных.**

Письменные согласия на обработку ПДн

- 152-ФЗ:
  - Согласие на обработку ПДн может быть дано в любой позволяющей подтвердить факт его получения форме.
  - В отдельных случаях – только письменное согласие, содержащее ЦЕЛЬ обработки персональных данных.
- ТК РФ
  - Не сообщать ПДн работника третьей стороне без письменного согласия работника.

Цель может быть только одна

- 152-ФЗ:
  - Согласие на обработку ПДн может быть дано в любой позволяющей подтвердить факт его получения форме.
  - В отдельных случаях – только письменное согласие, содержащее ЦЕЛЬ обработки персональных данных.
- ТК РФ
  - Не сообщать ПДн работника третьей стороне без письменного согласия работника.
- Вывод
  - В случае передачи ПДн работников (за рамками ТК) нужны отдельные письменные согласия под каждую цель (зарплатный проект, турагентства, ДМС и т.д.).
  - Аналогично и для других субъектов ПДн.

Суды придерживаются такой позиции Роскомнадзора.

Требования к поручению обработки ПДн

Нарушение 5. **Нарушение требований к поручению обработки ПДн**

…в поручении должны быть определены

- перечень действий (операций) с персональными данными;
- цели обработки;
- обязанность соблюдать конфиденциальность и обеспечивать безопасность ПДн;
- **требования к защите ПДн в соответствии со статьей 19 ФЗ-152**.

Поручение обработки ПДн

Оформление «Поручения обработки ПДн» требуется:

При передаче части функций и процессов обработки ПДн Компанией сторонним организациям:

- осуществление пропускного режима арендодателем;
- расчет заработной платы;
- предоставление «внешних» ИТ-сервисов по хранению и обработке ПДн;
- предоставление услуг по обучению, семинары;
- оформление билетов и виз агентствами по оказанию соответствующих услуг

Передача ПДн третьим лицам

Нарушение 6. Незаконная передача третьим лицам

Передача ПДн третьим лицам при «аутсорсинге» процессов обработки ПДн **требует согласия субъектов ПДн.**

Примеры «аутсорсинга» процессов:

- хранение документов;
- ведение бухгалтерского учета;
- обработка анкет и заявлений клиентов;
- работа с ПДн при администрировании систем и баз данных.

Обработка ПДн из «открытых» источников

Нарушение 7. Незаконная обработка ПДн из «открытых» источников

Обработка ПДн на сервисах Авито, Вконтакте, Viber и др., осуществляется в соответствии с Правилами этих сервисов в строго определенных целях, например:

- установить контакт с потенциальным покупателем;
- выполнение обязательств перед пользователями;
- обрабатывать платежи.

Правила запрещают обработку ПД с иными целями.

Статья 5 ФЗ-152 определяет:

- обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей, **не допускается обработка ПДн, несовместимая с целями** (ч. 2);
- обработке подлежат только **персональные данные, которые отвечают целям их обработки** (ч.4).

ПДн разрешенные для распространения

30 декабря 2020 года N 519-ФЗ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О ВНЕСЕНИИ ИЗМЕНЕНИЙ
В ФЕДЕРАЛЬНЫЙ ЗАКОН "О ПЕРСОНАЛЬНЫХ ДАННЫХ"

Принят
Государственной Думой
23 декабря 2020 года

Одобрен
Советом Федерации
25 декабря 2020 года

Статья 1

Внести в Федеральный закон от 27 июля 2006 года N 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; 2010, N 31, ст. 4173, 4196; N 49, ст. 6409; 2011, N 23, ст. 3263; N 31, ст. 4701; 2013, N 14, ст. 1651; N 30, ст. 4038; N 51, ст. 6683; 2014, N 23, ст. 2927; N 30, ст. 4217, 4243; 2016, N 27, ст. 4164; 2017, N 27, ст. 3945; N 31, ст. 4772; 2018, N 1, ст. 82; 2019, N 52, ст. 7798; 2020, N 17, ст. 2701) следующие изменения:

1) статью 3 дополнить пунктом 1.1 следующего содержания:

"1.1) персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;";

2) пункт 10 части 1 статьи 6 признать утратившим силу;

3) статью 9 дополнить частью 9 следующего содержания:

"9. Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, устанавливаются уполномоченным органом по защите прав субъектов персональных данных.";

4) пункт 2 части 2 статьи 10 изложить в следующей редакции:

"2) обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 настоящего Федерального закона;";

Федеральный закон от 30.12.2020 N 519-ФЗ вносит изменения в 152-ФЗ с 1 марта 2021 года

- Новое понятие в 152-ФЗ – «персональные данные, разрешенные субъектом для распространения»
- Введена Статья 10.1. - Особенности обработки ПДн, разрешенных субъектом ПДн для распространения

Статья 10.1 – Особенности обработки…

- Отдельное согласие на распространение ПДн
- Если субъект сам разместил ПДн на общедоступном ресурсе, то это не дает оснований для распространения и иной обработки ПДн
- Роскомнадзор готовится к запуску информационной системы для сбора согласий на обработку разрешенных для распространения персональных данных (http://www.garant.ru/news/1452912/)
- В согласии на обработку ПДн, разрешенных субъектом ПДн для распространения, субъект ПДн вправе установить запреты на передачу (кроме предоставления доступа) этих ПДн оператором неограниченному кругу лиц
- Передача (распространение, предоставление, доступ) ПДн, разрешенных субъектом ПДн для распространения, должна быть прекращена в любое время по требованию субъекта ПДн.

Согласие на распространение

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ (РОСКОМНАДЗОР)

ПРИКАЗ

_____ №_____

Москва

Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения

В соответствии с частью 9 статьи 9 Федерального закона «О персональных данных» от 27 июля 2006 г. № 152-ФЗ (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2021, № 1, ст. 58), абзацем 2 пункта 1 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16 марта 2009 г. № 228 (Собрание законодательства Российской Федерации, 2009, № 12, ст. 1431; 2020, № 21, ст. 3281), п р и к а з ы в а ю:

1. Утвердить требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

Руководитель А.Ю. Липов

- Ф.И.О. субъекта
- Контактная информация субъекта
- Наименование оператора
- Цель (цели) обработки ПДн (должны соответствовать положениям законодательства и (или) политике оператора в отношении ПДн)
- Категории и перечень ПДн
- Условия и запреты обработки
- Срок действия
- Сведения об информационных ресурсах оператора (Интернет-адрес), посредством которых будет осуществляться предоставление доступа неограниченному кругу лиц и иные действия с ПДн

Почему модель угроз – это важно?

- Модель угроз ложится в основу системы защиты
- Результатами моделирования обосновывается выбор мер по защите и оценка их эффективности
- Тип актуальных угроз определяет требуемый уровень защищенности ПДн, обрабатываемых в ИСПДн

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ
об утверждении Методики оценки угроз безопасности информации
от 15 февраля 2021 г. № 240/22/690

В соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, ФСТЭК России разработана и утверждена 5 февраля 2021 г. Методика оценки угроз безопасности информации (далее – Методика).

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
5 февраля 2021 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

МОСКВА
2021

Методика оценки угроз

Область действия

- Предназначена для ИСПДн, ГИС, МИС, ОКИИ, АСУ, ОПК, КВО, ИТКС, ЦОД, облака…
- Модели, утвержденные до утверждения Методики **(5 февраля 2021 г.)** продолжают действовать до модернизации объектов защиты
- Отменяются методики моделирования для ИСПДн и КСИИ

Общие подходы к моделированию

- Исходные данные
  - перечни и описания угроз (Банк данных угроз ФСТЭК, Указания ЦБ РФ и др.)
  - документация на объекты защиты – техническая, эксплуатационная, организационно-распорядительная
  - договоры с провайдерами ЦОД и других услуг
  - результаты оценки рисков
- Оценка угроз должна быть систематической
- Особенности для ЦОД – моделирование должно осуществляться в том числе для инфраструктуры ЦОД с участием провайдеров ЦОД
- Допустимо разрабатывать одну модель для нескольких систем

