Методика оценки рисков приватности, включая персональные данные

написано Александр Астахов | 10 июня, 2023

Отсутствие какой-либо логически объяснимой связи между требованиями по обеспечению безопасности персональных данных и степенью конфиденциальности этих данных – основная причина отторжения, вызываемого в деловой среде действующим законодательством в этой области. Бизнес заставляют тратить деньги непонятно на что. В большинстве случаев ущерб, связанный с нарушением безопасности ПДн не очевиден ни для субъектов ПДн, ни для обработчиков этих данных. Для наведения мостов в этой области, очевидно, необходима согласованная методика, позволяющая определять характер и степень ущерба, наносимого субъектам ПДн, а также оценивать соответствующие риски.

Обратимся к разработанному британским информационным комиссариатом руководству по «оценке ущерба, вызванного нарушением приватности» – ICO PIA Handbook. Privacy impact assessment (PIA). Что такое приватность, на что она влияет и как можно оценивать степень этого влияния?

Приватность (privacy) означает частную жизнь и право личности на неприкосновенность своей частной жизни. Приватность включает в себя 4 составляющих:

1. приватность персональной информации (обеспечение прав граждан в области персональных данных, включая защиту ПДн)
2. приватность самой личности (защита организма человека от нежелательных воздействий на него, начиная с пересадки органов и заканчивая биометрической идентификацией)

3. приватность поведения этой личности (защита личного пространства и приватных мест от несанкционированных наблюдений и вторжений)
4. приватность персональных коммуникаций (тайна переписки и телефонных переговоров)

Британские регуляторы подразделяют риски приватности на две категории:

1. Риски индивидуума, связанные с нарушением его приватности (нарушением прав субъектов ПДн) в результате искажения, повреждения, фальсификации, разглашения и т.п. его персональной информации
2. Риски организации, допускающей нарушение приватности и выражающиеся в выплатах штрафов, компенсаций, утраты репутации и доверия, приостановке деятельности и т.п.

Далее в этих категориях со свойственной англичанам дотошностью рассматриваются все возможные риски приватности и их категории, а также стратегии обработки этих рисков.

Процесс оценки рисков приватности включает в себя следующие основные этапы:

1. Предварительная оценка. Анализ проекта (создаваемой или уже существующей ИСПДн), идентификация всех заинтересованных лиц, первоначальная высокоуровневая оценка рисков приватности с целью определения подхода к последующей оценке приватности (полной или сокращенной)
2. Полномасштабная оценка и обработка рисков приватности, включая детальный анализ риска и интервьюирование всех заинтересованных лиц
3. Упрощенная оценка и обработка рисков приватности, менее формализованная, включающая в себя менее детальный анализ более ограниченного объема информации. В ходе упрощенной оценке обычно фокусируются лишь на наиболее

критичных аспектах проекта.

4. Оценка соответствия требованиям законодательства и нормативной базы в области приватности и персональных данных, начиная с законодательных актов и заканчивая руководящими документами регуляторов, устанавливающих требования к защите персональных данных
5. Последующая плановая переоценка рисков приватности и вытекающие из этой переоценки корректирующие действия

Далее каждый из перечисленных этапов очень подробно расписывается и прилагаются списки проверки для оценки соответствия требованиям, ущербов и рисков приватности.

В заключении рассматриваются четыре вида стратегии организации в области обеспечения приватности: минималистская, всеобъемлющая, расширенная и социально ориентированная.

Если бы сократить этот документ раз в десять и соединить с ISO 27001-совместимой методикой оценки рисков, то получится нормальное руководство по управлению рисками приватности (и рисками ПДН в частности).

Онлайн версия ICO PIA Handbook:
http://www.ico.gov.uk/pia_handbook_html_v2/html/0-advice.html