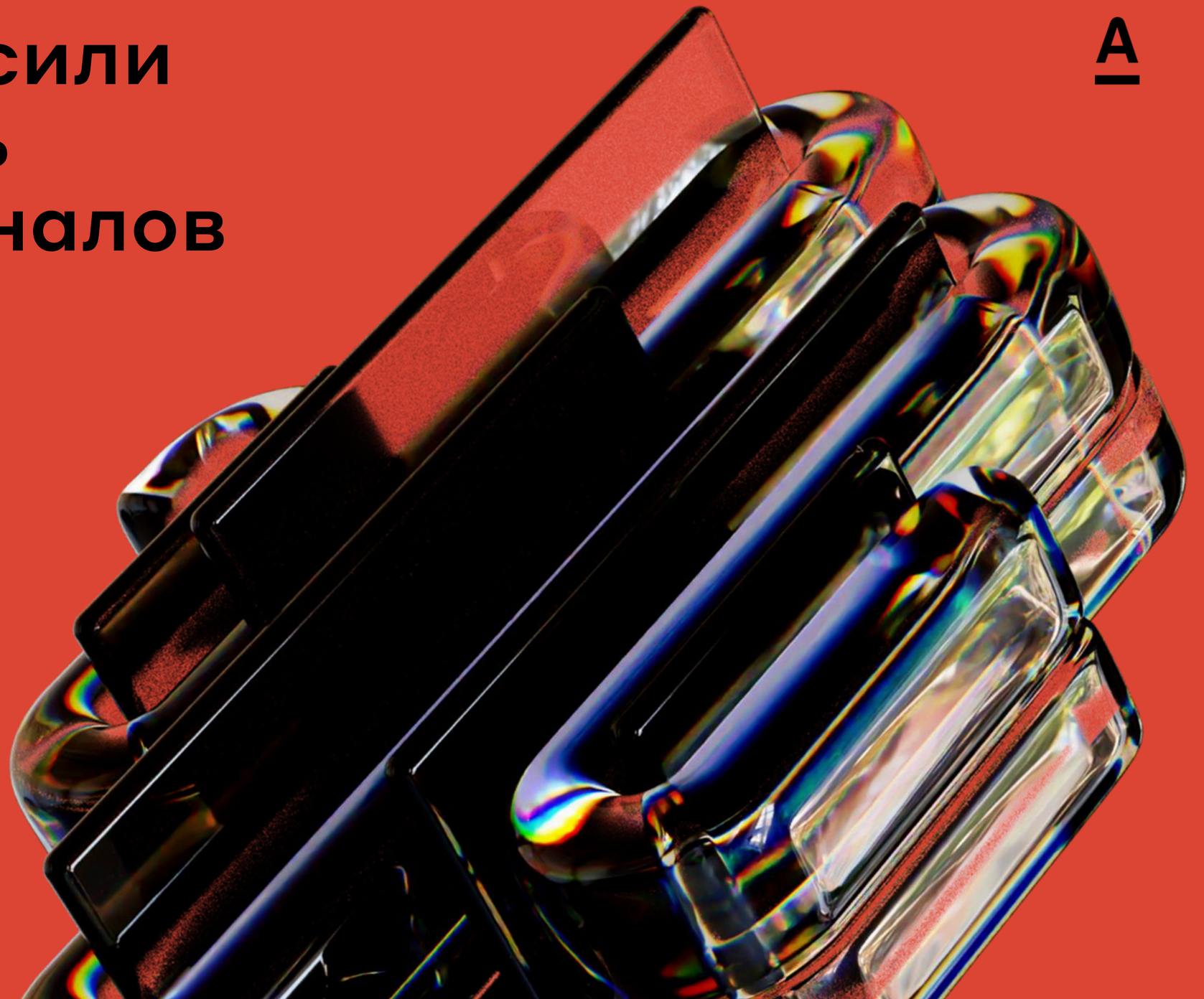
Как мы повысили безопасность цифровых каналов для бизнеса



