РОСКОМСВОБОДА
На защите цифровых прав!
веб-сайт: roskomsvoboda.org e-mail: roskomsvoboda@rublacklist.net тел.: +7-903-003-89-52

Председателю Комитета Государственной Думы
по информационной политике,
информационным технологиям и связи
Хинштейну Александру Евсеевичу

ОТЗЫВ
на проект федерального закона № 946734-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»

Общий комментарий

Биометрические идентификаторы с каждым годом становятся все более популярными как в государственном, так и в частном секторе в качестве средства идентификации граждан и предоставления альтернативной возможности для аутентификации пользователей. Как правило, биометрические идентификаторы включают отпечатки пальцев, подписи, а также узоры сетчатки и радужной оболочки. Могут также использоваться такие идентификаторы как образцы вен, геометрия лица или даже образцы голоса.

Следует отметить, что биометрические данные уязвимы к взломам точно также, как и другие методы аутентификации, но в отличие от паролей, биометрические индикаторы нельзя просто сбросить по мере необходимости. Это создает более высокие риски для безопасности граждан, поскольку становится все труднее исправить утечки или взлом биометрических данных, а следовательно, и восстановить неприкосновенность биометрических систем.

Сбор и использование биометрических данных сопряжены со значительными рисками для граждан. Учитывая потенциал для использования этих данных мы не рекомендуем разрешать удаленный сбор биометрии в локальных системах, с дальнейшим размещением этих данных в единой биометрической системе. Учитывая конфиденциальность биометрической информации и факт того, что возможность восстановления неприкосновенности ограничена, когда информация скомпрометирована, следует избегать централизации, принимая во внимание, что централизованная база данных больше уязвима, поскольку создает единую точку отказа.

В законопроекте также не предусмотрено механизмов контроля пользователей над доступом к данным со стороны третьих лиц. Использование биометрических данных третьими лицами должно обеспечиваться доступом пользователей к инструментам подотчетности, например, посредством обязывания оператора сбора данных вести логирование всех действий по

доступу к данным и их использованию, а так обеспечивать пользователю журнал доступа, который связан с аккаунтом пользователя. Журнал доступа должен содержать следующую информацию: кто получил доступ к данным, когда, где и с какой целью.

Кроме того, в законопроекте отсутствуют каких-либо правовые механизмы для жалоб и возмещения ущерба. Гражданин должен иметь соответствующие механизмы получения компенсации по жалобам, связанным со злоупотреблением или неправильным использованием его личных данные, а также за утечку данных. С этой целью, представляется правильным обязать всех операторов данных вести подробные журналы, когда сотрудники получают доступ к сохраненным данным, а также документировать и сохранять записи, детализирующие цель такого доступа.

Общий вывод:

В связи с тем что биометрические данные представляют из себя особо чувствительные данные, а их неправомерное использование может привести к почти не устранимым последствиям, в том числе к взломам, утечкам и случаям мошенничества с данными, мы полагаем, что спешка в принятии указанного законопроекта недопустима до проведения всех необходимых исследований, а также тщательного консультирования с экспертами по правам человека и цифровой безопасности в ходе открытого, прозрачного и инклюзивного общественного обсуждения.

Руководитель общественной организации «РосКомСвобода»,
член экспертного совета Комитета Государственной Думы
по информационной политике, информационным
технологиям и связи

Козлюк Артём Валерьевич

9 августа 2020 г.