ОБЗОР ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Илья Романов
Руководитель Отдела консалтинга
АО «ДиалогНаука»

ДиалогНаука

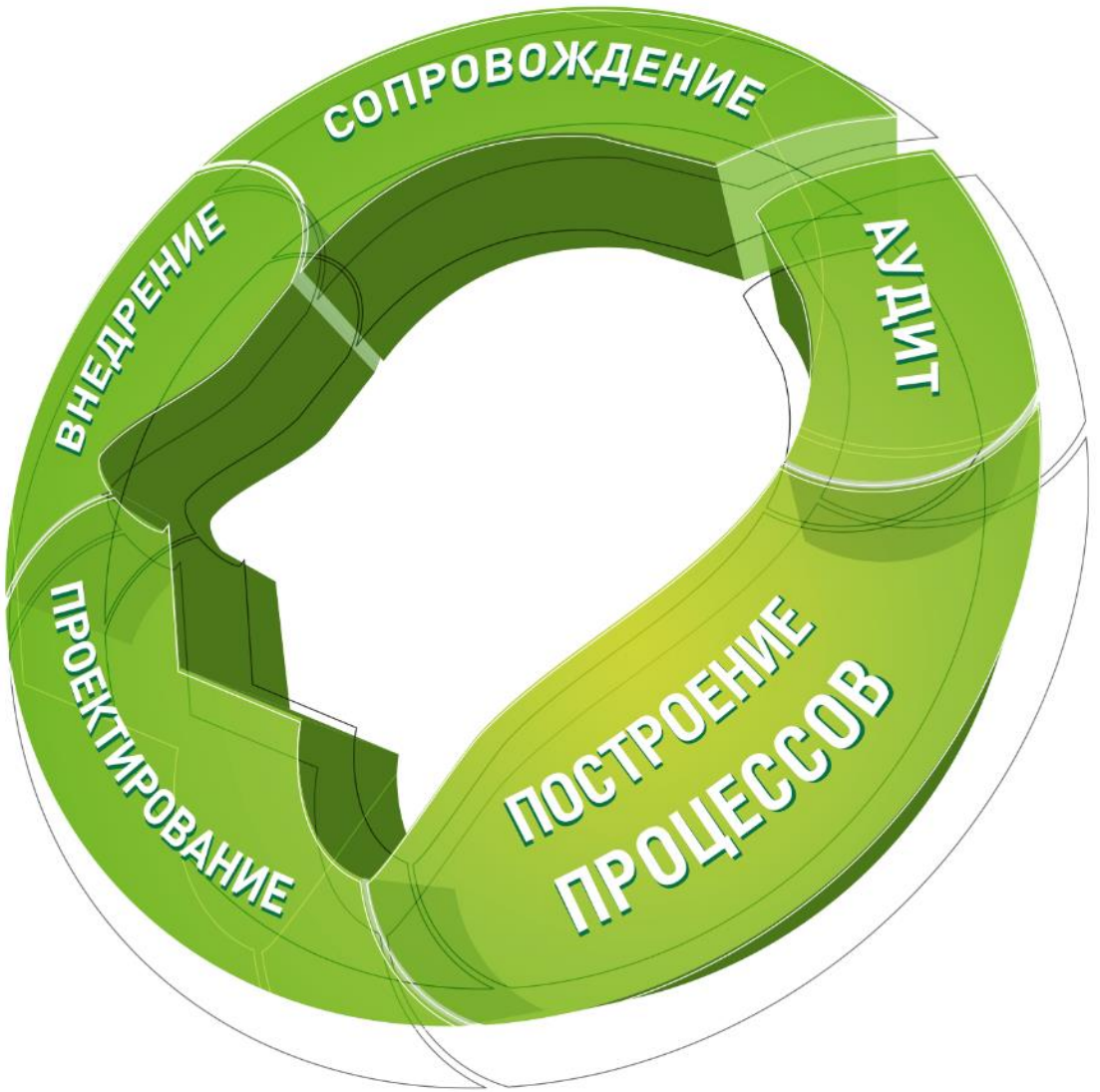
О компании

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)
- СТО БР ИББС
- PCI DSS
- 382-П, 672-П, 683-П, 684-П
- ISO 27001
- АСУ ТП
- Коммерческая тайна
- Сведения ДСП
- Защита ГИС



О компании «ДиалогНаука»: ключевые клиенты

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.

Использование тепловизоров

Разъяснения об использовании тепловизоров для предотвращения COVID-19:

- Температура тела – сведения о здоровье
- Согласие на обработку не требуется:
  - выявление заболевания работников = определение возможности выполнения трудовых функций (ст. 88 ТК РФ)
  - посетители выражают согласие посредством конклюдентных действий
- Рекомендуется
  - разместить на входе в организацию соответствующее объявление
  - показатели тепловизора уничтожать в течение суток (достижение цели сбора)

Сайты

…отсутствует однозначное понимание того, в каких случаях собираемые и обрабатываемые данные будут относиться к персональным, а в каких — нет.