ADC

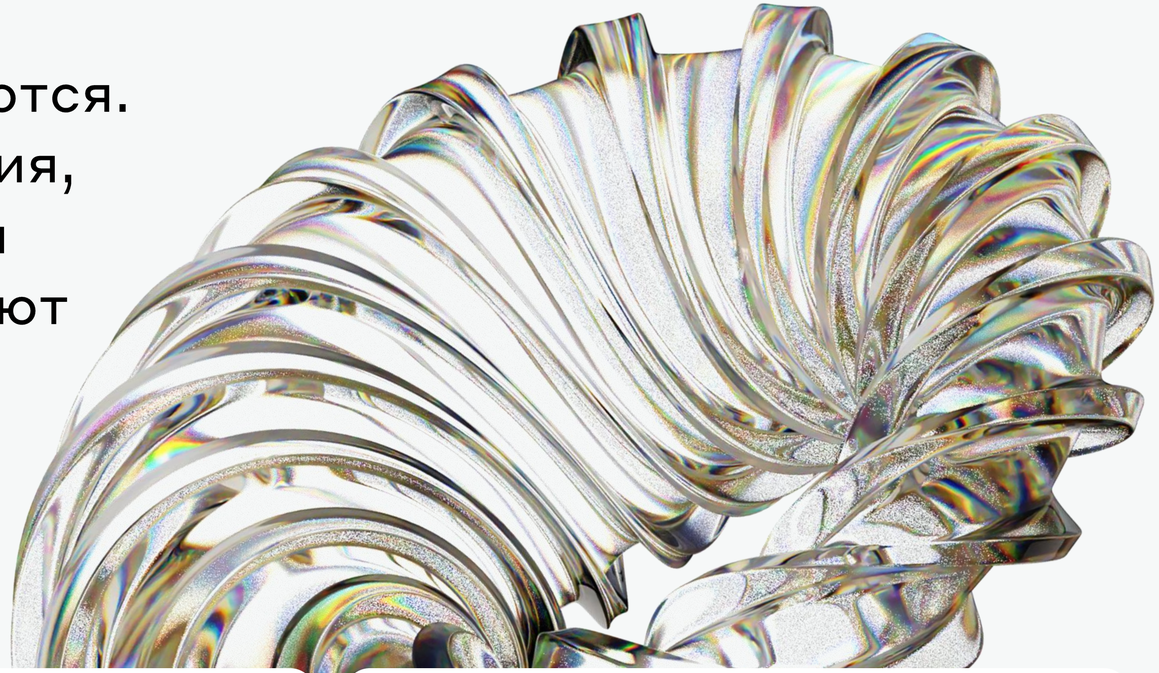
Бизнес хочет больше контроля за процессом управления финансами

безопасность важна не только на этапе входа в интернет-банк или приложение для бизнеса, но и в дальнейшей деятельности. Клиентам недостаточно установить пароль или пин-код: они хотят контролировать всё — когда, откуда и с каким уровнем доступа авторизуются сотрудники, какие действия они совершают.

Банки помогают бизнесу решить проблему лишь частично

мы уже привыкли, что можем держать личные данные под контролем:
в каждом браузере, почтовом сервисе или мессенджере можно самостоятельно управлять подключёнными устройствами, просматривать историю действий.

Банки активно развивают такие возможности для физических лиц. Но для корпоративных клиентов подобные сервисы только появляются. В интернет-банках для бизнеса есть решения, которые закрывают отдельные потребности клиентов в безопасности, но не обеспечивают полной защиты.



1

Клиент может отслеживать локации подключений, но не может удалённо завершать сеансы

