ОБЗОР ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Илья Романов
Руководитель Отдела консалтинга
АО «ДиалогНаука»

ДиалогНаука

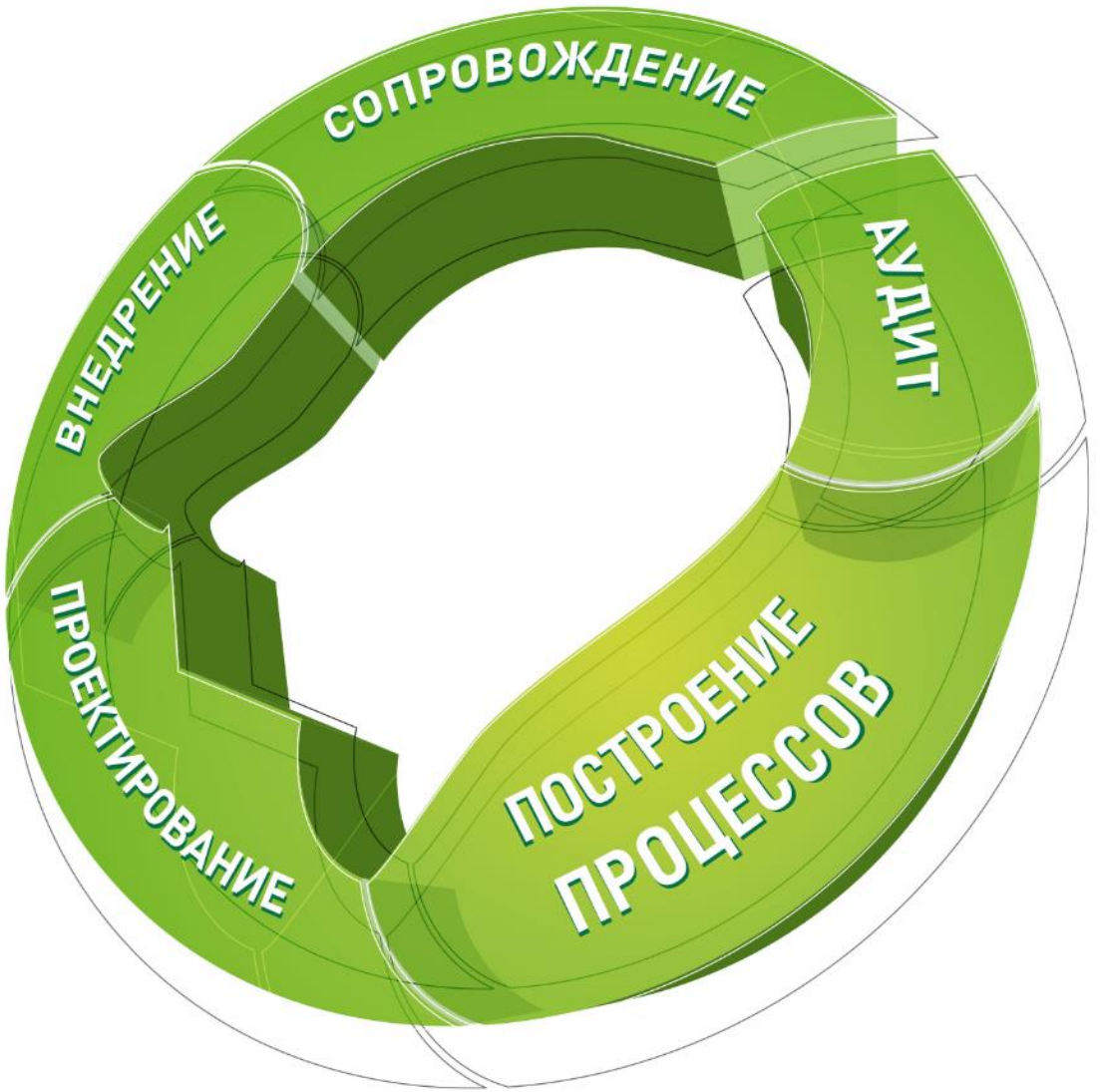
О компании

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

~~ОБЗОР ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ~~
~~В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ~~

ОБЗОР ИННОВАЦИЙ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

ДиалОгНаука

Изменения в законодательстве о ПДн

Новый тип ПДн – ПДн, разрешенные субъектом для распространения

Новая методика оценки угроз безопасности информации (в том числе ПДн)

Увеличение штрафов и сроков привлечения к ответственности

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»
- Понятие «общедоступных» ПДн утратило актуальность
- 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 поддержания Модели в актуальном состоянии
- Требование о включении в состав разработчиков Модели
  - экспертов по ИБ (без их участия разработка невозможна в принципе);
  - лиц администрирующих и эксплуатирующих объект защиты.
- Сложности при оценке возможных негативных последствий (отсутствие методики)
- Необходимость тщательной проработки описания нарушителей (обоснования)
- Сложности в описании сценариев реализации угроз
  - сценарии – 10 тактик, 145 техник
  - отсутствие четкой методики
  - необходимость широкой компетенции по ИБ
  - частичная «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.

