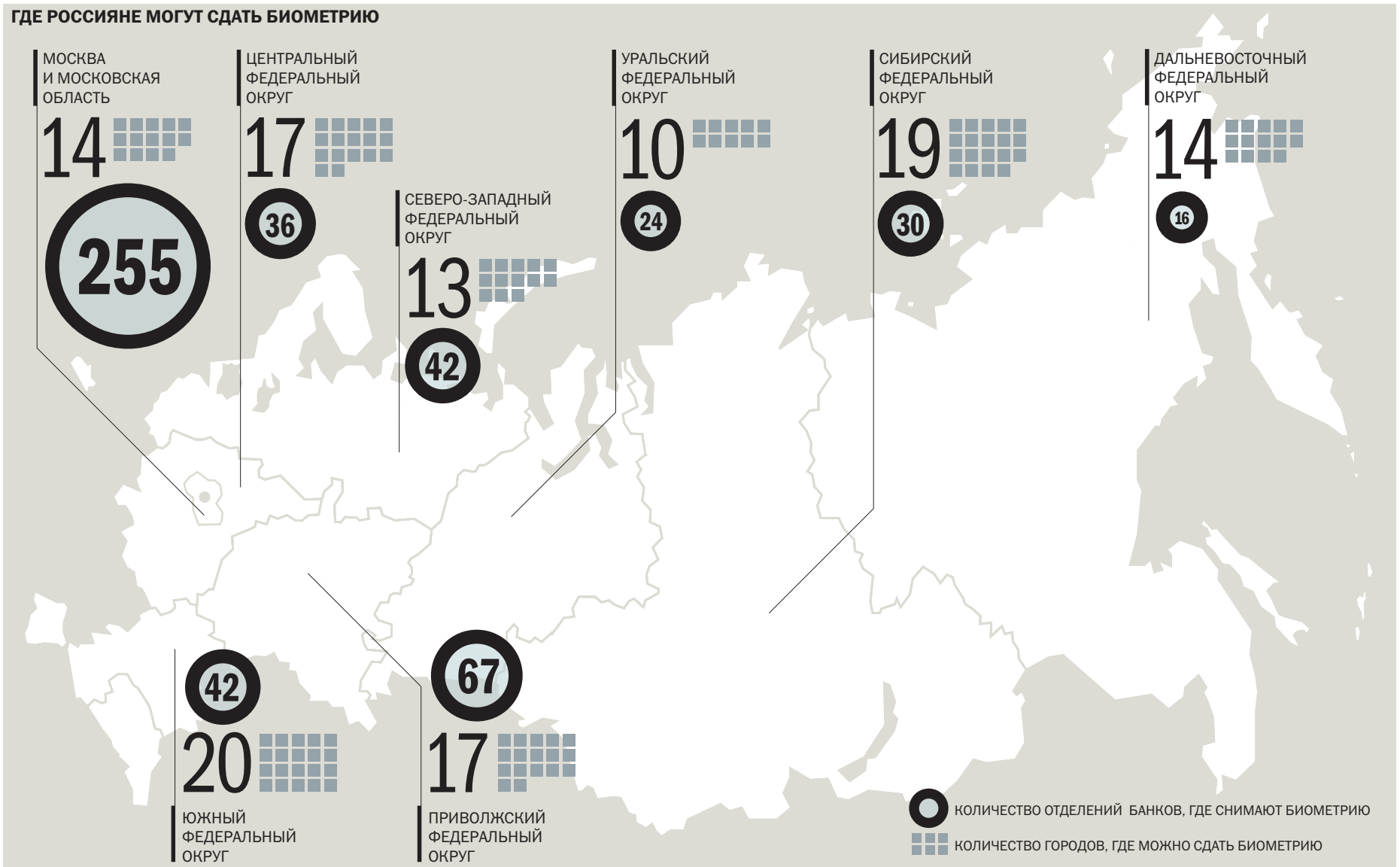

клиента месте. Как отмечают в банке, чаще всего граждане предпочитают сдавать биометрию в офисе или дома. С 2019 года дистанционный сбор биометрии планирует запустить и Росбанк.