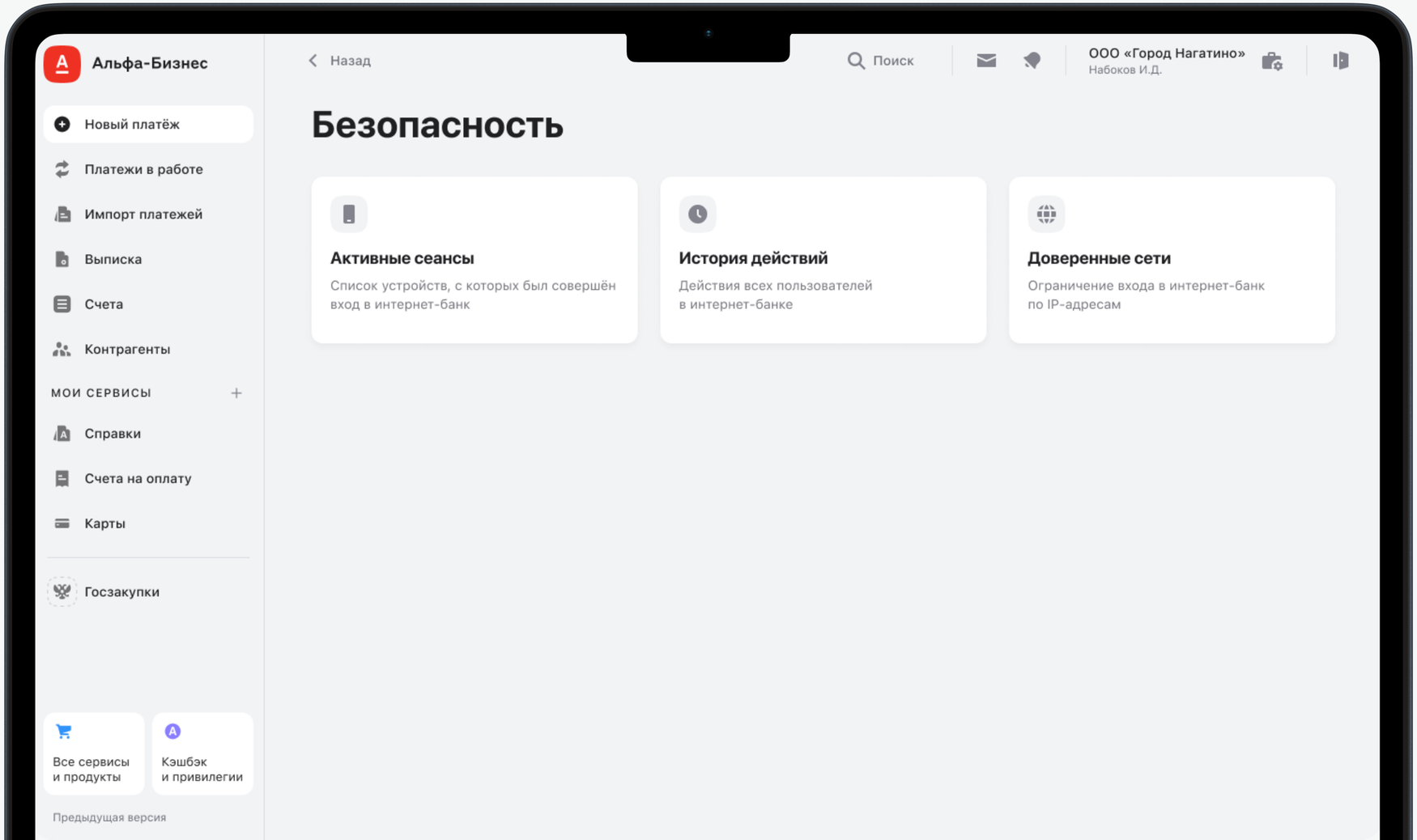
2

Клиент видит подключённые устройства, но не видит, какой сотрудник на нём авторизован

