ПРАВОПРИМЕНИТЕЛЬНАЯ ПРАКТИКА В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Романов Илья | CISA, CISM
Заместитель руководителя 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 Doctor Web.
- В настоящее время – системный интегратор в области информационной безопасности.

Направления деятельности

В соответствии с требованиями нормативных документов и стандартов:

- 152-ФЗ,
- СТО БР ИББС,
- PCI DSS,
- 382-П,
- ISO 27001,
- АСУ ТП,
- Коммерческая тайна,
- Сведения ДСП,
- Защита ГИС.

О компании «ДиалогНаука»: ключевые клиенты

Проверки в области ПДн

Проверки в области ПДн

- Сильно поменялся порядок к проведению проверок (вышли из под действия 294-ФЗ).
- Новые аспекты и вопросы, на которые обращает внимание Роскомнадзор.
- Проверки ФСБ по ПДн.
- Блокировка сайтов нарушителей.
- Новые штрафы (с 1 июля).

«ДиалогНаука»

- опыт сопровождения ряда крупных Заказчиков в ходе проверок в области ПДн (в том числе «международных» Компаний);
- отслеживаем результаты проверок и судебных решений;
- участвуем в публичных мероприятиях.

Проверки Роскомнадзора

- Вышли из под действия 294-ФЗ (о защите прав при проверках):
  - продление сроков проверки, задержка с выдачей акта;
  - нет возможности оспорить результат (только через суд).
- Большие запросы (требуют свыше 50 справок и официальных ответов).
- Детально смотрят и «бумажные» документы и информационные системы, особое внимание – сайтам.
- Неохотно идут на обсуждение спорных вопросов.

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.

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.

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.

Общедоступные ПДн

- Обработка общедоступных ПДн:
  - Принцип «Целеполагания» - обработка ПДн должна соответствовать целям сбора ПДн. Например, если данные размещаются с целью поиска одноклассников, то нельзя их использовать для продвижения услуг и взыскания долгов.
  - На обработку ПДн должны быть полномочия. Например ЕГРЮЛ может вести только ФНС и «тиражировать» ЕГРЮЛ незаконно.
- «Big Data» - регулятор планирует усиление контроля: «*Мы хотим получать внятные ответы об использовании ПДн российских граждан*».

Анализ ИСПДн

- Товарные накладные на серверы.
- Изучение информационных потоков (SQL-запросы).
- Поиск ПДн с истекшими сроками хранения.
- Проверка учетных записей (если есть аутсорсинг – должно быть поручение обработки ПДн с согласия субъекта).
- Локализация баз данных– с использованием «whois»: «В судебно-претензионной практике установление ответчиков в основном осуществляется посредством whois-сервисов».

Локализация баз персональных данных

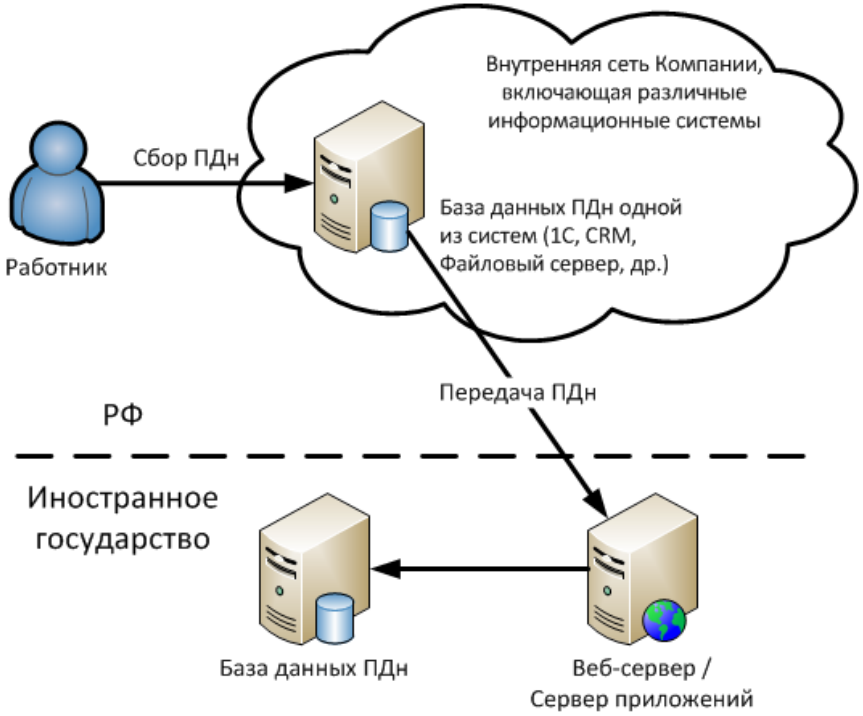
Подход к трактовке требований о локализации баз данных, содержащих ПДн остался без изменений:

- «Первичный» сбор ПДн должен осуществляться с использованием БД на территории РФ.
- После этого – можно передавать в другие страны, с соблюдением требований к трансграничной передаче и передаче третьим лицам

Полезные ссылки:

- http://minsvyaz.ru/ru/personaldata/
- https://pd.rkn.gov.ru/library/p195/

Позиция РКН:
Только доступ к ПДн в режиме просмотра - не является трансграничной передачей.



Актуальность Уведомлений

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

- Не учтены отдельные категории ПДн:
  - подпись и расшифровка подписи,
  - 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.

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.

Последствия проверок РКН

- Блокировка интернет-сайтов
- Предписания (срок исполнения – 3 месяца)
- Штрафы

В подавляющем большинстве случаев Операторам не удается оспорить результаты проверок в суде.

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,
  - смотрят оборудование и информационные системы.

Проверки ФСБ

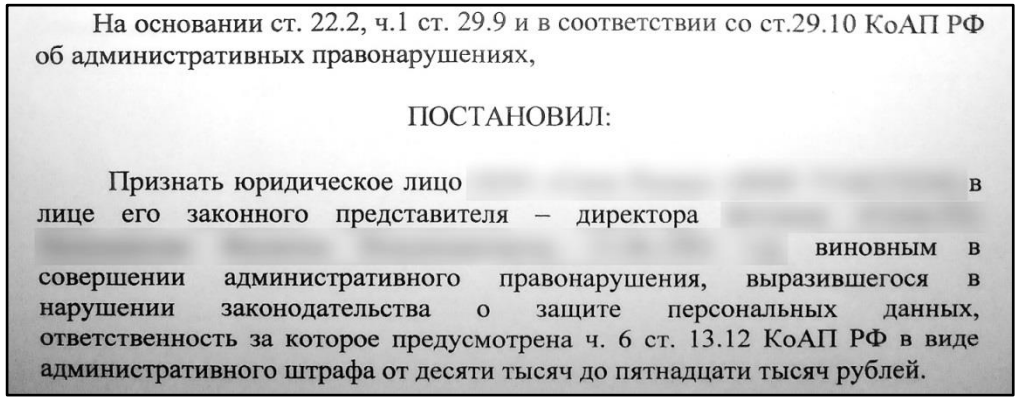
Что проверяет ФСБ:

- назначение ответственных лиц (допуск к ПДн, защита ПДн),
- учет машинных носителей ПДн,
- наличие сертифицированных СЗИ и СКЗИ,
- модель угроз и совокупность предположений о нарушителе,
- определение уровня защищенности и требуемого класса СКЗИ.

