



Риск-ориентированный подход к выполнению требований законодательства о персональных данных



Алексей Мунтян, *15 лет в Data Privacy*

Основатель и CEO в компании Privacy Advocates

Соучредитель в Russian Privacy Professionals
Association - RPPA.ru

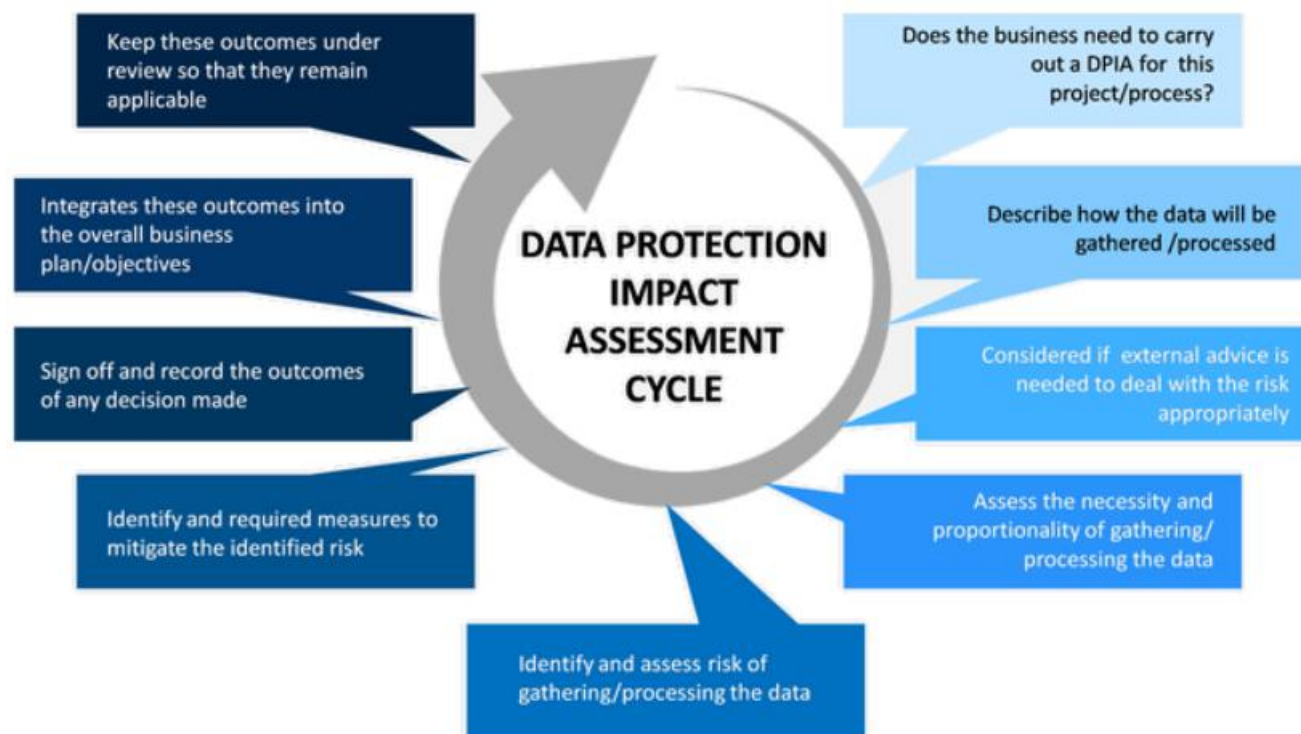
Внешний Data Protection Officer в нескольких
транснациональных холдингах

+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru



- Оценка воздействия на защиту персональных данных (Data Protection Impact Assessment, DPIA) — процедура, предусмотренная ст. 35 Общего регламента защиты персональных данных ЕС (GDPR).
- Она заключается в выявлении и описании всех процессов работы с персональными данными внутри компании.
- DPIA проводится для оценки рисков негативного воздействия на данные, поиска наиболее уязвимых мест в системе защиты, но главное — для выработки действий по недопущению утечек и ошибок.
- **Важным аспектом для принятия решения о необходимости DPIA является качественная оценка рисков в процессах обработки персональных данных.**





С 1 июля 2021г. при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных применяется система оценки и управления рисками. Надзорный орган при осуществлении государственного контроля (надзора) относит поднадзорные объекты к одной из пяти категорий риска причинения вреда (ущерба).