Биометрию не проведешь

Биометрическая идентификация достаточна точна. Например, по словам заместителя директора по операционной деятельности Росбанка Марии Фроловой, при личном обращении в офис близнец может запросто ввести в заблуждение операциониста и получить кредит по паспорту брата. Однако с биометрией этот фокус уже не пройдет. «Голоса у близнецов различаются, а значит, система сразу определит подлог — точность распознавания системы 10–7, и это значит, что она может допустить неточность только в одном случае на 10 млн»,— отметила Мария Фролова.

Сегодня пройти удаленную идентификацию можно практически с любого мобильного устройства или веб-камеры

Впрочем, не стоит искушать судьбу и сдавать биометрию в своем нетипичном состоянии. Как пояснили «Деньгам» в ВТБ, наличие бороды у мужчин или косметики у женщин не повлияют на процесс аутентификации клиента, а вот темные очки могут стать причиной отказа в биометрической идентификации. По словам директора по управлению рисками Почта-банка Святослава Емельянова, лучше не использовать толстые оправы, цветные или другие линзы, изменяющие форму и размер глаз, крупные элементы прически, закрывающие часть лица. «Главное — быть просто собой и не волноваться,— отметил он.— В дальнейшем при прохождении идентификации лучше снять или надеть очки в зависимости от того, как вы сдавали биометрию, а в остальном — макияж, загар или изменение прически или цвета волос не повлияют на результат».

По словам Марии Фроловой, на процесс идентификации могут повлиять серьезные изменения голоса (например, сильная охриплость) или внешности — к примеру, пластическая операция.

Бывают исключения

По словам экспертов, в ряде случаев сдача биометрии может быть затруднена. Конкретного перечня заболеваний, при которых съем биометрии затруднен или невозможен, не определен. Однако эксперты отметили, что препятствием может быть сильное заикание, ДЦП, нарушение зрения и т. д. Как сообщил собеседник «Денег» в крупном банке, у них был случай, когда у одного клиента пытались снять биометрию около 40 минут, но так ничего и не вышло.

На сегодняшний день альтернативного способа съема биометрии для

БИОМЕТРИЯ БЕЗ РИСКА

АНДРЕЙ ШУРЫГИН,
руководитель дирекции биометрических технологий Почта-банка

Самое уязвимое в процессе сдачи биометрии — человеческий фактор. Именно поэтому к собирающим биометрию у граждан предъявляются жесткие требования. Этот сотрудник банка должен иметь подтвержденную запись на госуслугах. Кроме того, он имеет право снимать биометрию лишь в конкретном офисе банка. При каждом входе в систему сотрудник подтверждает свою личность не только через логин и пароль, но и (в нашем банке) путем сдачи фото биометрии. Таким образом, риск, что биометрию снимет неустановленное лицо, полностью исключен. И до того как допустить сотрудника к сбору биометрии, его обязательно проверяет служба безопасности банка на предмет благонадежности и отсутствия криминального прошлого. Для обеспечения безопасности канала передачи данных между местом сбора и центральным офисом банка собранные данные идут в зашифрованном виде. Для шифрования используются отечественные средства криптозащиты. В центральном офисе банка установлено оборудование под названием HSM, которое по еще более защищенному алгоритму шифрует собранные данные для передачи в ЕБС. Уровень защиты данных там как у сведений, составляющих гостайну. Зашифрованные сведения в ЕБС отправляются также по строго защищенному каналу. Можно чисто теоретически говорить о злоумышленниках, которые могут попытаться «подложить» свою биометрию вместо снятой у граждан и отправить ее в ЕБС. Однако для этого им нужно будет как-то проникнуть во внутреннюю сеть банка, а отделения обычно не имеют выхода во внешнюю сеть, то есть на практике это фактически невозможно. В самой единой ЕБС биометрический шаблон будет храниться отдельно от персональных данных человека — ФИО, паспортных данных, СНИЛС и других, включенных в базы ЕСИА. И потому если вдруг в результате атаки хакеров, утечки данных или по иным причинам биометрические образы попадут в руки злоумышленников, то использовать их в противоправных целях не удастся.