Методика оценки угроз

Порядок моделирования:

- определение негативных последствий (важно участие представителей «бизнеса»)
- определение объектов воздействия на всех уровнях (пользовательский, прикладной, системный, и т.д.)
- определение источников угроз (описание и оценка нарушителей);
- оценка способов реализации угроз;
- определение возможных и актуальных угроз (фактически все возможные угрозы являются актуальными)

Основные сложности

- Необходимость включения в состав разработчиков Модели
  - экспертов по ИБ (без их участия разработка невозможна в принципе);
  - лиц администрирующих и эксплуатирующих объект защиты.

- Большое количество не согласованных между собой требований:
  - Методика ФСТЭК
  - Приказ ФСБ № 378
  - Банк данных угроз
  - Указание ЦБ РФ № 3889-У

- Большое количество «темных» пятен в методике, сложная «логика» действий, отсутствие конкретики и инструкций по реализации ряда шагов.

- «Несовместимость» Методики с Банком данных угроз

Изменения в статье 13.11 КоАП (штрафы)

Вячеслав Володин в своем канале в Telegram сказал, что часто слышит на встречах с гражданами вопросы, как личные данные появляются в общем доступе и почему людям поступают десятки назойливых рекламных звонков.

«Это происходит из-за безответственности компаний, в том числе иностранных, которые собирают персональные данные граждан, чтобы использовать их для собственного обогащения. В погоне за прибылью они не думают о безопасности людей, не хотят или не могут обеспечить защиту их личных сведений. Это недопустимо», — считает Председатель ГД.

«Теперь за обработку персональных данных без письменного согласия их владельца организации придется заплатить штраф до 150 000 рублей. При повторном нарушении — до 500 000 рублей», — напомнил Вячеслав Володин.

«Работа в этом направлении будет продолжена. Мы посмотрим, как будут применяться нормы этого закона, и в случае необходимости примем дополнительные решения», — заключил он.

http://duma.gov.ru/news/51115/

Изменения в статье 13.11 КоАП (штрафы)

Часть	Нарушение	Должностные лица	Юридические лица
1	Незаконная обработка	20 000 (повторно 50 000)	100 000 (повторно 300 000)
2	Отсутствие (несоответствие требованиям) согласия в письменной форме	40 000 (повторно 100 000)	150 000 (повторно 500 000)
3	Отсутствие общедоступной политики	12 000	60 000
4	Непредоставление информации субъекту	12 000	80 000
5	Невыполнение требований субъекта / РКН	20 000 (повторно 50 000)	90 000 (повторно 500 000)
6	Невыполнение требований безопасности (неавтоматизированная обработка)	20 000	100 000
7	Нарушение требований по обезличиванию	12 000	---
8	Нарушение требований «локализации баз данных ПДн» *(без изменений)*	200 т (повторно 800 т)	6 млн (повторно 18 млн)

Сроки привлечения к ответственности

Сроки привлечения к ответственности за нарушение в области персональных данных (13.11 КоАП):

- было – 3 месяца;
- стало – 12 месяцев.

До настоящего времени с учетом всех бюрократических процедур Роскомнадзор зачастую «не успевал» накладывать штрафы.

Дальнейшие ожидания – увеличение числа штрафов на должностных и юридических лиц.

Сопровождение при проверках

Сопровождение при проверках.
Подход АО «ДиалогНаука».

- успешное прохождение проверок Роскомнадзора, ФСТЭК, ФСБ, ЦБ РФ, ФОМС;
- помощь в формировании письменных ответов на запросы;
- отстаивание позиции Заказчика (в том числе очное участие);
- оперативное устранение замечаний.

Наши контакты

117105, г. Москва, ул. Нагатинская, д. 1

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: info@DialogNauka.ru