3

В активных сеансах отображаются только мобильные устройства без десктопа

Как мы повысили безопасность

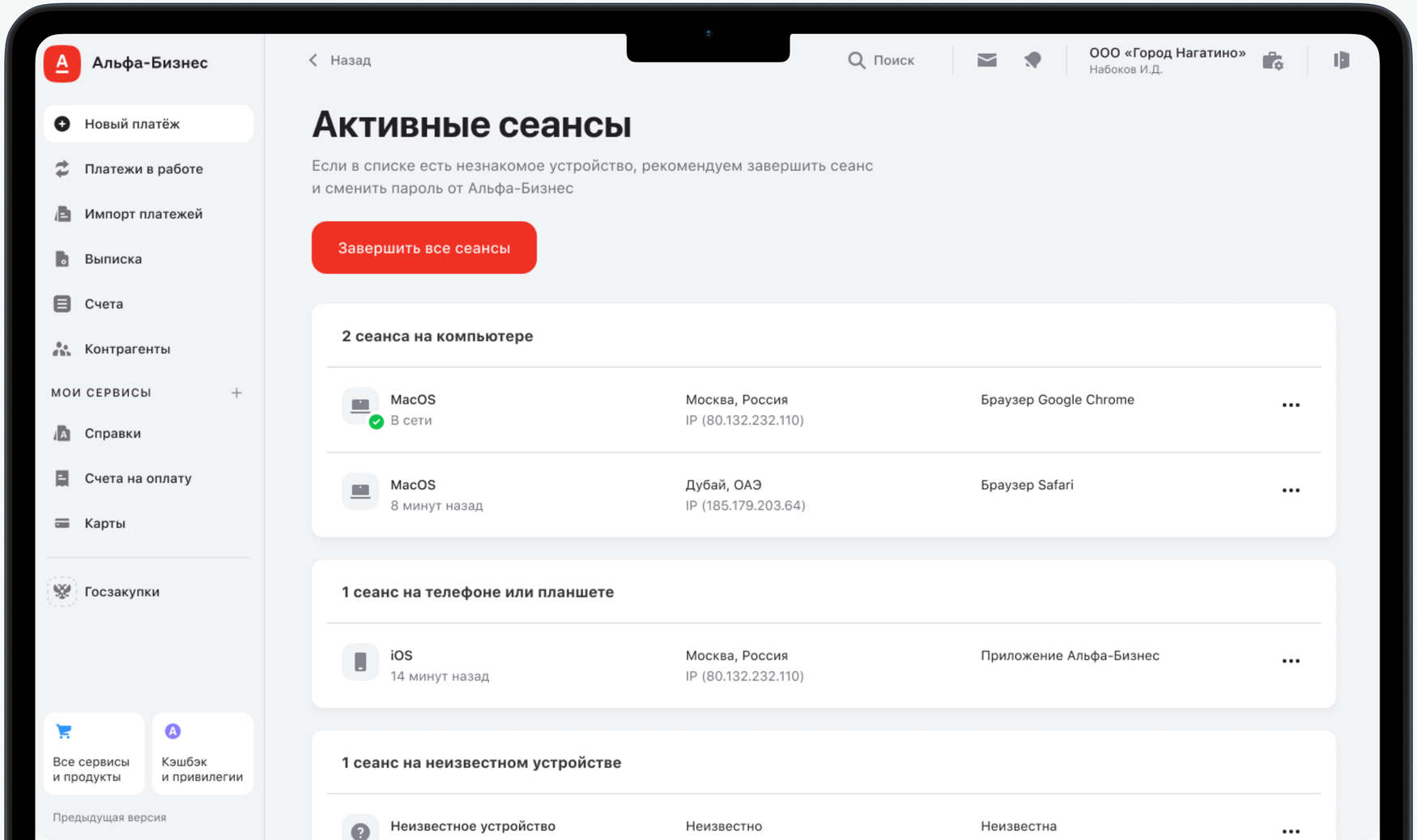


Теперь в одном месте есть всё, чтобы минимизировать возможные угрозы.

Клиент может:

- отслеживать активные сеансы в системе и завершать их в любой момент
- устанавливать ограниченный список IP-адресов, с которых возможен доступ в интернет-банк
- контролировать любые операции в разделе История действий: кто, где и когда сменил или установил пароль, номер телефона, роль сотрудника
- отключать или блокировать пользователей, если какие-то действия покажутся подозрительными