А что с утечками ПДн и жалобами субъектов?

- За утечку ПДн, обрабатываемых в информационных системах, штрафы не предусмотрены.

- Однако, утечки ПДн и жалобы субъектов ПДн – основания плановых и **внеплановых** проверок Роскомнадзора (могут быть инициированы по решению Прокуратуры).

Участились случаи внеплановых проверок по ПДн со стороны

- Роскомнадзора (проверяют процессы обработки ПДн, и общие вопросы защиты ПДн)
- ФСБ России (проверяют вопросы, связанные с СКЗИ)

Штрафы и санкции РКН

- Блокировка интернет-сайтов
- Предписания (срок исполнения – 3 месяца)
- Штрафы
  - Умножение суммы штрафа на количество нарушений (новость на сайте РКН):

    В отношении Оператора ПДн составлено 5 протоколов об административном правонарушении по ч. 1 ст. 13.11 КоАП РФ. Судом назначен штраф на общую сумму 150 тысяч рублей.

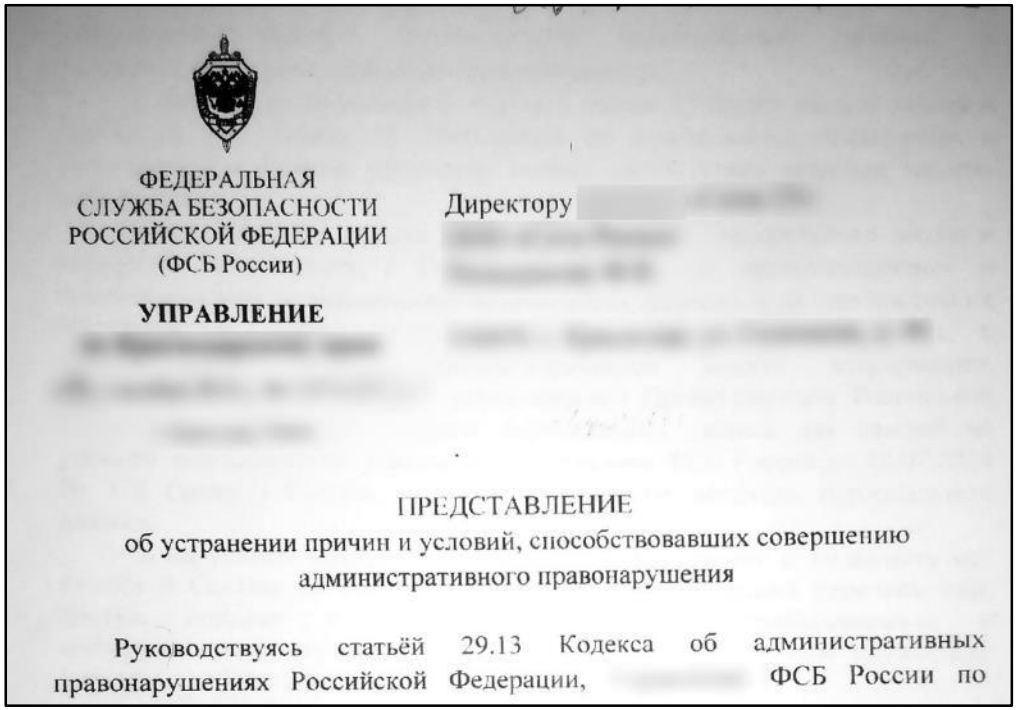
  - За нарушение требований о локализации баз ПДн (ч. 8-9 ст. 13.11 КоАП РФ):

    до 6 млн. рублей (первое нарушение)
    до 18 млн. рублей (повторное нарушение)

Проверки ФСБ

Результаты:

- штрафы (ч. 6, ст. 13.12 КоАП РФ) – от 10 000 рублей
- представления об устранении причин и условий (срок – 1 месяц в соответствии со ст. 29.13 КоАП РФ)



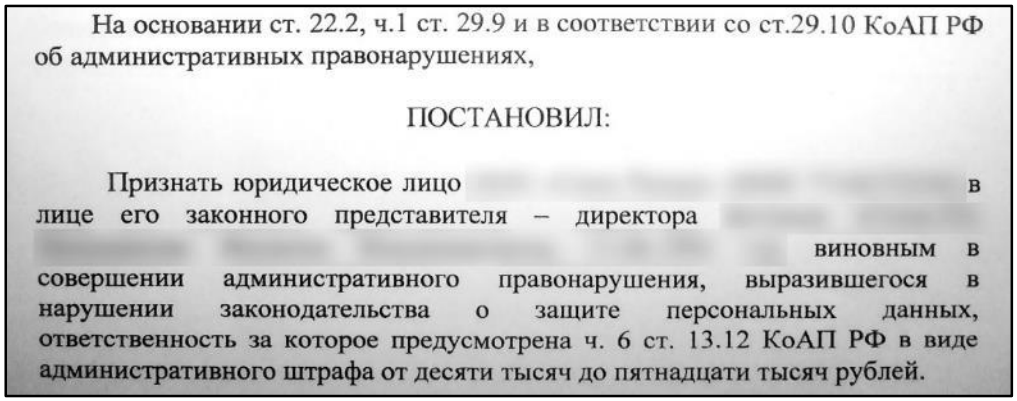
ФЕДЕРАЛЬНАЯ
СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(ФСБ России)

