

Согласовано 09.06.2020 г.

Рекомендательные стандарты по проведению идентификации клиентов-физических лиц кредитными организациями с использованием видеосвязи

Настоящие стандарты к проведению идентификации с использованием видеосвязи согласованы членами Ассоциации участников рынка электронных денег и денежных переводов. Принявшие их организации взяли на себя обязательство придерживаться этих требований, с учетом следующего:

- данные требования являются технологически нейтральными, то есть не предусматривают использование конкретной технологии, программного обеспечения или услуг конкретного вендора;
- кредитные организации вправе устанавливать более строгие требования к процедурам идентификации клиентов с использованием видеосвязи;
- кредитные организации определяют порядок идентификации клиентов на основе собственного риск-профиля, масштаба бизнеса, типов продуктов и услуг;
- кредитные организации при осуществлении деятельности, установления деловых отношений и обновления данных руководствуются требованиями действующих нормативно-правовых актов.
- кредитные организации несут ответственность за проведение идентификации клиентов-физических лиц вне зависимости от используемого программного обеспечения или технических процедур.

1. Юридические основания для проведения идентификации клиентов-физических лиц с использованием видеосвязи

Федеральный закон № 115-ФЗ¹ устанавливает обязанность кредитных организаций до приема на обслуживание идентифицировать клиента, представителя клиента и (или) выгодоприобретателя, а также устанавливать в отношении физических лиц ряд сведений.

При этом запрет на установление деловых отношений без личного присутствия (за исключением ряда изъятий) распространяется только на открытие банковских счетов.

Положение Банка России № 499-П² не устанавливает конкретных процедур сбора и проверки сведений и документов о клиенте-физическом лице, а также содержит открытый перечень источников информации, которые при этом могут использоваться.

При этом согласно Положению № 375-П³ порядок идентификации клиента, в том числе сбора необходимых сведений и документов, разрабатывается каждой кредитной организацией,

¹ Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

² Положение Банка России от 15 октября 2015 г. № 499-П «Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

³ Положение Банка России от 02.03.2012 № 375-П «О требованиях к правилам внутреннего контроля

самостоятельно с учетом особенностей вида и масштаба ее деятельности, организационной структуры, характера продуктов (услуг), предоставляемых кредитной организацией, клиентам, и включается в правила внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Таким образом, использование технологий видеосвязи в целях идентификации осуществляется без нарушения требований нормативно-правовых актов с учетом предъявляемых ими требований.

2. Требования к оценке рисков

Согласно требованиям Глобальных стандартов по противодействию отмыванию денег и финансированию терроризма (Рекомендация 15), финансовые организации обязаны определять и оценивать риски отмывания денег или финансирования терроризма, которые могут возникнуть в связи с использованием новых или развивающихся технологий как для новых, так и для уже существующих продуктов. При этом анализ рисков и определение методов их снижения должны осуществляться до начала использования новой технологии.

Положение № 375-П обязывает кредитные организации разрабатывать программу идентификации клиента, представителя клиента, выгодоприобретателя, бенефициарного владельца, а также программу управления риском легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

В связи с этим, кредитные организации, до момента начала использования средств видеосвязи для проведения идентификации клиентов-физических лиц обязуются проанализировать сопряженные с этим риски, документировать их в программах идентификации клиента и управления риском, с учетом особенностей вида и масштаба ее деятельности, организационной структуры, характера продуктов (услуг).

3. Требования к процедуре идентификации клиента с использованием видеосвязи

– Перед началом процедуры идентификации с использованием видеосвязи кредитная организация:

- получает согласие клиента на обработку персональных данных;
- информирует клиента о правилах прохождения идентификации с использованием видеосвязи;
- предупреждает клиента об ответственности за предоставление заведомо ложных сведений.

