СОВРЕМЕННЫЙ GR И ЭКОНОМИЧЕСКОЕ РАЗВИТИЕ

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ МЕР БЕЗОПАСНОСТИ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ (ДБО)

Сенин В.Б.[19], Соболев П.А .[20]

В последнее время, на фоне стремительного технологического роста, для банков создаются все более продвинутые решения для взаимодействия с клиентами. Практически все банки стараются увести свое обслуживание в удаленные каналы. Это позволяет банкам увеличить свою клиентскую базу, сократить издержки, увеличить скорость обработки операций, повысить конкурентоспособность банка, предоставить клиентам совершать свои операции самостоятельно, без посещения офиса банка и т.д.

Ключевые слова:
Технологический рост, банки, дистанционное банковское обслуживание, конкурентоспособность

[19] **Сенин Владимир Борисович -** к.ю.н., профессор кафедры теории и практики взаимодействия бизнеса и власти НИУ ВШЭ, заместитель Председателя Правления АО «Альфа-Банк».

[20] **Соболев Павел Александрович -** sobolev_1995@icloud.com

ВВЕДЕНИЕ

В последнее время, на фоне стремительного технологического роста, для банков создаются все более продвинутые решения для взаимодействия с клиентами. Практически все банки стараются увести свое обслуживание в удаленные каналы. Это позволяет банкам увеличить свою клиентскую базу, сократить издержки, увеличить скорость обработки операций, повысить конкурентоспособность банка, предоставить клиентам совершать свои операции самостоятельно, без посещения офиса банка и т.д.

Любой банк обязан проводить комплекс мероприятий по обеспечению мер безопасности для удаленной идентификации клиента при дистанционном банковском обслуживании, при том, что первичная идентификация должна производиться при личном посещении банка, либо посещении другого банка со сдачей персональных данных в ЕБС.

Кредитным организациям запрещается открывать счета (вклады) клиентам без личного присутствия физического лица, открывающего счет (вклад), либо представителя клиента, за исключением случаев использования информации и документов, при которых клиент либо представитель клиента был идентифицирован при личном присутствии организацией, осуществляющей операции с денежными средствами или иным имуществом, которая является участником банковской группы или банковского холдинга и в которую входит соответствующая кредитная организация, а также в иных случаях, предусмотренных Федеральным законом.

Организации, осуществляющие операции с денежными средствами или иным имуществом, обязаны до приема на обслуживание идентифицировать клиента, представителя клиента и (или) выгодоприобретателя, за исключением ряда установленных случаев. Например, кредитные организации и иные организации, осуществляющие операции с денежными средствами или иным имуществом, регулирование, контроль и надзор за которыми в соответствии с законодательством Российской Федерации осуществляет Центральный банк Российской Федерации, при приеме на обслуживание клиентов для совершения операций (сделок) вправе идентифицировать клиента – физическое лицо, представителя клиента – юридического лица, имеющего право без доверенности действовать от имени юридического лица и являющегося физическим лицом, без личного присутствия путем установления и подтверждения достоверности сведений о них, с использованием единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном статьей 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», при соблюдении условий упомянутых в этом законе, а также, такой банк должен быть в списках, который публикует ЦБ. Для всех банков с универсальной лицензией обеспечение клиенту - физическому лицу возможности дистанционного открытия счёта с использованием ЕБС стало обязательным с 1 января 2021 г. Разумеется, если этого захочет клиент и подпишет согласие на биометрию по 152-ФЗ (биометрические персональные данные).

Постановления и распоряжения Правительства Российской Федерации № 820 от 14.07.2018 г., № 1322-Р от 30.06.2018 г.,

№ 772 от 30.06.2018 г., № 747 от 29.06.2018 г., № 321 от 25.06.2018 г., № 335 от 28.03.2018 г. периодически обновляются, в соответствии с развитием банковских технологий, а также в связи с выявлением новых методов обхода законодательства. В удаленных каналах обслуживания банку все также необходимо идентифицировать клиента, подтвердить сведения, которые клиент предоставил в банк, но уже с применением технических средств. Исключением является взятые Единой биометрической системой (ЕБС) слепок лица и голос, которые сняты при личном присутствии клиента. Объектом исследования являются технологии дистанционного банковского обслуживания, а предметом – проблемы регулирования (нормативные требования). Целью стать является выявление проблемы в обеспечении мер безопасности при дистанционном банковском обслуживании.

1. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПРИ ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ

Реализация системного подхода к регулированию в сфере развития финансовых технологий предполагает создание необходимых условий для их применения, в том числе, за счет повышения гибкости и адаптивности регулирования; совершенствование инструментов защиты прав потребителей цифровых финансовых услуг, а также требований по информационной безопасности, защите персональных данных или иных мер.

В целях обеспечения условий для развития инноваций на финансовом рынке и перехода к цифровой экономике в Российской Федерации в Банке России создана специальная «регулятивная песочница» для апробации инновационных финансовых технологий, продуктов и услуг. Регулятивная площадка Банка России может обеспечить быструю проверку гипотез о положительных эффектах для финансового рынка и потребителей от внедрения инновационных финансовых технологий и сервисов, анализ рисков и формирование моделей угроз, возникающих при их использовании; формирование предложений по изменению действующего нормативно-правового регулирования. Реализация данного механизма предусмотрена перечнем поручений Президента Российской Федерации от 21.10.2017 г. № Пр-2132. Одновременно Банк России совместно с заинтересованными федеральными органами исполнительной власти принимают участие в реализации мероприятий, которые также содержатся в указанном перечне поручений Президента Российской Федерации и предусматривают внесение в законодательство Российской Федерации следующих изменений в области регулирования цифровых технологий в финансах:

- определение статуса цифровых технологий, применяемых в финансовой сфере, и их понятий, исходя из обязательности рубля в качестве единственного законного платежного средства в Российской Федерации;
- установление требований к организации и осуществлению майнинга;
- регулирование публичного привлечения денежных средств и криптовалют путем размещения токенов.

