

ОБМЕН ПЕРСОНАЛЬНЫМИ ДАННЫМИ В УСЛОВИЯХ ОБЛАКОВ И АУТСОРСИНГА

Илья Романов

Руководитель Отдела консалтинга

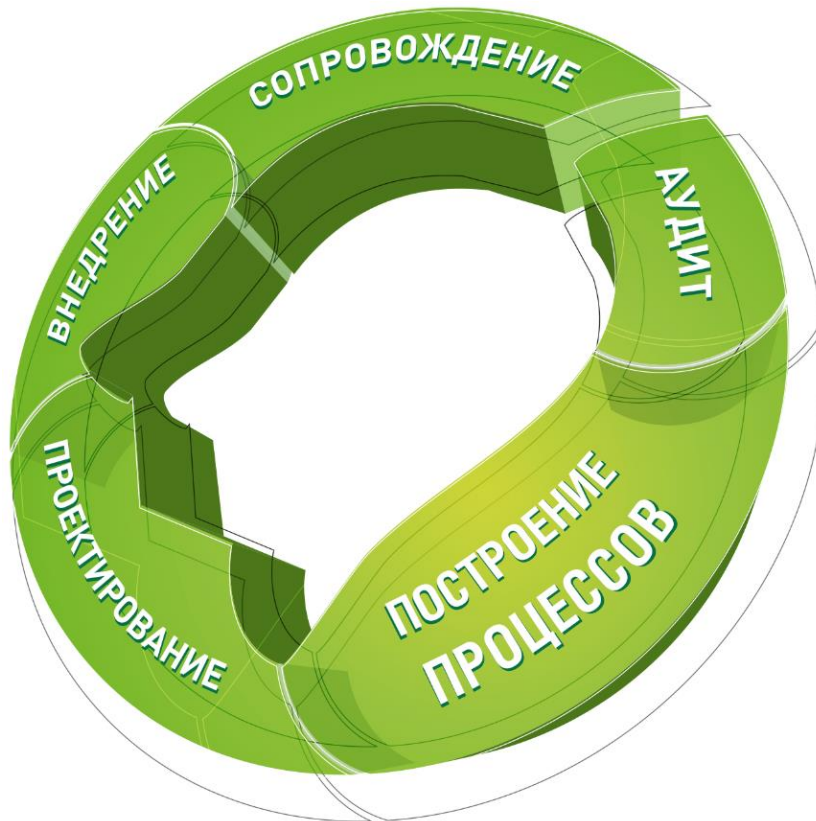
ДуалОгНаука

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)
- ❖ Положения Банка России
- ❖ ГОСТ 57580
- ❖ PCI DSS
- ❖ ISO 27001
- ❖ АСУ ТП
- ❖ Коммерческая тайна
- ❖ Сведения ДСП
- ❖ Защита ГИС





Исходя из опыта реализации проектов и анализа результатов деятельности РКН большое число нарушений возникает при обмене ПДн

- **в рамках получения/оказания ИТ-услуг и аутсорсинга**
- **в рамках взаимодействия внутри групп компаний (в том числе дочерних и головных организаций)**

Услуги, предполагающие передачу ПДн провайдерам:

- ИТ-услуги
- Аутсорсинг процессов

- проектирование, внедрение, сопровождение ПО/железа/систем
- Colocation, Bare Metal
- IaaS, PaaS, SaaS
- разработка (доработка) ПО
- ИИ и машинное обучение

По оценке портала **TADVISER** объем российского рынка ИТ-услуг растет в среднем на 15% в год.

