



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(ФСБ России)

ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ
И СПЕЦИАЛЬНОЙ СВЯЗИ
(8 Центр)

9 февраля 2018 г. № 149/7/2/6-184

Москва

В Центре Ваше обращение об отнесении технологии хеширования к обезличиванию персональных данных рассмотрено.

Функции хеширования, определяемые национальным стандартом ГОСТ Р 34.11-2012, относятся к криптографическим методам защиты информации, и используются для обеспечения контроля целостности данных, аутентификации, при формировании и проверке электронной цифровой подписи.

Указанные функции хеширования являются криптографически стойкими и удовлетворяют следующим свойствам:

- 1) по данному значению функции сложно вычислить исходные данные, отображаемые в это значение (задача нахождения прообраза);
- 2) для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в то же значение функции (задача нахождения второго прообраза);
- 3) сложно вычислить какую-либо пару исходных данных, отображаемых в одно и то же значение (задача поиска коллизий).

При этом, как Вам было уже разъяснено Минкомсвязью России, как федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере обработки персональных данных (№ П11-26924-ОГ от 28.12.17), хеширование не входит в число методов обезличивания персональных данных.

Кроме того, отмечаем, что в целом объем персональных данных ограничен и при их хешировании возникают дополнительные требования к строгому

соблюдению определенного, структурированного формата текстовой информации исходных данных. Данные условия сокращают множество входных значений и, как следствие, область значений функции хеширования, что в совокупности приводит к возможности возникновения угрозы подбора нарушителем персональных данных для конкретного субъекта методом перебора.

Таким образом применение хеширования для обезличивания персональных данных является нелегитимным.

Заместитель руководителя
службы ФСБ России –
начальник Центра



А.М. Ивашко