…если совокупность данных необходима и достаточна для идентификации лица, такие данные следует считать ПДн, даже если они ***не включают в себя данные документов, удостоверяющих личность****.*

- Обработка ПДн с использованием счетчиков посещаемости сайтов:
  - IP-адрес компьютера, страна, дата и время посещения, тип браузера, тип операционной системы, модель мобильного устройства, тип мобильного устройства.
- Требуется согласие:
  - в отдельных случаях достаточно «галочки»,
  - в других – обязательна публичная оферта на сайте.

Сайты

Типовые формы (электронных) анкет на сайте должны соответствовать ПП-687:

- Обработка ПДн не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что ПДн содержатся в ИСПДн либо были извлечены из нее.
- Формы на сайте должны содержать цель, сроки обработки, перечень действий, отметку о согласии и т.д.

Отсутствие в Реестре Операторов

Операторов вправе без уведомления осуществлять обработку ПДн в соответствии с трудовым законодательством.

При этом как только работодатель выходит за рамки ТК, он обязан подавать уведомление. Примерами могут служить:

1) оформление полисов ДМС
2) передача ПДн сторонним организациям для осуществления пропускного режима

Позиция РКН:

В подавляющем большинстве случаев у Операторов нет оснований не подавать уведомление в реестр Операторов ПДн.

Актуальность записи в Реестре Операторов

- Не учтены отдельные категории субъектов ПДн:
  - родственники работников (карточка Т-2);
  - посетители сайтов.

- Не учтены отдельные категории ПДн, например, сведения, содержащиеся в свидетельстве о браке, в удостоверении офицера и паспорте моряка.

- Неполные сведения о правовых основаниях обработки ПДн.

Позиция РКН:

Для граждан наличие Компании в Реестре свидетельствует о легитимности обработки ПДн.

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.

General Data Protection Regulation (GDPR)

- General Data Protection Regulation (GDPR) – европейский регламент по защите ПДн.
- Вступает в действие 25 мая 2018.

Действие регламента распространяется на

- Компании, учрежденные в ЕС (например, дочерние структуры).
- Компании, учрежденные в иных государствах, которые:

  а) предлагают товары или услуги субъектам в ЕС (например, онлайн-сервисы, банки, телеком-операторы);

  б) осуществляют мониторинг действий, поведения субъектов, находящихся в ЕС (например, любой интернет-сайт).

Отличия от 152-ФЗ

- Вместо Операторов ПДн – контролеры и обработчики
- Простое и понятное согласие
- Отозвать согласие должно быть также просто, как и получить
- Право субъекта на перенос данных
- Обязанность уведомления регулятора и субъектов ПДн об инцидентах
- Назначение представителя в ЕС
- Обязанность проведения оценки нарушения конфиденциальности (DPIA)

Штрафы за нарушение GDPR

- Утечки ПДн – 100 000 000 $
- Отсутствие правовых оснований для обработки ПДн – 1 000 000 $
- Хранение ПДн по достижению целей обработки и истечении законных сроков обработки – 200 000 $
- Рассылка маркетинговых сообщений без согласия субъекта – 100 000 $

Типичные нарушения

- Нарушения, связанные с сайтами:
  - нет Политики,
  - обработка данных посетителей без согласия,
  - некорректные типовые формы (см. ПП-687).

- Незаконная обработка ПДн:
  - обработка без согласия,
  - согласие не соответствует требованиям,
  - обработка (хранение) по достижению целей.

- Нарушение конфиденциальности:
  - передача третьим лицам.

- Неактуальное уведомление об обработке ПДн.

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)