Услуги, предполагающие передачу ПДн провайдерам:

- **ИТ-услуги**
- **Аутсорсинг процессов**

- обеспечение пропускного режима (включая СКУД)
- привлечение клиентов и заключение договоров (агентские схемы)
- подбор и обучение персонала
- кадровый и бухгалтерский учет
- аналитика и визуализация
- маркетинговые исследования

Дочерние и головные компании

Особенности взаимодействия внутри групп компаний:

- Тесный информационный обмен между компаниями
- Использование «общих» процессов (например, кадры, бухгалтерия, юристы, ИТ)
- Преимущественно единая централизованная ИТ-инфраструктура
- Наличие собственных «уникальных» систем в отдельных компаниях
- Работа по совместительству
- Ситуация схожа с использованием услуг провайдеров, но зачастую это неформализовано (отсутствуют договоры)

Риски при передаче ПДн

- Использование услуг, связанных с обработкой ПДн
- Обмен ПДн между «родственными» компаниями



Риски, связанные с утечкой ПДн на стороне получателя



Риски, связанные с невыполнением требований при обмене ПДн

Проблемы, связанные с передачей ПДн

- Получатели ПДн не обеспечивают должной защиты своей инфраструктуры, как следствие:
 - утечки ПДн на стороне получателей
 - атаки из скомпрометированной сторонней инфраструктуры
- Получатели ПДн не обеспечивают комплаенс при обработке и защите ПДн
- Отправители ПДн не получили **согласие субъектов** на передачу ПДн
- Отправители и Получатели ПДн не заключили **поручение обработки** ПДн

Согласия работников на передачу ПДн

- 152-ФЗ:
 - Оператор вправе поручить обработку ПДн с согласия субъекта
 - Согласие 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 нужны **отдельные** письменные согласия под каждую цель

Поручение обработки ПДн

Требования к составу поручения обработки ПДн:

- ✓ перечень ПДн, цели их обработки;
- ✓ требования, предусмотренные ч.5 ст.18 и ст.18.1 ФЗ-152 (обязанности при сборе и обработке ПДн);
- ✓ обязанность по запросу оператора ПДн предоставлять свидетельства принятия мер и соблюдения требований, установленных поручением и Законом о ПДн («право на аудит»);
- ✓ требования к защите ПДн в соответствии со ст.19 ФЗ-152, включая требование уведомления оператора об инцидентах с ПДн*

* фактах неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн

Пример определения зон ответственности

Для обеспечения «реальной» безопасности необходимо определять и фиксировать в поручении/договоре зоны ответственности

IaaS	PaaS	SaaS
Управление пользователями (учетные записи и доступ)	Управление пользователями (учетные записи и доступ)	Управление пользователями (учетные записи и доступ)
Приложения	Приложения	Приложения
Гостевые ОС	Гостевые ОС	Гостевые ОС
Виртуальное сетевое взаимодействие (Overlay)	Виртуальное сетевое взаимодействие (Overlay)	Виртуальное сетевое взаимодействие (Overlay)
Платформа виртуализации	Платформа виртуализации	Платформа виртуализации
Инфраструктурное обеспечение	Инфраструктурное обеспечение	Инфраструктурное обеспечение
Техническое (аппаратное) обеспечение	Техническое (аппаратное) обеспечение	Техническое (аппаратное) обеспечение
Физическое сетевое взаимодействие (Underlay)	Физическое сетевое взаимодействие (Underlay)	Физическое сетевое взаимодействие (Underlay)
Инженерное обеспечение	Инженерное обеспечение	Инженерное обеспечение

Частые проблемы защиты ПДн при обмене с партнерами и провайдерами:

- 1) Как обеспечивается защита канала, и кто за нее отвечает?
- 2) Есть ли необходимая документация (ОРД, Модели угроз и пр.) у всех участников обмена?
- 3) Есть ли лицензии ФСТЭК/ФСБ на оказание услуг по защите?

Проблемы, связанные с «поручением»

Что имеем на практике?

- На сайте провайдера – аттестат ЦОД и обещание защищать ПДн
- В договоре с провайдером – нет ни поручения обработки ПДн, ни обязательств по защите

Заблуждение 1:

- Провайдер не обрабатывает ПДн

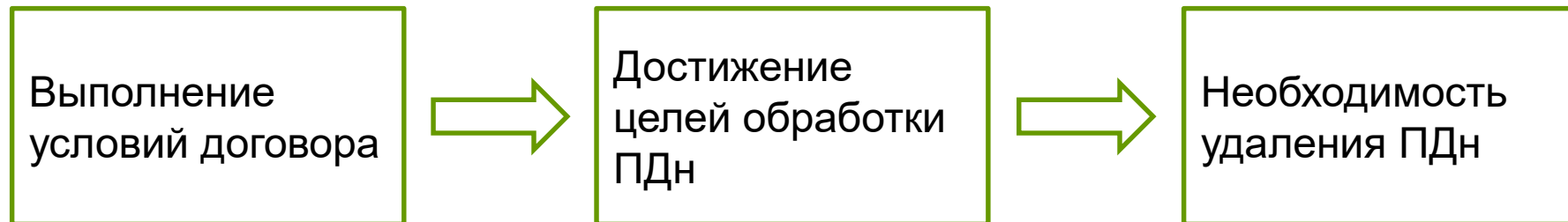
Проблемы, связанные с «поручением»

Заблуждение 2:

- Если провайдер подпишет поручение, то ему придется подавать уведомление РКН и выполнять требования по защите ПДн

Что на самом деле означает отсутствие поручения?

- Нарушение законодательства со стороны и Оператора, и Обработчика
- У Обработчика нет законных оснований для обработки ПДн
- При этом Обработчик все равно осуществляет обработку ПДн и обязан выполнять соответствующие требования в том числе по защите



Приказ Роскомнадзора от 28 октября 2022 г. № 179 «Об утверждении Требований к **подтверждению уничтожения** персональных данных»

Используются ли
средства
автоматизации?

НЕТ

ДА

Акт, включающий в том числе:

- ✓ ФИО субъектов, или **иную информацию, относящуюся к субъекту**;
- ✓ перечень категорий ПДн;
- ✓ наименования носителей с указанием кол-ва листов в каждом
- ✓ причину, способ, дату уничтожения

- Знаем ФИО – указываем ФИО;
- Не знаем ФИО – указываем «иную информацию», которая прямо, или косвенно идентифицирует субъекта ПДн

Используются ли
средства
автоматизации?

НЕТ

ДА

Акт, включающий в том числе:

- ✓ ФИО субъектов, или иную информацию, относящуюся субъекту);
- ✓ перечень категорий ПДн;
- ✓ наименования носителей с указанием кол-ва листов в каждом
- ✓ причину, способ, дату уничтожения

Выгрузка из журнала ИСПДн, включающая:

- ✓ ФИО субъектов, или иную информацию, относящуюся субъекту);
- ✓ перечень категорий ПДн;
- ✓ наименование ИСПДн;
- ✓ причину и дату уничтожения

ч. 3.1, ст. 19 ФЗ-152:

Для уничтожения ПДн должны использоваться прошедшие в установленном порядке процедуру оценки соответствия СрЗИ, в составе которых реализована функция уничтожения информации

- Программные СрЗИ от НСД с функцией удаления информации
- ПО поиска и гарантированного уничтожения информации на дисках
- ОС специального назначения с функцией удаления информации
- Аппаратные средства уничтожения (только для магнитных носителей)

Передача ПДн трансграничным провайдерам

- ✓ Перед началом трансграничной передачи ПДн – нужно подать уведомление о таком намерении.
 - *Исключения – ПП-2526, например для почтовой связи*
- ✓ Если поданные ранее сведения о трансграничной передаче изменились – нужно также подать уведомление.
- ✓ Роскомнадзор, рассмотрев уведомление, может ограничить или запретить трансграничную передачу (ПП-24).
 - *Исключения – ПП-2526, например, использование платежных систем*

Обработчик ПДн	Ответственность перед субъектом ПДн
Российское лицо	✓ Оператор ПДн
Иностранное лицо	✓ Оператор ПДн ✓ Обработчик

Обработчик ПДн несет ответственность перед Оператором ПДн

Возможные изменения штрафов и санкций

Изменения в Кодекс об административных правонарушениях:

- Существенно увеличиваются штрафы на Оператора и его работников за нарушения в области ПДн:
 - обработку ПДн без законных правовых оснований,
 - несвоевременное уведомление РКН об обработке ПДн,
 - несвоевременно уведомление РКН об утечке ПДн.
- Вводятся внушительные штрафы за действия, повлекшие неправомерную передачу ПДн:
 - **на компании – до 500 млн. рублей**
 - **на работников – до 5 млн. рублей**

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