УПРАВЛЕНИЕ

Директору

ПРЕДСТАВЛЕНИЕ
об устранении причин и условий, способствовавших совершению административного правонарушения

Руководствуясь статьёй 29.13 Кодекса об административных правонарушениях Российской Федерации, ФСБ России по



На основании ст. 22.2, ч.1 ст. 29.9 и в соответствии со ст.29.10 КоАП РФ об административных правонарушениях,

ПОСТАНОВИЛ:

Признать юридическое лицо в лице его законного представителя – директора виновным в совершении административного правонарушения, выразившегося в нарушении законодательства о защите персональных данных, ответственность за которое предусмотрена ч. 6 ст. 13.12 КоАП РФ в виде административного штрафа от десяти тысяч до пятнадцати тысяч рублей.

Инциденты за время COVID-19

Инциденты ИБ в медицинской сфере за время COVID-19:

- В Астрахани распространяются персональные данные пассажиров злополучного авиарейса (выявлен коронавирус) – ссылка
- Персональные данные сахалинки с подозрением на COVID-19 распространили в соцсетях – ссылка
- В Якутии произошла утечка персональных данных граждан с коронавирусом – ссылка
- Паспортные данные оштрафованных за нарушение самоизоляции обнаружились в интернете – ссылка
- Данные жителей Подмосковья, заразившихся COVID-19, слили в Whatsapp – ссылка
- Названы имена заразившихся COVID-19 сотрудников НИИ скорой помощи им. Джанелидзе – ссылка
- Белгородцы с COVID-19 беспокоятся об утечке персональных данных – ссылка

Построение системы защиты

Целесообразно построение комплексной системы защиты, соответствующей требованиям (ПДн / ГИС / КИИ / ЦБ РФ).

Основные шаги при построении системы защиты:

- Определение состава объектов защиты (композиция / декомпозиция систем и элементов)
- Определение потенциальных угроз и нарушителей, классификация объектов защиты
- Определение (адаптация) требований, исходя из структурно-функциональных особенностей
- Техническое проектирование системы защиты
- Поставка, установка и настройка средств защиты информации
- Испытания и оценка эффективности принимаемых защитных мер.

Особенности построения системы защиты

Особенности построения системы защиты ПДн и КИИ:

- Важно правильно определить состав объектов защиты и предъявляемые требования (оптимизация)
- Необходимость использования средств защиты информации, прошедших оценку соответствия в установленном законодательством порядке
- С учетом потенциальных угроз и нарушителей часть защитных мер может реализовываться за счет внедрения организационных мероприятий (адаптация требований)
- Помимо формального выполнения требований законодательства **система защиты должна быть полезной** для организации (инвестирование в ИБ)

Сложности реализации требований по ИБ

- Большое количество обязательных нормативных документов по различным тематикам (ПДн, КИИ, ГИС, ЦБ РФ)
- Неоднозначность отдельных трактовок законодательства, необходимость изучения правоприменительной практики
- Необходимость реализации как технических, так и «бумажных» требований (разработка документации)
- Сложность и разнообразие применяемых систем и технологий (локальные системы, внешние облака, аутсорсеры и т.д.)
- Нарушители постоянно совершенствуют и усложняют используемые техники
- Для грамотного построения «полезной» системы защиты необходимы знания и опыт

Основные шаги и рекомендации

Основные шаги и рекомендации по построению системы защиты и приведению в соответствие требованиям законодательства :

- Назначение ответственных лиц
- Обязательное проведение обследования (уточнение состава защищаемой информации, процессов ее обработки, используемых систем и т.д.)
- Вовлечение всех «участников» информационного обмена – ИБ, ИТ, персонал систем, «бизнес»-подразделения, третьи стороны.

Приведение в соответствие GDPR и 152-ФЗ

Приведение в соответствие GDPR и 152-ФЗ:

1. Проведение обследования, выявление несоответствий
2. Актуализация процессов обработки ПДн, проектирование системы защиты
3. Внедрение процессов обработки ПДн и средств защиты информации
4. Мониторинг и контроль, сопровождение при проверках регуляторов

Основные этапы реализации Проекта по ПДн

Этап	Работы	Применяемые 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
5. Сопровождение	Консультации, актуализация документации, сопровождение при проверках	• Очно • По телефону • По электронной почте

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