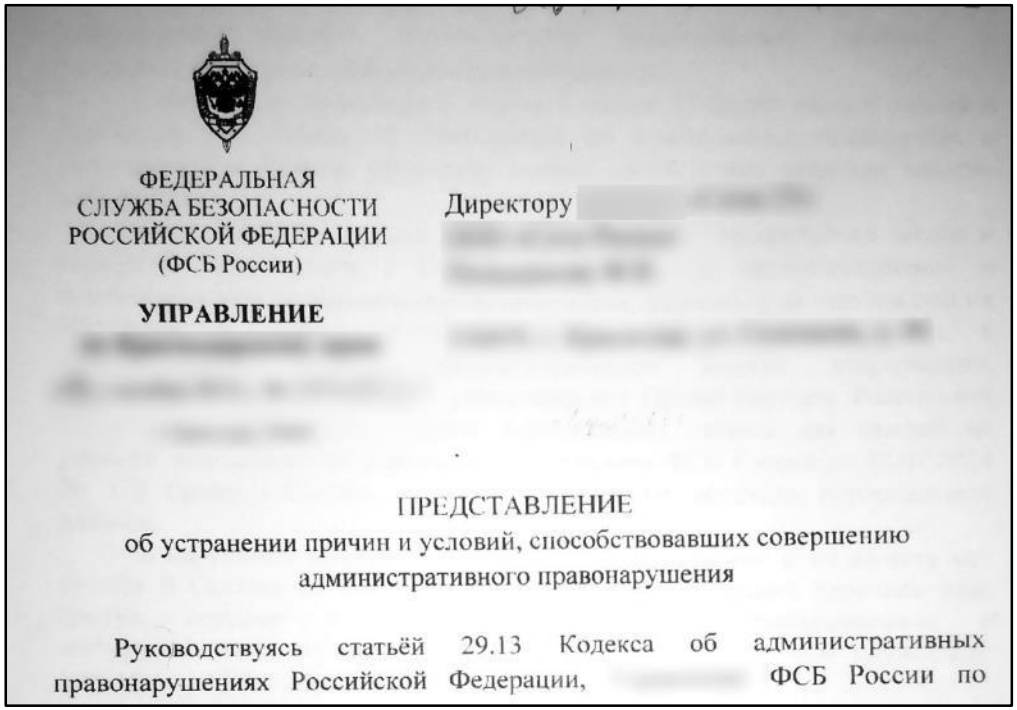
Проверки ФСБ

- Как называется: Обследование помещений, зданий, сооружений, участков местности и транспортных средств.
- Основания:
  - ФЗ «Об оперативно-розыскной деятельности» (144-ФЗ),
  - внутренний план?
- Порядок проведения:
  - приходят без предупреждения,
  - смотрят документы (модель угроз, приказы, инструкции)
  - смотрят оборудование, информационные системы, средства защиты и сертификаты

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)



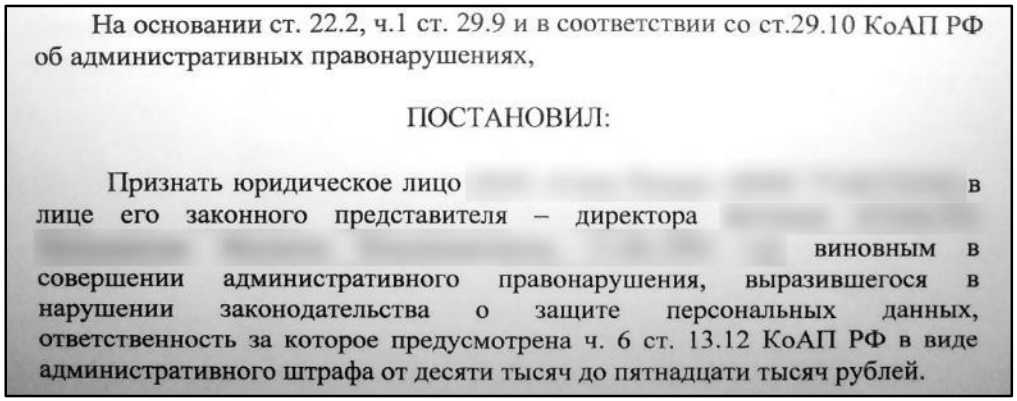
ФЕДЕРАЛЬНАЯ
СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(ФСБ России)

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.

Проверки ЦБ

Центральный Банк является регулятором в отношении

- Кредитных организаций – банков и НКО.
- Некредитных финансовых организаций – страховых, НПФ, МФО, БКИ, участников рынка ценных бумаг, ломбардов и др.

Проверки ЦБ

Запрашивается в рамках проверки процессов обработки и защиты ПДн:

- Аттестат и (или) иной документ, подтверждающий соответствие требованиям по безопасности.
- Приказы о назначении ответственных лиц и утверждении документов.
- Модель угроз, техническое задание и технический проект на создание ИСПДн, сведения о средствах защиты информации
- Сведения об обеспечении защиты информации при ее обработке, хранении и передаче сертифицированными средствами защиты.
- Сведения, документы и справки о выполнении требований по защите (ПП-1119, ФСТЭК-21)

Проверки Прокуратуры

В соответствии с п. 13 Положения обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться так образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

В нарушение данных требований из представленных документов невозможно установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Вышеизложенное свидетельствует о ненадлежащем исполнении работниками требований законодательства о персональных данных, что нарушает права граждан, получающих банковские услуги.

Перечисленные нарушения закона стали возможными в результате ненадлежащего исполнения своих обязанностей должностными лицами и отсутствия должного контроля со стороны руководителя.

Нарушения являются существенными, подлежат устранению в полном объёме и подпадают под признаки дисциплинарного проступка.

На основании изложенного, руководствуясь ст. 24 Федерального закона «О прокуратуре Российской Федерации»,

ТРЕБУЮ:

1. Рассмотреть по существу настоящее представление и принять исчерпывающие меры к устранению и недопущению указанных в нем нарушений закона.
2. Рассмотреть и решить вопрос об ответственности должностных лиц допустивших нарушения требований федерального законодательства.
3. О дате и месте рассмотрения настоящего представления сообщить в прокуратуру.

В течение месяца со дня внесения представления должны быть принять конкретные меры по устранению допущенных нарушений закона, их причин и условий, им способствующих.

4. О результатах принятых должно быть сообщено прокурору в письменной форме.

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