Как мы повысили безопасность



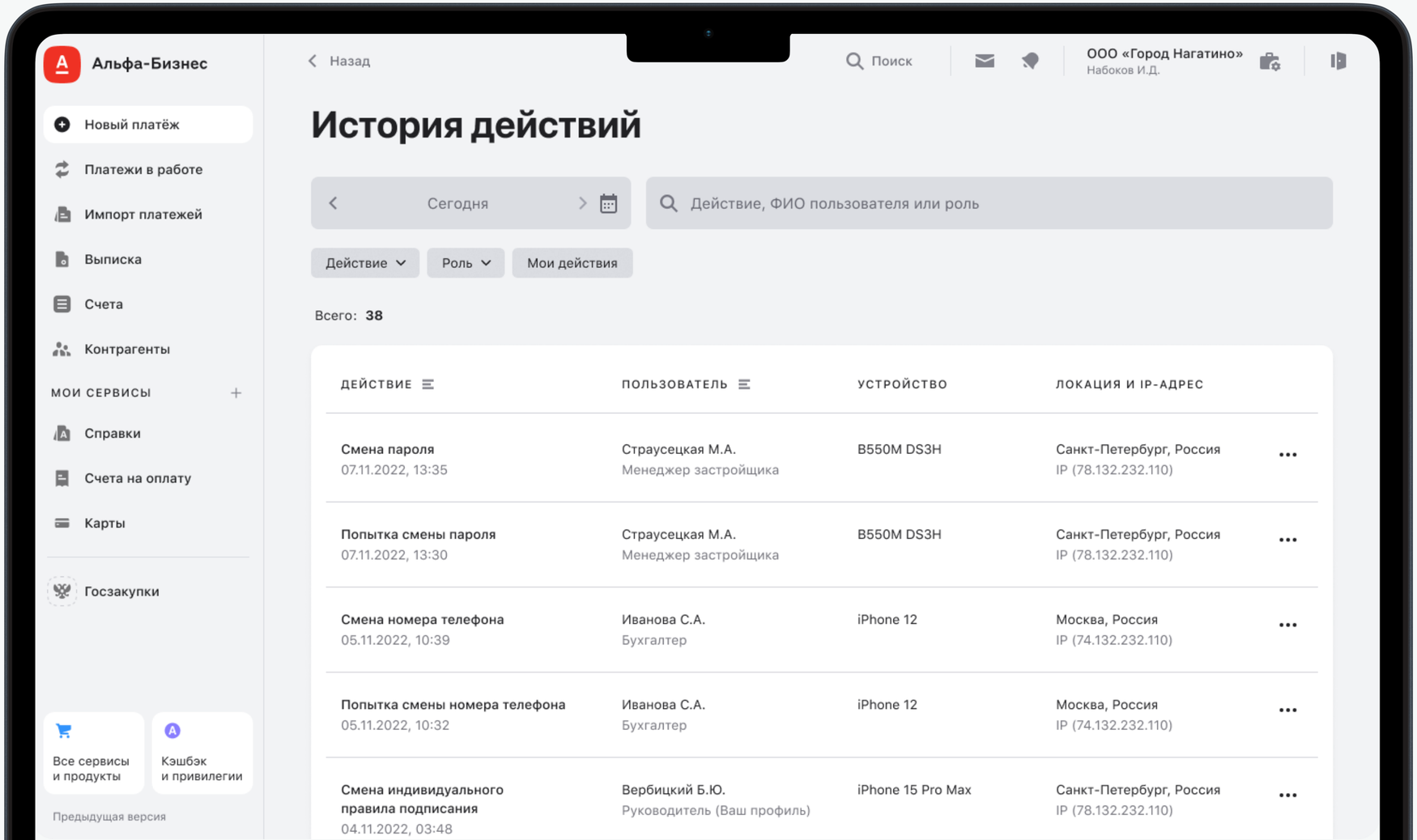
проблема

«Зашел в интернет-банк с чужого устройства и забыл разлогиниться — нужно было срочно подписать платёжку, а телефон разрядился. Что мне теперь делать?»

наше решение

В разделе Активные сеансы клиент видит, с каких устройств и в какое время пользователи входили в интернет-банк, и может завершить любой сеанс.