Принятие данных изменений в законодательство позволит обеспечить эффективное и безопасное развитие финансовых технологий в интересах государства, участников рынка и населения. Для банка одним из основных условий для благоприятного развития стоит облегчение на уровне

законодательства доступа и идентификации, чтобы предложить клиенту максимальное количество банковских сервисов через дистанционное обслуживание.

В последнее время инициирование актов, относящихся к регулированию предоставления дистанционных услуг, наиболее активно. К основным документам относятся:

- Указ президента РФ от 09.05.2017 № 43 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» (далее – Указ);
- Стратегия государственной политики РФ в области защиты прав потребителей на период до 2030 года (утв. распоряжением Правительства РФ от 28.08.2017 № 1837-р);
- Стратегия пространственного развития Российской Федерации на период до 2025 года (утв. Распоряжением Правительства РФ от 13.02.2019 №207-р);
- Решение Высшего Евразийского экономического совета от 19.05.2020 № 6 «Об основных ориентирах макроэкономической политики государств – членов Евразийского экономического союза на 2020-2021 годы»;
- Перечень поручений Президента РФ по итогам совещания о планах реализации принятых мер по поддержке российской экономики в части, касающейся банковского кредитования от 09.05.2020 г. № Пр-795;
- Стратегия повышения финансовой доступности в Российской Федерации на период 2018-2020 годов (одобрена Советом директоров Банка России 26.03.2018);
- Основные направления развития финансового рынка Российской Федерации на период 2019-2021 годов (утв. Банком России);
- Доклад «Цифровой рубль. Доклад для общественных консультаций (октябрь 2020 года)» (утв. Банком России).

Регуляторы, исходя из вышеперечисленных документов, ставят перед собой следующие задачи:

- внедрение информационно-телекоммуникационных технологий;
- усиление влияния научно-технического прогресса на пространственное развитие РФ;
- законодательная регламентация доступа организаций к персональным данным граждан и данных ЮЛ, порядок их обработки и государственной защиты;
- внедрение механизма удаленной идентификации через ЕБС (Единая биометрическая система);
- обеспечение равных возможностей доступа граждан к финансовым услугам вне зависимости от их местоположения;
- ускоренное внедрение в финансовый сектор онлайн-технологий, обеспечивающих возможность дистанционного заключения кредитных договоров с идентификацией (соответствующей нормам законодательства) клиентов с использованием ЕСИА;
- обеспечение доступности базовых финансовых услуг путем комбинации офисного, агентского, дистанционного финансового обслуживания.

ЦБ в рамках «Регулятивной песочницы» (Регулятивная песочница — особый правовой режим, позволяющий юридическим лицам, занимающимся разработкой новых финансовых продуктов и услуг, проводить в ограниченной среде эксперименты по их внедрению без риска нарушения действующего законодательства) реализует пилотный проект проведения сеанса

видеоконференции с физическим лицом в целях реализации кредитной организацией процедуры проверки личности физического лица и сбора идентификационных сведений согласно ФЗ от 07.08.2001 г. № 115ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Стартовал данный пилот в ноябре 2020 г.

Минэкономразвития РФ в январе 2021 г. применил ЭПР (Экспериментальный правовой режим) – применение специального регулирования в сфере цифровых инноваций в течение определенного периода времени в отношении определенного круга лиц с возможностью неприменения НПА или их отдельных норм общего – действующего на момент установления ЭПР – регулирования, которыми установлены, в частности, обязательные требования по лицензированию, аккредитации, сертификации, обязательному подтверждению соответствия, получению допуска и разрешения, направлению и получению юридически значимых сообщений, способам проведения идентификации сторон правоотношений в сфере цифровых инноваций. Целью данной инициативы является – формирование новых видов и форм экономической деятельности, способов их осуществления.

2. ОСУЩЕСТВЕЛЕНИЕ МЕР БЕЗОПАСНОСТИ ДБО

Применение цифровых финансовых технологий, с одной стороны, способствует развитию финансового рынка, повышению финансовой доступности и развитию конкуренции, с другой – появлению новых рисков информационной безопасности. С развитием цифровых технологий возникает рост киберугроз, требующих оперативного и своевременного обнаружения, оценки и разработки соответствующих мер по их предотвращению либо минимизации возможных последствий.

Меры и способы контроля уполномоченного органа для обеспечения безопасности при применении новых технологий

Наиболее обширными сферами регулирования при обеспечении безопасности со стороны регулятора и коммерческих банков остается противодействие отмыванию денег, валютный контроль, а также информационная безопасность. Для государства борьба с сомнительными операциями, несущие повышенный риск по ПОД/ФТ (определенные 375-П ЦБ РФ) является очень важной задачей, ведь невозможно эффективно бороться с криминалом, не перекрыв его финансовые потоки, применяя не только административные меры, но и экономические.

Банк России ведет борьбу с сомнительными операциями в финансовой системе во взаимодействии с Росфинмониторингом, правоохранительными органами, Федеральной налоговой службой и другими контрольно-надзорными органами. Но эффективность механизма противодействия незаконным финансовым потокам возможна, только если финансовая система сама ставит заслон для экономической активности преступных элементов. Так, банки имеют право отказывать в открытии счетов, а также блокировать их, если таковые открыты, не открывать депозитные счета или проводить операции клиентам, чья добросовестность вызывает сомнения.

Легализация преступных доходов — это серьезное экономическое преступление. Преступники стремятся

скрыть истинное происхождение и назначение своих денег, которые обычно связаны с коррупцией, уклонением от уплаты налогов, наркобизнесом, деятельностью террористических организаций и другими видами организованной преступности. Для банков выявление сомнительных операций — сложная и дорогостоящая работа. Банк России постоянно оказывает им методологическую поддержку, например, определяет основные признаки сомнительности операций, а также предоставляет банкам информацию о лицах, которым ранее было отказано в банковском обслуживании из-за сомнений в их добросовестности.