Критерии отнесения объектов федерального государственного контроля (надзора) за обработкой персональных данных к определенной категории риска согласно постановлению Правительства РФ от 29.06.2021 № 1046

Критерии отнесения к группе вероятности	Критерии отнесения к группе тяжести				
	Вероятность	Группа 1	Группа 2	Группа 3	Группа 4
<ul style="list-style-type: none"> РКН в течение последних 2 лет были выданы предписания, требования или предупреждения <i>и (или)</i> вступило в законную силу решение о привлечении к адм. отв. в течение последних 3 лет 	в отношении нарушений, предусмотренных ч.ч. 1.1, 2.1, 5.1, 9 ст.13.11 КоАП РФ	в отношении нарушений, предусмотренных ч.ч. 1, 2, 5, 6, 8 ст.13.11 КоАП РФ	в отношении нарушений, предусмотренных ч.ч. 4, 7 ст.13.11 КоАП РФ	Отсутствие обстоятельств, предусмотренных для 1-3 группы вероятности	
Критерии отнесения к группе тяжести	Вероятность	Группа 1	Группа 2	Группа 3	Группа 4
<ul style="list-style-type: none"> обработка специальной категории ПД и (или) биометрических ПД сбор ПД, в т.ч. в Интернете, с использованием БД за пределами РФ трансграничная передача ПД в государства, не указанные в приказе РКН от 05.08.2022 №128 обезличивание ПД согласно законодательству РФ с последующей передачей третьим лицам 	Группа А	Высокий риск	Значительный риск	Значительный риск	Средний риск
<ul style="list-style-type: none"> обработка ПД в целях, отличных от целей обработки ПД при их сборе обработка ПД несовершеннолетних лиц в случаях, не предусмотренных федеральными законами обработка ПД более чем 20,000 субъектов в ИСПД сбор ПД, в т.ч. в Интернете, с использованием иностранных программ и сервисов 	Группа Б	Высокий риск	Средний риск	Средний риск	Низкий риск
<ul style="list-style-type: none"> обработка ПД близких родственников субъекта ПД трансграничная передача ПД в государства – не стороны Конв. СЕ 108, но указанные в приказе РКН от 05.08.2022 №128 обработка ПД 1,000-20,000 субъектов в ИСПД обезличивание ПД согласно законодательству РФ без последующей передачи третьим лицам 	Группа В	Средний риск	Средний риск	Умеренный риск	Низкий риск
<ul style="list-style-type: none"> трансграничная передача ПД в государства – стороны Конв. СЕ 108 обработка ПД менее чем 1,000 субъектов в ИСПД обработка ПД, не требующая направления уведомления в РКН обработка ПД, полученных из общедоступных источников 	Группа Г	Умеренный риск	Умеренный риск	Низкий риск	Низкий риск

Контроль рисков обработки ПД с учетом риск-толерантности и (или) разумных ожиданий заинтересованных сторон (в первую очередь, субъектов ПД и лиц, осуществляющих обработку ПД)