Как мы повысили безопасность



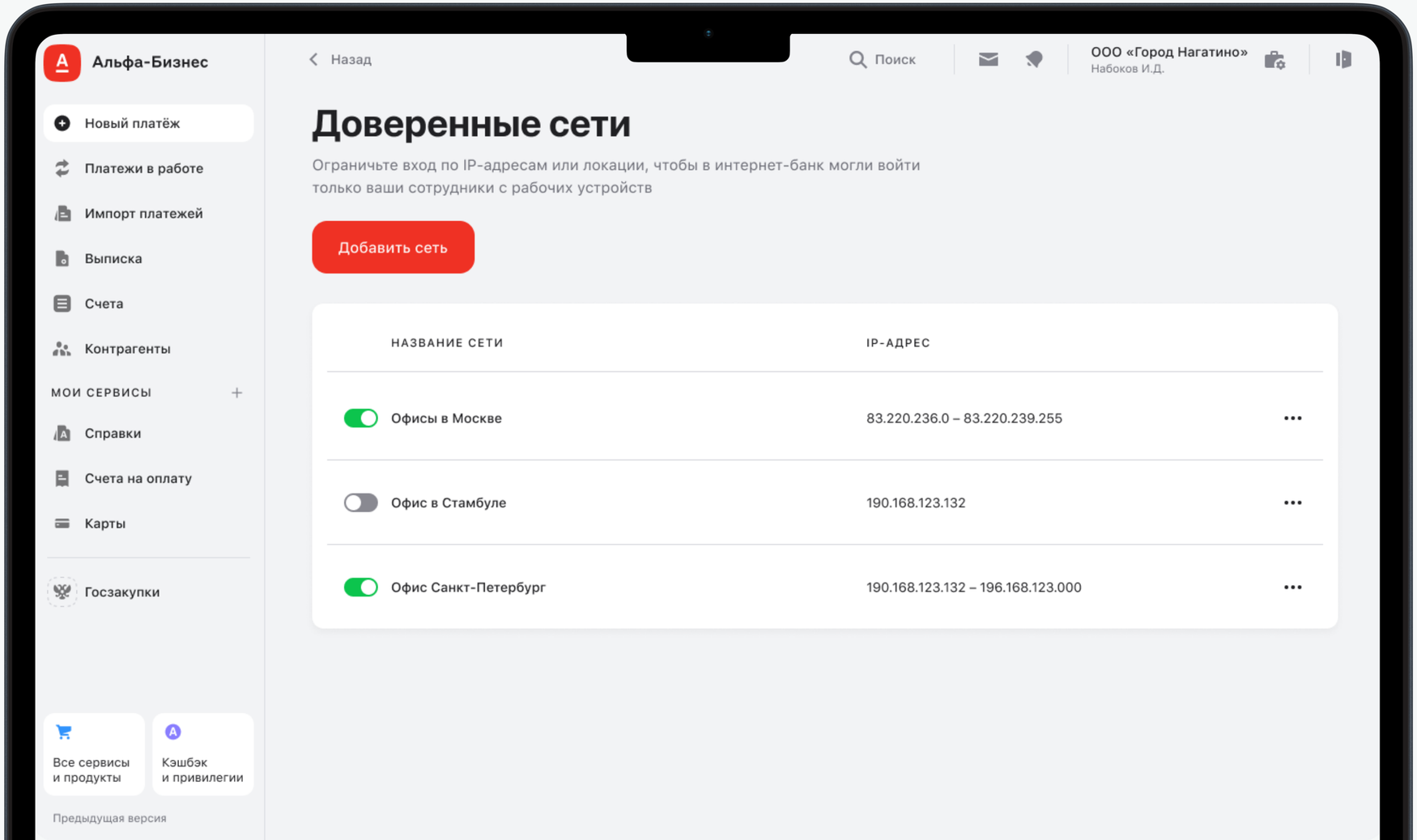
проблема

«Мой новый сотрудник работает удалённо — я хочу знать, как часто он заходит в интернет-банк и может ли совершить действия, угрожающие безопасности финансов компании?»

наше решение

В разделе История действий вы видите все операции, которые совершали вы и ваши сотрудники: смена пароля или роли сотрудника, добавление нового уполномоченного лица и другие.
Если заметили подозрительные действия, пользователя можно отключить или заблокировать.

Как мы повысили безопасность



проблема

«У меня крупная логистическая компания. Мне важно, чтобы вход в интернет-банк мои сотрудники совершали только из офиса — внутри корпоративной сети, так как есть риски утечки данных, особенно если они в отпуске в другой стране подключаются по чужой сети, например через wi-fi отеля»

наше решение

В разделе Доверенные сети вы можете самостоятельно настроить сеть и включить в неё ограниченный список IP-адресов. Тогда вход будет возможен только в определенной локации, например, в головном офисе и филиалах компании. Это особенно важно для клиентов крупного бизнеса.

Спасибо