Во второй половине 2021 г. Банк России планирует запустить платформу для банков «Знай своего клиента» — систему, которая будет предоставлять необходимую информацию об уровне риска вовлеченности в проведение сомнительных операций потенциальных и существующих клиентов. Предполагается, что это сократит и издержки банков (в необозримом будущем), и число необоснованных отказов их клиентам. Однако, данная платформа не находит широкого применения в мире (Известно, что лишь Сингапур работает в данном направлении), поскольку из-за этого сокращается функционал банков; обеспечивается менее демократичное отношение к клиентам, которые находятся в красной зоне (изъятие денежных средств во внесудебном порядке); данная система очень дорогостояща, и естественно это бремя ляжет на коммерческие банки, а потом, соответственно, на клиентов.

Незаконные финансовые операции часто носят трансграничный характер, поэтому борьба с отмыванием денег, полученных преступным путем, и финансированием терроризма ведется на международном уровне. Для эффективной борьбы с этими явлениями разработаны и постоянно актуализируются международные рекомендации в сфере противодействия отмыванию денег, финансированию терроризма, распространению оружия массового уничтожения (ПОД/ФТ/ФРОМУ). Разработкой стандартов и контролем за их выполнением всеми государствами занимается специализированная межправительственная организация — Группа разработки финансовых мер борьбы с отмыванием денег (Financial Action Task Force, FATF). Банк России и Росфинмониторинг принимают активное участие в работе FATF и активно взаимодействует с зарубежными партнерами в сфере ПОД/ФТ. Основные положения, регламентирующие вопросы ПОД/ФТ/ФРОМУ, содержатся в Федеральном законе от 07.08.2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Банк России также контролирует проведение валютных операций кредитными и не кредитными финансовыми организациями. Валютный контроль — часть государственной политики: он направлен на обеспечение устойчивость профицита платежного баланса РФ и стабильности внутреннего валютного рынка страны. Это направление деятельности регулируется ФЗ от 10.12.2003 г. № 173-ФЗ «О валютном регулировании и валютном контроле».

Активное внедрение современных технологий дает новые возможности как потребителям финансовых услуг, так и тем, кто их предоставляет: скорость, доступность, комфорт получения разного рода сервисов постоянно увеличиваются. Однако новые технологии несут и новые угрозы — киберриски, к которым относятся:

- хищение средств клиентов финансовых организаций,
- финансовые потери самих участников рынка,
- нарушение надежности и непрерывности предоставления финансовых услуг,
- развитие системного кризиса (например, биржи, платежные системы, клиринговый центр, центральный депозитарий) из-за кибератак, поразивших крупнейшие организации.

Чтобы киберриски не приводили к таким серьезным последствиям, Банк России следит за киберустойчивостью финансовых организаций, предупреждает их о возможных новых типах атак и способах реагирования на них. В целях обеспечения технологической безопасности и устойчивости на финансовом рынке, являющейся ключевым элементом для эффективного внедрения цифровых технологий, будет осуществлен ряд мероприятий, в том числе, с учетом Стратегии развития Системы обеспечения информационной безопасности (СОИБ) Банка России и информационной безопасности банковской сферы и иных сфер финансового рынка Российской Федерации на 2018–2022 гг.:

- совершенствование комплекса отраслевых стандартов и правил, устанавливающих требования к обеспечению технологической устойчивости, бесперебойности и безопасности при применении финансовых технологий, и нормативное закрепление обязанности по их применению;
- разработка новых форм и методов взаимодействия и реагирования на информационные угрозы в рамках деятельности ФинЦЕРТ Банка России;
- проведение комплекса мероприятий по повышению технологической устойчивости, бесперебойности и безопасности при применении финансовых технологий, а также мониторингу состояния информационных систем финансовых организаций.

В результате планируется повысить уровень технологической безопасности и устойчивости при использовании финансовых технологий, а также оперативного взаимодействия с участниками финансового рынка на базе ФинЦЕРТ Банка России для своевременного реагирования и предотвращения кибератак.

Единая биометрическая система

Удаленная идентификация через единую биометрическую систему (ЕБС) — это механизм, который позволяет, физическим лицам получать финансовые услуги дистанционно в банках, подтвердив свою личность с помощью биометрических персональных данных (изображение лица и голос). Работа над созданием системы была начата в 2017 г. Инвестиции «Ростелекома» в создание единой биометрической системы составили ок. 250 млн руб. В декабре 2017 г. был принят закон, регулирующий отношения банков и физических лиц по удалённому созданию банковского счёта, а также были внесены поправки в ряд законов.

Демонстрацию работы ЕБС «Ростелеком», Центробанк и «Почта Банк» провели 7 июня 2018 г. на Международном финансовом конгрессе. Запуск ЕБС был осуществлён 30 июня 2018 г.: в список коммерческих организаций, уполномоченных собирать биометрическую информацию и предоставлять дистанционные услуги с использованием удалённой идентификации, было внесено 438 банков. В октябре 2018 г. «Ростелеком» и «Почта Банк» запустили удалённую идентификацию в мобильном

приложении. При этом крупнейший розничный банк России — «Сбербанк» — решил запустить ЕБС позже, в течение первого полугодия 2018 г. Осенью 2018 г. была опубликована карта точек банковского обслуживания, где можно сдать биометрические данные. Такие точки появились к тому моменту более чем в 100 городах РФ. Предполагалось, что к концу 2019 г. сервис сбора и фиксации биометрических данных будут предоставлять уже все подразделения уполномоченных для этого банков. Позже планы по ускоренному внедрению ЕБС в банках были скорректированы — Банк России признал наличие объективных трудностей (особенно у малых банков) и заявил о смягчении требований к банкам в части внедрения системы.

По состоянию на февраль 2020 г. темпы внедрения ЕБС были заметно ниже, чем планировалось ранее — из уполномоченных 438 банков к системе подключились только 233 (то есть чуть более половины). В ЕБС поступило около 120 тыс. образов биометрических данных граждан. В январе 2020 г. Государственная Дума приостановила принятие законопроекта (на скорейшем принятии которого настаивал Банк России), предписывающего банкам собирать биометрические данные клиентов. Однако заметное ускорение развитию нормативной базы ЕБС и всего проекта дистанционной идентификации потребителей финансовых услуг в целом придала эпидемия CoVid-19. Уже в апреле 2020 г. спрос на удалённую идентификацию вырос на 16 % по сравнению с мартом.