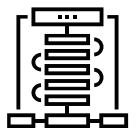
Не навреди

Отказ от снижения риска обработки ПД за счет увеличения иных рисков



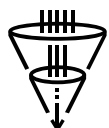
Активное взаимодействие

Вовлечение в оценку и обработку рисков заинтересованных сторон



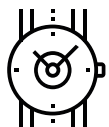
Не существует универсальной методики

Методика риск-менеджмента должна быть специфичной и удобной



Чем проще, тем лучше

Методика и результат риск-менеджмента должны быть понятны и воспроизводимы



Ограниченный срок годности результатов риск-менеджмента

Оценка и обработка рисков зависят от изменения риск-факторов во времени

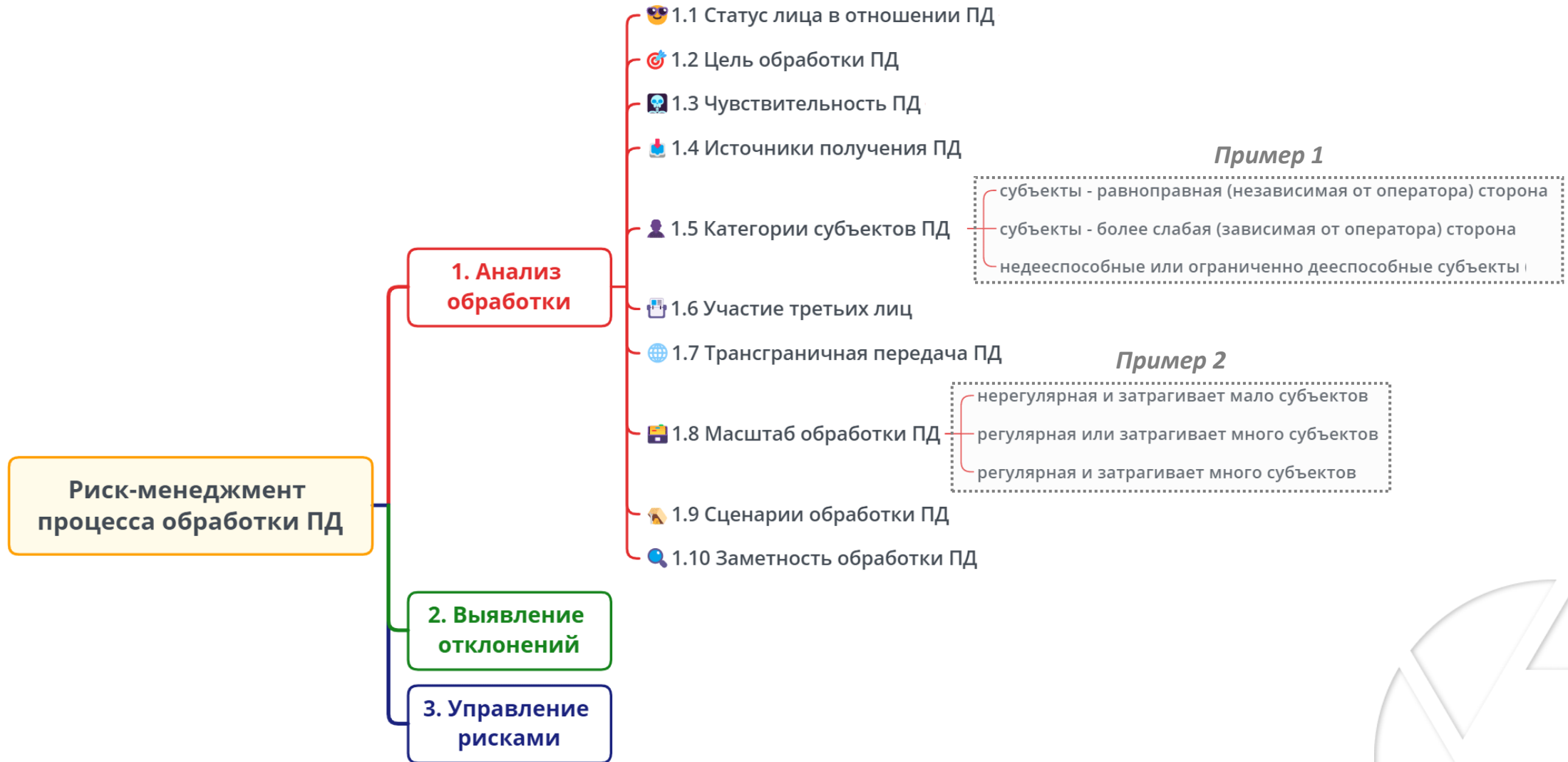


Нет документированной информации – нет риск-менеджмента

Те, кто пренебрегает документами, – воск в руках тех, кто документами не пренебрегает

