

Обезличивание персональных данных

Е.Ю. Мищенко, А.Н. Соколов

ФГБОУ ВПО «Южно-Уральский государственный
университет» (НИУ), г. Челябинск

E-mail: eug6303@mail.ru, ANSokolov@inbox.ru

Обезличивание – способ обработки персональных данных (ПД), целью которого является приведение этих данных в защищённое состояние, которое не позволяет злоумышленнику использовать их во вред физическому лицу. В докладе рассматривается терминология процесса обезличивания как способа защиты ПД, особенностью которого является изменение не среды обработки, а самого представления информации.

Ключевые слова: персональные данные, обезличивание, изменение представления информации.

1. Обезличивание как процесс. В статье 3 Федерального закона «О персональных данных» (далее – Закон [1]) приведено определение: «Обезличивание ПД – действия, в результате которых невозможно без использования дополнительной информации определить принадлежность ПД конкретному субъекту ПД».

Закон определяет следующие стороны процесса обработки ПД (см. рис. 1):

- 1) Сам субъект – физическое лицо (Человек);
- 2) Персональные данные этого субъекта (ПД);
- 3) Оператор (уполномоченный) – обрабатывает ПД;
- 4) Контролер – следит за выполнением Закона.

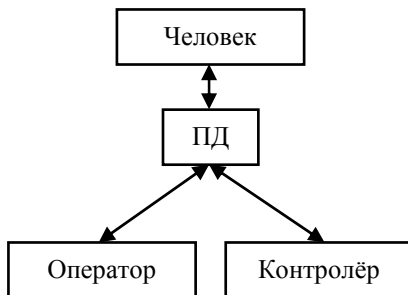


Рис. 1. Связи сторон процесса обработки ПД

Определение обезличивания можно перефразировать: это такие действия Оператора с ПД конкретного Человека, в результате которых Контролер не сможет без помощи Оператора доказать, что полученная информация является ПД того конкретного Человека. Различные стороны процесса обезличивания связаны друг с другом.

2. Связь Человек – ПД. Закон [1] определяет, что ПД – это любая информация, относящаяся к Человеку «прямо или косвенно определённомu или определяемому». «Прямо» – значит Человек сам подтверждает принадлежность своих ПД, «косвенно» – любым другим способом. Связь устанавливается от Человека к ПД – значит «определённому», от ПД к Человеку – «определяемому».

Видим две формы связи Человека и его ПД: ПД «принадлежат» Человеку и «относятся» к нему. «Отношение» отражает причинно-следственную связь (Человек – причина существования своих ПД). «Принадлежность» отражает право собственности (Человек – владелец своих ПД). Если информация «относится» к Человеку, то это ПД, и они этому Человеку «принадлежат».

Человек непрерывно порождает ПД независимо от его воли в необрабатываемом виде. Очень малую долю ПД удастся зафиксировать на каком-либо носителе (фотография, звукозапись, читаемый текст). Закон регулирует обработку ПД именно на носителях.

Но даже ПД на носителях редко сопровождаются подтверждением принадлежности. Без подтверждения ПД ни к кому не относятся и не являются ПД. Подтверждение бывает только на бумажном носителе, а ПД хранятся в электронном виде. Поэтому на практике используются косвенные методы подтверждения.

3. Связь Оператор – ПД. ПД должны относиться к единственному Человеку, процесс проверки этого отношения называется идентификацией. Идентификация – это процесс сравнения двух различных наборов информации с целью удостовериться в их тождестве. Есть три варианта результатов сравнения:

- 1) положительный (все сравниваемые реквизиты совпадают) – данные являются ПД этого Человека;
- 2) отрицательный (не все сравниваемые реквизиты совпадают) – прочие данные не являются ПД этого Человека.