22 апреля 2020 г. в Государственную Думу был внесен законопроект № 946734-7 (инициатор — Анатолий Аксаков) о внесении изменений в Закон об информации, предусматривающий дистанционную регистрацию граждан в Единой биометрической системе. Внесение этих поправок объяснялось стремлением повысить доступность финансовых услуг для населения в условиях пандемии. Согласно этому же законопроекту, предоставление биометрических данных для ЕБС перестало быть инициативой исключительно граждан — было предложено установить право госорганов, банков и иных организаций, осуществляющих сбор и обработку биометрических персональных данных, размещать их в Единой биометрической системе с согласия граждан. Летом 2020 г. правительство предложило передать ЕБС в собственность государства и придать ей статус государственной информационной системы (ГИС), оставив за Ростелекомом функции её оператора. Осенью 2020 г. было объявлено, что до конца этого года будут приняты поправки к закону, расширяющие возможности использования биометрии. В результате банки смогут предоставлять различным торговым и другим розничным сетям (ресторанам, кафе и пр.) сервис оплаты покупок с помощью биометрических данных (то есть по лицу клиента). В ноябре 2020 г. стало известно, что технологии ЕБС будут использоваться как один из элементов системы открытия банковских счетов и проведения банковских операций по видеосвязи, которую ЦБ будет тестировать с рядом коммерческих банков.

Законом 479-ФЗ от 29 декабря 2020 г. были внесены изменения по вопросам сбора и использования биометрических персональных данных. Единая биометрическая система может применяться для оказания физическим и юридическим лицам любых финансовых услуг (а не только для открытия счета и выдачи кредита). Банки с базовой лицензией вправе (а не обязаны) собирать биометрические данные в единую биометрическую систему. Сведения о

клиенте размещаются в системе только с его согласия и на безвозмездной основе. Запрещено отказывать в обслуживании клиентам, не давшим согласие на передачу своих данных в систему. Единой биометрической системе присвоен статус государственной информационной системы. Все собранные банками биометрические персональные данные будут внесены в единую систему идентификации и аутентификации (ЕСИА). Появится возможность сбора биометрии через МФЦ. Также предусмотрена возможность реализации органами своих функций, в том числе, оказание государственных и муниципальных услуг, только с использованием единой биометрической системы. Оператор системы взимает плату за ее использование организациями, ИП и нотариусами в соответствии с утвержденной методикой расчета. Закон вступил в силу с 1 января 2021 г., за исключением отдельных положений, для которых предусмотрены иные сроки.

Механизм удаленной идентификации разработан Банком России в рамках реализации Основных направлений развития финансовых технологий на период 2018—2020 гг. Создание и развитие платформы для удаленной идентификации позволяет перевести финансовые услуги в цифровую среду, повысить доступность финансовых услуг для потребителей, в том числе, людей с ограниченными возможностями, пожилого и мало мобильного населения, а также увеличить конкуренцию на финансовом рынке. Для реализации механизма удаленной идентификации разработаны нормативные (правовые) акты, а также сформирована технологическая инфраструктура, в том числе, Единая биометрическая система, которая совместно с Единой системой идентификации и аутентификации (ЕСИА) обеспечит достоверную идентификацию пользователей, но для этого необходимо пересдавать слепок раз в 3 года.

Процедура для пользователя является добровольной и будет осуществляться только с согласия клиента. Для успешного пользования системой, гражданину необходимо соблюсти перечень необходимых действий:

1) Первичная регистрация биометрических данных, для чего гражданину нужно прийти в один из уполномоченных банков или МФЦ, обладающих правом проводить регистрацию физических лиц в Единой системе идентификации и аутентификации (ЕСИА) и Единой биометрической системе. Такой Банк проведет идентификацию физического лица при личном присутствии, зарегистрирует его в ЕСИА, а также снимет биометрические параметры (сфотографирует и запишет образец голоса) и направит их в Единую биометрическую систему.

2) Получение банковских услуг с помощью удаленной идентификации. Для получения услуги в банке гражданину нужно зайти на сайт или мобильное приложение этого банка и выбрать получение услуги с использованием удаленной идентификации. Далее необходимо пройти авторизацию в ЕСИА и подтвердить свои биометрические данные с помощью смартфона, планшета, ноутбука или стационарного компьютера с камерой и микрофоном. Для подтверждения своих биометрических данных с мобильного устройства необходимо скачать мобильное приложение Единой биометрической системы. Приложение доступно в APP STORE и GOOGLE PLAY. После сравнения лица и голоса гражданина с ранее внесенными в Единую биометрическую

систему данными, он сможет открыть счет (вклад), получить кредит, сделать перевод, не приходя в банк.

Вследствие постепенного инфраструктурного и технологического переустройства, банки в своих структурных подразделениях начали обеспечивать сбор биометрических данных очень динамично. На 1 марта 2020 года такой сервис предоставляется в более чем в 13,5 тыс. структурных подразделениях банков.

3. ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ДБО

Современные международные стандарты идентификации клиентов банка

К компетентным наднациональным регуляторам, занимающимся разработкой мер, которые позволят эффективно идентифицировать настоящего и будущего клиента, для кредитной организации относится ФАТФ. Рекомендации ФАТФ необходимо соблюдать, поскольку данные меры признаны международным сообществом как эффективные, а также позволят нашей стране быть звеном цепи глобальной и безопасной финансовой системы. ФАТФ занимается разработкой стандартов, направленных на содействие эффективному применению правовых, регулирующих и оперативных мер по борьбе с отмыванием денег, финансированием терроризма и распространением оружия массового уничтожения и иными связанными угрозами целостности международной финансовой системы злоупотреблениями. В рекомендации ФАТФ также входит перечень мероприятий, необходимых для надлежащей идентификации клиента, чтобы избежать вышеописанных рисков. ФАТФ рекомендует использовать риск-ориентированный подход для осуществления регулирования банковского контроля.