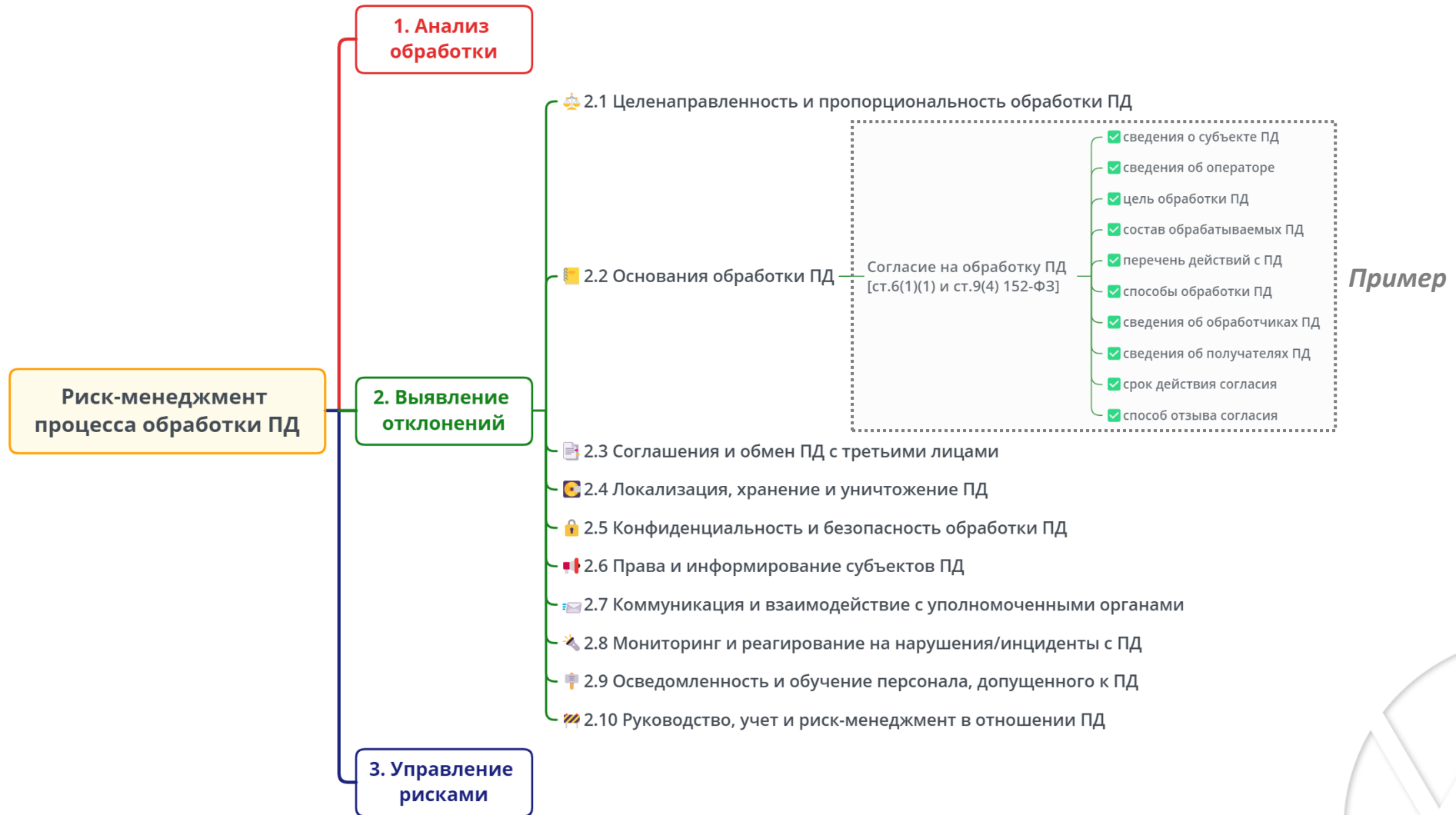






Инсайты (подсказки) — предварительно опишите характеристики процесса обработки ПД
 масштаб анализа м.б. разным (например, процесс маркетинга или маркетинговый сайт)



*Пример*

Инсайты (подсказки)

требования (контроли) см. в ПРКН-253 от 24.12.2021, ППРФ-1046 от 29.06.2021, ППРФ-24 от 16.01.2023 и отраслевые НПА (потребители, реклама, связь, банки, медицина, образование и т.д)

используйте чек-листы и схемы закрытых вопросов для оценки применимости требований и их соблюдения

Риск-менеджмент процесса обработки ПД

1. Анализ
обработки

2. Выявление
отклонений

3. Управление
рисками

3.1 Оценка уровня риска

3.2 Выбор методов реагирования