Проверки ФСБ

Результаты:

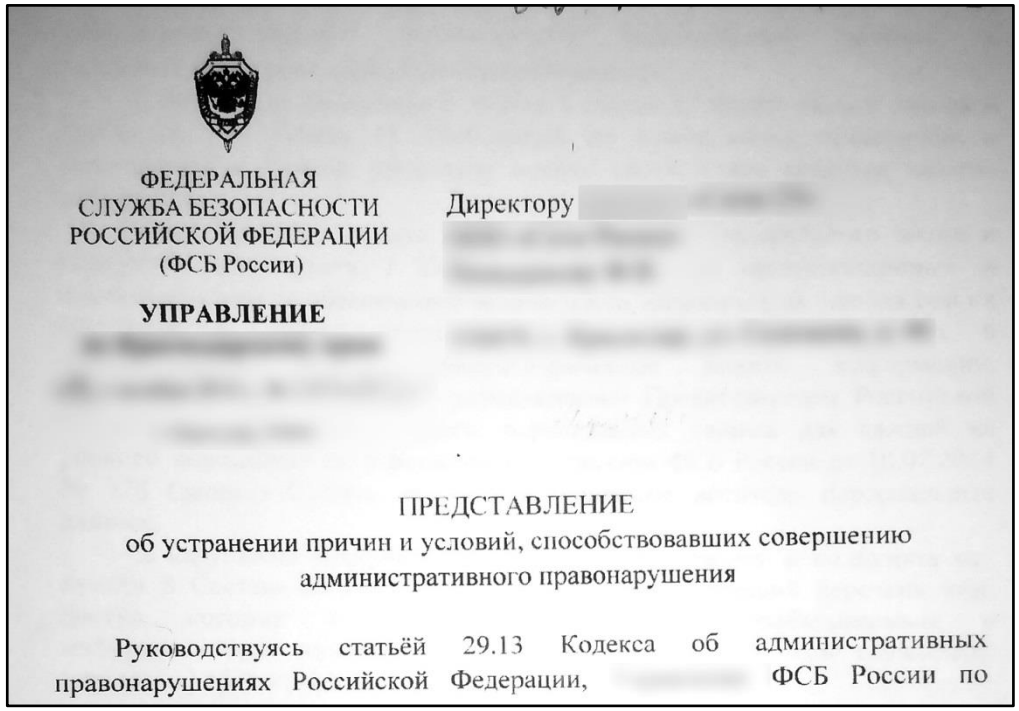
- штрафы (ч. 6, ст. 13.12 КоАП РФ) – от 10 000 рублей
- представления об устранении причин и условий (срок – 1 месяц в соответствии со ст. 29.13 КоАП РФ)



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 [redacted] в лице его законного представителя – директора [redacted] 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.



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ (ФСБ России)

УПРАВЛЕНИЕ [redacted]

Директору [redacted]

ПРЕДСТАВЛЕНИЕ

об устранении причин и условий, способствовавших совершению административного правонарушения

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

Штрафы и санкции в области ПДн

Статья 13.11. Нарушение законодательства РФ в области ПДн

Текущая редакция КоАП	
Нарушение порядка сбора, хранения, использования или распространения ПДн	до 10 000
с 1 июля 2017 года	
Обработка ПДн в случаях, не предусмотренных законодательством, либо обработка ПДн, несовместимая с целями сбора ПДн	до 50 000
Обработка ПДн без согласия в письменной форме, либо невыполнение требований к содержанию согласия в письменной форме	до 75 000
Необеспечение неограниченного доступа к Политике в области ПДн	до 30 000
Непредставление ответа на запрос субъекта ПДн	до 40 000
Невыполнение законных требований субъекта ПДн	до 45 000
Невыполнение требований по защите ПДн, повлекшее нарушение безопасности ПДн	до 50 000
Невыполнение обязанности по обезличиванию	до 6 000 на должностных лиц

Потенциально каждое из нарушений может быть классифицировано отдельно

Штрафы и санкции в области ПДн

- 13.12 КоАП РФ. Нарушение правил защиты информации (пример с ФСБ)
- 19.7 КоАП РФ. Непредставление сведений (например, уведомление в реестр)
- Блокировка Интернет-сайтов
- И другие…

Гарантии и поддержка

Гарантии, поддержка и сопровождение.
Подход АО «ДиалогНаука».

- гарантийные обязательства на результаты работ;
- объекты работ: документация и средства защиты;
- поддержка при проверках и запросах;
- обязательства – 12 месяцев, включаются в договор.

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