Существуют обстоятельства, характеризующиеся более высокой степенью риска отмывания денег или финансирования терроризма и требующие принятия усиленных мер НПК (надлежащая проверка клиента). При оценке рисков отмывания денег и финансирования терроризма, связанных с типами клиентов, странами или географическими областями, конкретными продуктами, услугами, операциями (сделками) или каналами поставок, примеры ситуаций потенциально высокого риска (помимо указанных в Рекомендациях с 12-й по 16-ю ФАТФ), могут быть следующими:

(a) факторы риска, связанные с клиентом:

- деловые отношения осуществляются при необычных обстоятельствах (например, слишком большое необъяснимое географическое расстояние между финансовым учреждением и клиентом);
- клиенты не являются резидентами;
- для управления личными средствами используются юридические лица или образования;
- компании имеют номинальных акционеров или акции на предъявителя;
- бизнес интенсивно использует наличную форму расчетов;
- структура собственности компании кажется необычной или излишне сложной, учитывая характер деятельности компании;

(b) страновые или географические факторы риска:

- страны, не имеющие надлежащих систем ПОД/ФТ, что должно быть установлено такими надежными источниками, как отчеты о взаимной оценке, или отчеты о деталь страны, в отношении которых применены санкции,

эмбарго или аналогичные меры, установленные, например, ООН;

▪ страны, определенные надежными источниками как имеющие высокий уровень коррупции или другой преступной деятельности;

▪ страны или географические области, которые, по данным надежных источников, предоставляют финансирование или поддержку террористической деятельности или на территории которых действуют установленные террористические организации.

Существуют обстоятельства, в которых риск отмывания денег или финансирования терроризма может быть ниже. В таких обстоятельствах и при условии, что страной или финансовым учреждением был проведен должный анализ риска, страна имеет все основания разрешить своим финансовым учреждениям применять упрощенные меры НПК (надлежащая проверка клиента). При оценке рисков отмывания денег и финансирования терроризма, связанных с категориями клиентов, странами или географическими областями, а также определенными продуктами, услугами, операциями (сделками) или каналами поставки, примеры потенциально низкого риска могут быть следующими:

(a) факторы риска, связанные с клиентом:

▪ финансовые учреждения и Установленные нефинансовые предприятия и профессии (УНФПП), (если они обязаны выполнять требования по борьбе с отмыванием денег и финансированием терроризма в соответствии с Рекомендациями ФАТФ) эффективно выполняют эти требования, и в отношении них в соответствии с Рекомендациями осуществляется должный надзор и контроль, обеспечивающий соблюдение этих требований;

▪ публичные компании, зарегистрированные на фондовой бирже и обязанные раскрывать информацию в целях обеспечения достаточной прозрачности бенефициарной собственности (либо по правилам биржи, либо по закону, либо в соответствии с иными требованиями);

▪ органы государственной власти, государственные организации и предприятия;

(b) факторы риска, связанные с продуктами, услугами, операциями (сделками) или каналами поставки:

▪ полисы страхования жизни с незначительной суммой страхового взноса; например, годовой страховой взнос не превышает 1000 долларов США / евро или общий взнос не превышает 2500 долларов США / евро;

▪ страховые полисы в рамках пенсионной системы, если отсутствует положение об уступке и полис не может использоваться в качестве обеспечения;

▪ системы пенсионного обеспечения, включая пенсии по старости или аналогичные системы, если взносы осуществляются путем вычета из заработной платы и если правила системы не допускают переуступку выплаты процентов участника пенсионной системы;

▪ четко определенные и ограниченные по объему финансовые продукты и услуги, предоставляемые определенной категории клиентов для облегчения доступа к этим продуктам и услугам;

(c) страновые факторы риска:

▪ страны, которые, по данным надежных источников, таких как отчеты о взаимной оценке, или детальные отчеты об оценке, или опубликованные отчеты о

прогрессе, имеют эффективные системы ПОД/ФТ;

▪ страны, которые, по данным надежных источников, характеризуются низким уровнем коррупции или другой преступной деятельности;

▪ при оценке риска страны или финансовые учреждения также могут при необходимости учитывать возможные различия в рисках отмывания денег и финансирования терроризма в различных областях или регионах внутри страны.

Наличие более низкого риска отмывания денег и финансирования терроризма для целей идентификации и проверки вовсе не означает, что тот же самый клиент характеризуется низкой степенью риска для всех мер НПК, в особенности для постоянного мониторинга операций (сделок). При оценке рисков отмывания денег и финансирования терроризма, связанных с категориями клиентов, странами или географическими областями, а также определенными продуктами, услугами, операциями (сделками) или каналами поставки, финансовое учреждение должно принимать во внимание переменные риска, связанные с указанными категориями риска. Эти переменные факторы, по отдельности или в совокупности, могут повысить или снизить потенциальный риск, влияя таким образом на определение необходимого уровня мер НПК. Примеры таких переменных факторов включают: цель открытия счета или установления отношений; уровень активов, размещаемых клиентом, или сумма проводимых трансакций; регулярность и длительность деловых отношений.

Финансовые учреждения обязаны принимать меры по надлежащей проверке клиентов (НПК) при:

1) установлении деловых отношений;

2) совершении разовых операций (сделок): (1) на сумму, превышающую установленное пороговое значение (15 тыс. долл. США / евро); или (2) которые являются электронными переводами при обстоятельствах, подпадающих под действие положений Пояснительной записки к Рекомендации 14;

(3) наличии подозрений в отмывании денег или финансировании терроризма;

(4) наличии у финансового учреждения сомнений в достоверности или достаточности полученных ранее данных о личности клиента.

Принцип, устанавливающий обязанность финансовых учреждений проводить НПК, должен быть установлен в законе. Каждая страна может определить, каким образом она налагает конкретные обязанности по НПК - либо через закон, либо через другие обязательные для исполнения меры.

Необходимо принимать следующие меры НПК:

(a) идентификация клиента и подтверждение личности клиента с использованием надежных, независимых первичных документов, данных или информации;

(b) определение бенефициарного собственника и принятие таких разумных мер по проверке личности бенефициарного собственника, которые позволят финансовому учреждению считать, что ему известно, кто является бенефициарным собственником. Для юридических лиц и образований это должно включать получение информации финансовыми учреждениями о структуре управления и собственности клиента;

(c) понимание и, когда это необходимо, получение информации о целях и предполагаемом характере деловых отношений;

(d) проведение на постоянной основе надлежащей проверки деловых отношений и тщательный анализ сделок, совершенных в рамках таких отношений, чтобы убедиться в соответствии проводимых сделок сведениям финансового учреждения о клиенте, его хозяйственной деятельности и характере рисков, в том числе, когда необходимо, об источнике средств.

