УДК 004.05

ПОДХОДЫ К ОЦЕНКЕ КАЧЕСТВА РАБОТЫ МЕТОДОВ ОБЕЗЛИЧИВАНИЯ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Покасова А.И. (Университет ИТМО**)**

Научный руководитель – кандидат технических наук, доцент Коржук В.М.(Университет ИТМО)

Введение. Активное развитие технологий, направленных на работу с большими объёмами данных, затронуло и области, связанные с обработкой персональных данных различных модальностей: как текста, так и, например, изображений и голоса. Существует множество алгоритмов, выполняющих анонимизацию и обезличивание персональных данных, однако методы оценки данных алгоритмов, описанные в статьях, чаще всего берутся по аналогии для методов идентификации или же полностью отсутствует адекватная мотивация выбора конкретного метода оценки.

Основная часть. В зависимости от вида действий, входящих в процесс обезличивания персональных данных, можно выделить обратимое и необратимое обезличивание.

Необратимое обезличивание также называется анонимизацией, так как в данном случае все чувствительные данные “источника” либо удаляются, либо видоизменяются таким образом, что задача обратной персонификации определенного человека становится невозможной. По завершении процесса анонимизации идентификатор человека заменяется соответствующим анонимным идентификатором [1].

Отдельно выделяется процесс псевдонимизации данных [1], при котором, как и при анонимизации, атрибуты, относящиеся к чувствительной информации изменяются или удаляются из записи, однако обезличенные данные помечаются специальным “псевдонимом” владельца, выделенным ему на основе набора определенных правил. Наличие такого “псевдонима” позволяет при необходимости провести процедуру восстановления личности человека по записи.

Обратимое обезличивание подразумевает наличие детерминированного алгоритма, позволяющего провести процедуру однозначного установления личности, являющейся владельцем персональных данных.

В работе рассмотрены методы оценки качества работы алгоритмов обезличивания и анонимизации биометрических персональных данных. Особый акцент сделан на подходах, позволяющих выполнить повторную идентификацию видоизмененной биометрии, а также подходах, использующих концепцию «интерпретируемого искусственного интеллекта» («explainable artificial intelligence») [2]. Последняя технология привлекает всё большее внимание в связи с тем, что позволяет построить надежные иинтерпретируемые модели прогноза работы методов машинного обучения, используя в своей основе принципы кооперативной теории игр.

Для исследования вышеописанных подходов подбирался датасет, отвечающий показателям конфиденциальности и удобства использования [3]. В итоге был использован набор данных с отпечатками пальцев, содержащих как черно-белые исходные изображения, так и экземпляры, к которым были применены алгоритмы обезличивания биометрии.

Выводы. Были рассмотрены методы оценки качества работы алгоритмов обезличивания биометрических персональных данных, проведено исследование методов с использованием набора обезличенных данных, определены достоинства и недостатки рассмотренных подходов.

Список использованных источников:

1. Жаринов Р. Ф., Трифонова Ю. В. Возможности обезличивания персональных данных в системах, использующих реляционные базы данных. // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – Вып. № 2 (32). – С. 188–194.
2. Lee, J.; Jeong, J.; Jung, S.; Moon, J.; Rho, S. Verification of De-Identification Techniques for Personal Information Using Tree-Based Methods with Shapley Values. J. Pers. Med. 2022, 12, 190. https://doi.org/10.3390/jpm12020190
3. Shin, S.-Y. Privacy Protection and Data Utilization. Healthc. Inform. Res. 2021, 27, 1–2.