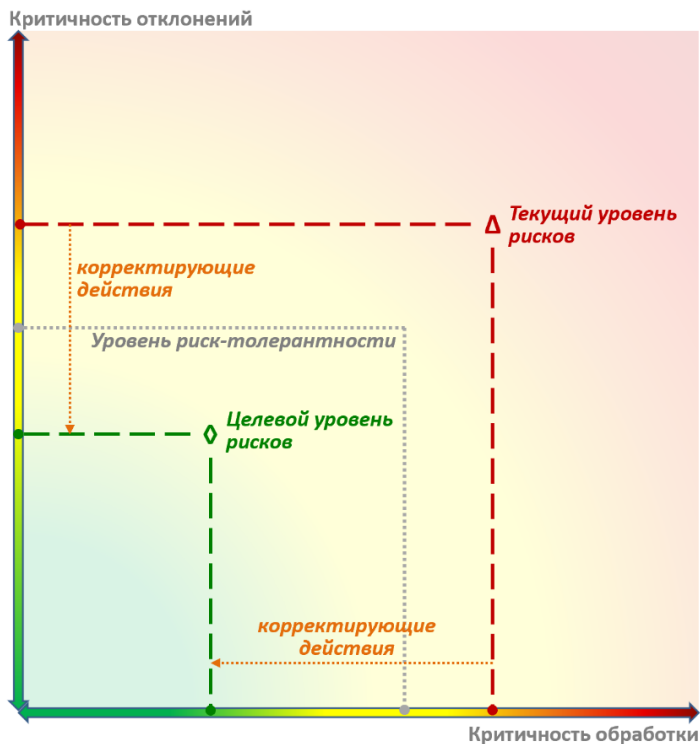
3.3 Определение мер реагирования

3.4 Планирование мер реагирования

Пример

- корректировка отношений с субъектами
- корректировка отношений с третьими лицами
- корректировка внутренней документации
- корректировка процесса обработки ПД
- изменение ИТ-систем/ИТ-инфраструктуры

Пример оценки уровня риска обработки ПД



💡 Инсайты (подсказки)

- риск-толерантность определяется вместе с владельцем процесса обработки ПД / риска
- критичность обработки ПД и отклонений надо регулярно пересматривать
- меры реагирования могут разделяться на краткосрочные и долгосрочные
- возможно принятие в т.ч. остаточных рисков (после обработки первоначальных рисков)