Финансовые учреждения обязаны применять каждую из мер НПК в соответствии с пунктами (a)–(d) выше, но им следует выбирать степень применения этих мер с помощью риск-ориентированного подхода (РОП) и в соответствии с Пояснительной запиской к этой Рекомендации и к Рекомендации 1. Финансовые учреждения обязаны проверять личность клиента и бенефициарного собственника до или в ходе установления деловых отношений или совершения операций (сделок) с разовыми клиентами. Страны могут разрешить финансовым учреждениям завершить проверку клиентов в разумно сжатые сроки после установления деловых отношений в том случае, если риски отмывания доходов и финансирования терроризма практически сведены к минимуму, и если это крайне важно для бесперебойного осуществления нормальной деятельности.

4. НАДЛЕЖАЩАЯ ПРОВЕРКА КЛИЕНТОВ И РАЗГЛАШЕНИЕ

Если во время установления или уже в ходе отношений с клиентом или при проведении разовых операций (сделок) у финансового учреждения возникнут подозрения, что операции (сделки) связаны с отмыванием денег или финансированием терроризма, то этому учреждению следует:

(a) в рамках обычной процедуры постараться установить и удостоверить личность клиента и бенефициарного собственника, будь то постоянного или разового, а также независимо от любых исключений или любых установленных пороговых значений, которые могли бы применяться в ином случае;

(b) направить сообщение о подозрительной операции (СПО) в подразделение финансовой разведки (ПФР) в соответствии с Рекомендацией 20.

В соответствии с Рекомендацией 21 финансовым учреждениям, их директорам, служащим и сотрудникам запрещается разглашать факт передачи в ПФР СПО или связанной с ним информации. Когда в данных обстоятельствах финансовое учреждение пытается выполнить обязательства по надлежащей проверке клиента (НПК), существует риск, что клиент может быть непреднамеренно об этом предупрежден. Знание клиента о возможном СПО или расследовании может помешать будущим усилиям по расследованию операции (сделки) по подозрению в связи с отмыванием денег или финансированием терроризма. Поэтому, если у финансовых учреждений возникают подозрения, что операции (сделки) связаны с отмыванием денег или финансированием терроризма, при осуществлении процесса НПК они должны учитывать риск разглашения информации клиенту. Если учреждение обоснованно считает, что осуществленного клиента, оно может предпочесть не инициировать этот процесс, а направить СПО. Учреждениям следует обеспечивать, чтобы их сотрудники были знакомы с этими вопросами и понимали их при проведении НПК.

При выполнении пунктов (a) и (b) мер НПК, указанных в Рекомендации 10, финансовые учреждения должны также быть обязаны проверять, обладает ли лицо, намеревающееся действовать от имени клиента, соответствующими полномочиями, а также установить и

удостоверить личность такого лица. При выполнении процедур НПК в отношении клиентов, являющихся юридическими лицами или юридическими образованиями, финансовые учреждения должны быть обязаны установить и удостоверить личность клиента, изучить характер его деятельности, форму собственности и структуру управления. Требования к идентификации и проверке клиентов и бенефициарных собственников, изложенные ниже в пунктах (a) и (b), направлены на решение двух задач: во-первых, предотвращение незаконного использования юридических лиц и образований посредством глубокого изучения клиента для правильной оценки связанных с деловыми отношениями потенциальных рисков отмывания денег и финансирования терроризма и, во-вторых, принятие соответствующих мер для снижения этих рисков.

В данном контексте финансовые учреждения должны быть обязаны:

(a) идентифицировать клиента и удостоверить его личность. Меры, которые обычно необходимы для удовлетворительного выполнения данной функции, потребуют получения следующей информации:

(1) название, юридическая форма и документ об учреждении — проверку можно осуществить, например, по свидетельству о регистрации, свидетельству о юридическом статусе и финансовом положении, партнерскому соглашению, трастовому договору или другим документам из надежного независимого источника, подтверждающим название, форму и текущий статус клиента;

(2) правомочия, регулирующие деятельность и обязательства юридического лица или образования (например, устав и учредительный договор), а также имена соответствующих лиц, занимающих высшие руководящие должности в структуре такого юридического лица или образования (например, старших управляющих, директоров компании, доверительных собственников траста);

(3) адрес зарегистрированного офиса и, если они отличаются, фактический адрес места осуществления деятельности;

(b) идентифицировать бенефициарных собственников клиента и принимать разумные меры для удостоверения личности таких лиц, используя следующую информацию:

(1) для юридических лиц:

(1.1) личные данные физических лиц (если таковые есть), владеющих в конечном итоге контрольной долей участия в юридическом лице;

(1.2) в тех случаях, когда имеются сомнения по пункту, являются ли лица (лицо) с контрольной долей участия бенефициарными собственниками (собственником), или ни одно физическое лицо не осуществляет контроль через имущественные интересы, личные данные физических лиц (если есть), осуществляющих контроль юридического лица или образования на иных основаниях;

(1.3) если физических лиц, указанных выше в пунктах (1.1) или (1.2), не выявлено, то финансовые учреждения должны идентифицировать и принять разумные меры для удостоверения личности соответствующего физического лица, занимающего старшую руководящую должность;

(2) для юридических образований:

(2.1) трасты — идентификационные данные учредителя, доверительных собственников, протектора (если есть), бенефициаров или класса бенефициаров и любого другого физического лица, имеющего действительный контроль над

трастом (в том числе, через цепочку контроля или владения). Контрольная доля участия зависит от структуры собственности компании. Она может базироваться на пороговом значении, например, любое лицо, владеющее долей участия свыше определенного процента компании (например, 25%). Для бенефициаров трастов, которые названы по характеристикам или по классу, финансовые учреждения должны получить достаточную информацию о бенефициаре, чтобы она убедила финансовое учреждение в том, что оно сможет установить личность бенефициара на момент выплаты или когда бенефициар намеревается воспользоваться предоставленными ему правами.