После обработки информации результат сравнения может измениться. При обезличивании мы увидим, что есть некий набор информации, идентифицирующий Человека. Если в результате обработки объем уже не идентифицирует Человека, то имеет место обезличивание ПД. Отсюда следует, что

- 1) имеющийся объем информации о Человеке только тогда является ПД этого Человека, когда данный объем однозначно определяет его (идентифицирует);
- 2) после любой обработки, кроме обезличивания, набор ПД должен идентифицировать Человека;
- 3) если имеющийся объем информации не определяет прямо или косвенно конкретного Человека, то этот объем информации не является ПД этого Человека.

Но по набору информации нельзя понять точно – получился ли он в результате обезличивания или нет. В определении обезличивания заложено еще одно требование – обратимость, иначе это будет уничтожение ПД.

4. Связь Контролер – ПД. При оценке обезличивания Контролер может столкнуться со следующей ситуацией:

- 1) можно идентифицировать Человека без дополнительной информации – это обычные ПД;
- 2) идентифицировать Человека можно при наличии дополнительной информации – либо ПД были обезличены, либо набор был неполным;
- 3) даже при наличии дополнительной информации Человека идентифицировать нельзя – либо ПД были уничтожены, либо этот набор информации не был ПД.

Первый случай кажется простым, но сравнивать информацию не с чем. Поэтому Человек идентифицируется по принципу уникальности (набор информации не может однозначно соответствовать различным людям).

Второй случай сложнее, так как термин «дополнительная информация» неочевиден, по сути.

Третий случай – самый сложный. Оценивать обезличивание будет не Оператор, а либо Контролер, либо Злоумышленник. Возможно, их средства были недостаточными, а возможно, ПД принципиально не восстанавливаются.

5. Идентификация. Процессы обезличивания и идентификации не могут быть описаны исключительно на качественном уровне. Поэтому необходимо ввести количественные характеристики обезличивания, такие как «вероятность идентификации» и «степень обезличивания».

Нормативного определения термина «идентификация» не существует. Идентификация решает две различные задачи – частную (принадлежат ли данные реквизиты заранее определенному Человеку – уточнение) и общую (какому именно Человеку принадлежат данные реквизиты – поиск).

Общая задача идентификации решается либо многократным повторением частного решения (перебор небольшого количества вариантов), либо поэтапным сужением области поиска с последующим перебором.

Идентификацию можно рассмотреть с нескольких сторон:

1. Физическое лицо (Человек), которого надо идентифицировать (во избежание путаницы не будем применять термины «объект» и «субъект»).
2. Набор информации, в рамках которого надо идентифицировать Человека (в случае успешной идентификации – это его ПД).
3. Инициатор процесса, выступающий в роли движущей силы идентификации (им может быть кто угодно, например, Контролер или Злоумышленник).
4. Метод идентификации – любой алгоритм идентификации, применяемый исполнителем, независимо от достигнутого результата.

К сожалению, отсутствие на сегодняшний день нормативно-технической документации по вопросам обезличивания и идентификации не позволяет обсуждать их в рамках принятой терминологии. Если ввести количественную характеристику «Вероятность идентификации» как величину, обратную количеству физических лиц, для которых имеющийся набор информации (ПД) является истиной, то можно вычислить минимальную вероятность идентификации конкретного Человека.

Библиографический список

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных» (в редакции 2011 года) [электронный ресурс]. URL: <http://www.garant.ru>

Depersonalization of personal information

E.Yu. Mishchenko, A.N. Sokolov

South Ural State University, Chelyabinsk
eug6303@mail.ru, ANSokolov@inbox.ru

Depersonalization is a way of processing of the personal information (PI) which purpose is a reduction of these data in the protected state which doesn't allow the malefactor to use them to the detriment of the natural person. Terminology of process of a depersonalization as way of protection of PI is considered which feature is change of the submission of information not the processing environment.

Keywords: personal information, depersonalization, change of submission of information.

References

1. *Federal'nyi zakon Rossiyskoi Federatsii ot 227 iyulya 2006 g. № 152 "O personal'nykh dannykh" (v redaktsii 2011 g.)* [The Federal law of the Russian Federation of July 27, 2006 No. 152 "About Personal Information" (in edition of 2011)]. Available at: <http://www.garant.ru>.