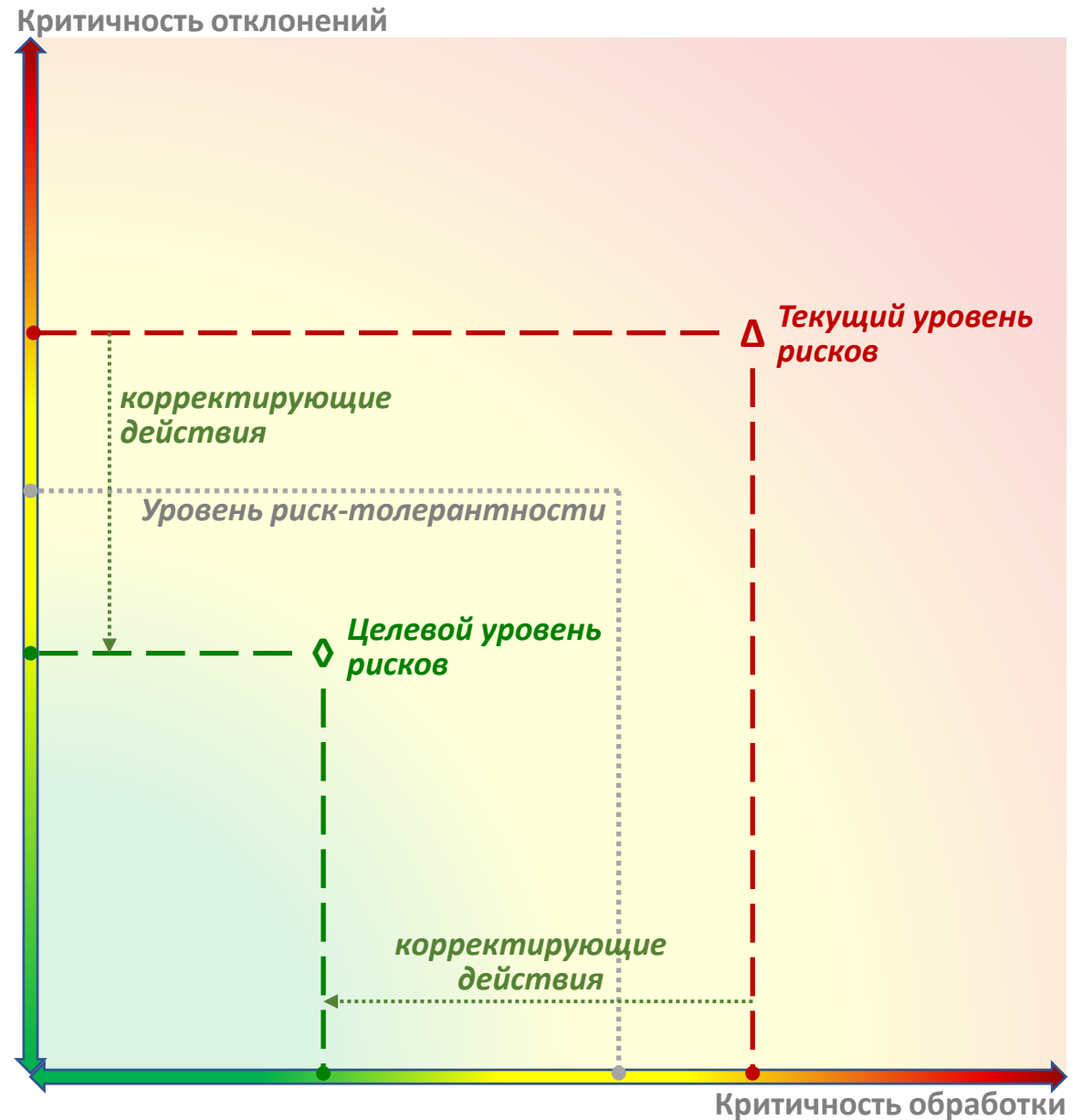
Как эффективно управлять рисками обработки ПД?

Минимизируйте обработку ПД



Вы великолепны!







**Privacy
Advocates**

Всегда рады сотрудничеству!

+7 (903) 762-64-15 | alexey.muntyan@privacy-advocates.ru | t.me/prv_adv



Telegram-канал