(2.2) другие типы юридических образований — идентификационные данные лиц, занимающих аналогичные позиции. Если клиент или владелец контрольной доли участия является компанией, зарегистрированной на фондовой бирже и подлежащей требованиям о публикации информации (либо по правилам фондовой биржи, либо по закону, либо согласно обязательным для исполнения актам), которые налагают требования обеспечить достаточную прозрачность бенефициарной собственности, или является дочерним предприятием, где мажоритарный пакет принадлежит такой компании, устанавливать и проверять личности акционеров или бенефициарных владельцев таких компаний не требуется. Необходимые идентификационные данные можно получить из открытого реестра, от клиента или из других надежных источников.

Меры по НПК, указанные в Рекомендации 10, не подразумевают, что финансовые учреждения должны повторно идентифицировать и подтверждать личность каждого клиента каждый раз, когда клиент осуществляет сделку. Учреждение имеет право полагаться на уже принятые им меры по установлению и подтверждению личности до тех пор, пока у него не появятся сомнения в отношении достоверности этой информации. Примерами ситуаций, которые могут привести учреждение к таким сомнениям, могут служить ситуации, когда возникает подозрение в связи с отмыванием денег в отношении данного клиента или когда имеет место существенное изменение в операциях по счету клиента, которое не соответствует деловому профилю бизнеса клиента.

От компаний и посредников в секторе ценных бумаг может требоваться проводить операции очень быстро, в соответствии с условиями рынка на момент, когда клиент связывается с ними, и проведение сделок может быть необходимым до завершения проверки личности. Финансовым учреждениям необходимо будет также установить процедуры управления рисками в отношении условий, в которых клиент может использовать деловые отношения до проведения проверки. Эти процедуры должны включать набор таких мер, как ограничение количества, видов и/или сумм сделок, которые могут быть проведены, и мониторинг крупных и сложных сделок, осуществляемых вне рамок ожидаемых для такого типа отношений норм.

От финансовых учреждений необходимо требовать применения мер НПК в отношении существующих клиентов с учетом значимости и риска и в соответствующее время проводить надлежащую проверку таких существующих отношений с учетом того, проводились ли и когда проводились предыдущие проверки и достаточно ли полученных данных.

Усиленные меры НПК

Финансовые учреждения должны изучать, в пределах разумного, основания и цель всех сложных, необычно крупных операций (сделок) и всех необычных схем сделок, которые не имеют очевидной экономической или правовой цели. При повышенном риске отмывания денег или финансирования терроризма финансовые учреждения должны быть обязаны принимать усиленные меры НПК в соответствии с выявленными рисками. В частности, они должны усилить степень и характер мониторинга деловых отношений, чтобы определить, являются ли соответствующие операции (сделки) или деятельность необычными или подозрительными. Примеры усиленных мер НПК, которые могут применяться в отношении деловых отношений, характеризующихся повышенным риском, включают:

- получение дополнительной информации о клиенте (например, род деятельности, размер активов, информация, доступная через открытые базы данных, Интернет и т.д.) и более частое обновление данных по клиенту и бенефициарному собственнику;
- получение дополнительной информации о характере деловых отношений;
- получение информации об источнике средств или источнике состояния клиента;
- получение информации о причинах запланированных или проведенных операций (сделок);
- получение от высшего руководства разрешения на установление или продолжение деловых отношений; осуществление усиленного мониторинга деловых отношений, путем увеличения количества и частоты проверок и выявления характера операций (сделок), которые требуют дальнейшей проверки;
- требование о проведении первого платежа через открытый на имя клиента счет в другом банке, подчиняющемся аналогичным стандартам НПК. Упрощенные меры НПК

При низкой степени риска отмывания денег или финансирования терроризма финансовым учреждениям может быть разрешено принимать упрощенные меры НПК в зависимости от характера низкого риска. Упрощенные меры должны быть соизмеримы с факторами более низкого риска (например, упрощенные меры могут применяться только в отношении принятия клиента на обслуживание или параметров текущего мониторинга). Примеры возможных действий:

- проверка личности клиента и бенефициарного собственника после установления деловых отношений (например, при превышении суммы сделок установленного порога);
- сокращение частоты обновления идентификационных данных по клиенту;
- снижение уровня текущего мониторинга и проверки трансакций на основе разумного порога суммы;
- определение целей и характера отношений на основе анализа характера операций (сделок) или установленных деловых отношений без проведения сбора особой информации или без выполнения особых мер.

Упрощенные меры НПК недопустимы, когда существуют подозрения в отмывании денег или финансировании терроризма или если применяются особые сценарии повышенной степени риска. Установленным порогом для разовых сделок по Рекомендации 10 является 15 тыс. долл. США / евро. Финансовые операции (сделки) выше установленного порога включают ситуации, когда операция (сделка) осуществляется одной операцией

или несколькими операциями (сделками), которые кажутся связанными. Финансовые учреждения обязаны обеспечить обновляемость и существенность документов, данных или информации, собираемой в рамках процесса НПК, путем проведения анализа существующих данных, особенно для категорий клиентов или деловых отношений более высокого риска.

В тех случаях, когда финансовое учреждение не может выполнить подходящие требования пунктов выше (с учетом соответствующей корректировки степени этих мер согласно риск-ориентированному подходу), оно должно быть обязано не открывать счет, не вступать в деловые отношения и не осуществлять сделку, или оно должно быть обязано прекратить деловые отношения и ему следует рассмотреть вопрос о направлении сообщения о подозрительной операции (сделке) в отношении этого клиента. Эти требования должны применяться ко всем новым клиентам, хотя финансовым учреждениям следует также применять эту Рекомендацию в отношении существующих клиентов, исходя из масштаба деловых отношений и риска, а также проводить надлежащую проверку таких существующих отношений в соответствующие сроки.