– Кредитная организация осуществляет сбор данных, предусмотренных нормативно-правовыми актами, любым способом (например, в мобильном приложении, на сайте, путем сканирования документа, удостоверяющего личность, со слов клиента);

– Кредитная организация осуществляет проверку достоверности полученных данных путем их сверки с информацией из открытых информационных систем органов государственной власти

кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Рекомендательные стандарты к проведению идентификации клиентов-физических лиц кредитными организациями с использованием видеосвязи

Российской Федерации, размещенных в информационно-телекоммуникационной сети «Интернет» либо Единой системе межведомственного электронного взаимодействия, а также иных источников, доступных ей на законных основаниях;

– Кредитные организации осуществляют проверку данных по перечню физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, принимают меры по выявлению категорий клиентов повышенного риска (например, иностранных должностных лиц) согласно действующим требованиям нормативно-правовых актов;

– Кредитная организация подтверждает канал связи, который в дальнейшем будет использоваться для связи с клиентом (например, путем отправки одноразового кода (пароля) в SMS-сообщении, пуш-уведомления в приложении и пр.);

– Кредитная организация проверяет принадлежность предоставленного клиентом документа, удостоверяющего личность, клиенту путем сверки изображения клиента и фотографии на документе;

– Кредитная организация фиксирует изображение, одновременно включающее лицо клиента и документ, удостоверяющий личность (страницу с фотографией).

– Сверка изображения и фотографии может осуществляться с использованием специального программного обеспечения или в ходе интервью с клиентом с участием сотрудника кредитной организации (либо с сочетанием обоих способов).

– В случае использования специального программного обеспечения (ПО) кредитные организации обеспечивают соблюдение следующих условий:

○ ПО не предусматривает возможность использования заранее записанного видеоизображения;

○ ПО предусматривает защиту от подмены видеоизображения ('liveness detection');

○ ПО осуществляет контроль качества изображения (в том числе, освещенность, наличие объектов, скрывающих лицо и т.д.).

– В случае если проводится интервью с клиентом с участием сотрудника кредитной организации:

○ сотрудник кредитной организации должен пройти обучение или инструктаж;

○ сотрудник кредитной организации обязан предпринимать меры для исключения подмены изображения (например, задавать вопросы в случайном порядке);

○ сотрудник кредитной организации обязан осуществлять контроль качества изображения (достаточную освещенность, отсутствие объектов, скрывающих лицо и т.д.).

– Вне зависимости от метода сверки изображения клиента и фотографии на документе, в случае сомнений в принадлежности документа клиенту, достоверности представленных сведений, процедура идентификации будет прекращена и будет считаться неуспешной.

Рекомендательные стандарты к проведению идентификации клиентов-физических лиц кредитными организациями с использованием видеосвязи

– Вне зависимости от методов и технологий, используемых кредитной организацией при проведении идентификации клиента с использованием видеосвязи, данные между ними передаются по защищенным каналам связи.

– В случаях, предусмотренных действующими нормативными актами, кредитная организация вправе поручать проведение идентификации или сбор сведений и документов третьим сторонам. Данное право распространяется и на случаи проведения идентификации с использованием видеосвязи, но при соблюдении кредитными организациями всех нормативных требований. При этом ответственность за соблюдение требований по идентификации возлагается на кредитную организацию.

4. Фиксируемые сведения и хранение данных

– Кредитные организации фиксируют сведения о клиентах-физических лицах, а также осуществляют их обработку, в том числе хранение, в соответствии с требованиями нормативно-правовых актов;

– По результатам проведения идентификации клиентов с использованием видеосвязи, кредитные организации хранят полученные фотографии и (или) видеозаписи в досье клиента, в течение сроков, предписанных законодательством. Фотографии и (или) видеозаписи хранятся без потери качества, к ним должен быть обеспечен доступ по запросу.

5. Информирование клиента и защита данных

– Кредитные организации информируют клиента об условиях проведения видеоидентификации, фиксируют согласие на обработку персональных данных;

– Кредитные организации предоставляют доступ к полученным фотографиям или видеозаписям третьим сторонам только с прямого разрешения клиента или если такой доступ предоставляется в соответствии с требованиями законодательства;

– Хранение и защита полученных данных осуществляется в соответствии с требованиями законодательства об информации, информационных технологиях и защите информации;

– В случае, если идентификация не проведена по техническим причинам (например, недостаточной освещенности, обрывов связи, некачественного соединения), кредитная организация уведомляет клиента о причине отказа.