Международное сообщество всецело заинтересовано в продвижении цифровых новшеств в области облуживания финансовых операций клиентов, посредством ДБО. Данные трансформации ведут к совершенствованию безопасности проведения внутренних и внешнеторговых финансовых операций. По данным доклада FATF по цифровой трансформации в области идентификации, список основных организаций, занимающихся данными разработками, следующий:

- Международная организация по стандартизации (ISO) - независимая международная организация, базирующаяся в Женеве, в состав которой входят 163 национальных органа по стандартизации (по одному на страну), которая разрабатывает добровольные, основанные на консенсусе, соответствующие рынку международные стандарты, которые предоставляют спецификации для продуктов. услуги и системы, обеспечивающие качество, безопасность и эффективность, а также поддержку инноваций. Некоторые из соответствующих стандартов включают: подтверждение личности и регистрацию физических лиц (ISO / IEC 29003: 2018); структура обеспечения аутентификации объекта (ISO / IEC 29115: 2013 - в стадии пересмотра) и применение Руководства по управлению рисками (ISO 3100: 2018) к рискам, связанным с идентификацией. Через свою недавно созванную Рабочую группу 7 TC6861 ISO в настоящее время работает над глобальными стандартами идентификации физических лиц, в том числе в цифровом контексте.

- Международный союз электросвязи (МСЭ) - специализированное учреждение ООН в области информационных и коммуникационных технологий (ИКТ), созданное для облегчения международного соединения в сетях связи. МСЭ распределяет глобальный радиочастотный спектр и спутниковые орбиты и разрабатывает технические стандарты, призванные обеспечить беспрепятственное соединение сетей и технологий ИКТ во всем мире.

- Консорциум World Wide Web (W3C) - международная организация, которая разрабатывает и продвигает широкий спектр добровольных, основанных на консенсусе открытых технических стандартов и протоколы для Интернета для поддержки

взаимодействия, масштабируемости, стабильности и отказоустойчивости. В области цифровых удостоверений W3C разработал стандарт браузера / платформы веб-аутентификации для MFA с использованием биометрии, мобильных устройств и ключей безопасности FIDO, а также разрабатывает стандарты для подтвержденных заявлений об идентичности в децентрализованных системах идентификации.

- Альянс Fast Identity Online (FIDO) - отраслевая ассоциация, которая продвигает эффективные, простые в использовании решения для строгой аутентификации путем разработки технических спецификаций, которые определяют открытый, масштабируемый, совместимый набор механизмов для аутентификации пользователей; действующие отраслевые программы сертификации для обеспечения успешного принятия спецификаций во всем мире; и представление зрелых технических спецификаций в признанные организации по разработке стандартов (например, ISO, ITUX.1277 и X.1278) для формальной стандартизации. FIDO также участвует в проверке через свою рабочую группу по проверке личности и привязке (IDWG).

- OpenID Foundation (OIDF) - некоммерческая торговая организация, не зависящая от технологий, которая занимается продвижением услуг цифровой идентификации на основе открытых стандартов.

- GSMA - глобальная отраслевая ассоциация операторов сетей мобильной связи, которая участвует в разработке различных технических стандартов, применимых к платформам мобильной связи, включая стандарты идентификации и аутентификации пользователей.

- Европейский институт стандартов электросвязи (ETSI) является одним из трех основных европейских органов по стандартизации наряду с CEN и CENELEC. ETSI предоставляет членам открытую и инклюзивную среду для поддержки разработки, ратификации и тестирования глобально применимых стандартов для систем и услуг ИКТ во всех секторах промышленности и общества. ETSI работает над проверкой личности, в первую очередь нацеленной на услуги доверия, как это определено eIDAS, с потенциальным применением в других областях, таких как выпуск eID и процессы CDD. ETSI разработала набор стандартов для реализации требований RTS в рамках PSD2 для использования квалифицированных сертификатов, определенных в eIDAS, для идентификации третьих сторон (TPP) в платежных транзакциях.

- Система электронной идентификации в Европейском союзе - elDAS. Структура eIDAS обеспечивает три уровня гарантии для средств электронной идентификации, предоставляемых в рамках уведомленной схемы электронной идентификации: низкий, существенный и высокий. Регламент Комиссии (ЕС) 2015/1502 от 8 сентября 2015 г. устанавливает минимальные требования к безопасности для каждого из этих уровней. Международный стандарт ISO / IEC 29115 был принят во внимание для спецификаций и процедур, изложенных в этом имплементирующем акте, как основной международный стандарт, доступный в области уровней гарантии для средств электронной идентификации, содержание Регламента eIDAS отличается от этого международного стандарта, в частности в отношении требований к подтверждению и верификации личности, а также того, как учитываются различия между процедурами идентификации в государствах-членах и существующими в ЕС инструментами для той же цели. Если в стране ЕС / ЕЭЗ орган государственного

сектора требует для доступа к одной из своих онлайн-услуг электронную идентификацию со значительным или высоким уровнем или гарантией, он также должен принять, чтобы получить доступ к этой онлайн-услуге, все средства электронной идентификации с таким же или более высоким уровнем уверенности и относящиеся к схеме идентификации, о которой уведомила Комиссия и которые опубликованы в OJ (Официальном журнале Европейского Союза). Кроме того, органы государственного сектора могут на добровольной основе принять решение о признании схем электронной идентификации с низким уровнем гарантии.

Для целей eIDAS компонентами системы цифровой идентификации являются:

- зачисление гарантирует идентификацию, однозначно представляющую либо физическое, либо юридическое лицо, либо физическое лицо, представляющее юридическое лицо. Регистрация включает в себя разные этапы:

а) Заявление и регистрация:

(1) убедитесь, что заявитель осведомлен об условиях использования средств электронной идентификации;

(2) убедитесь, что заявитель осведомлен о рекомендуемых мерах безопасности, связанных со средствами электронной идентификации;

(3) соберите соответствующие идентификационные данные, необходимые для подтверждения и проверки личности.

б) Подтверждение и проверка личности, состоящая из проверки подлинности и действительности документа, удостоверяющего личность, и относящаяся к реальному человеку, а также проверка того, что личность этого человека является заявленной.

- Электронная идентификация означает управление, имеет дело с количеством и характером факторов аутентификации, независимо от того, спроектировано ли средство электронной идентификации таким образом, чтобы его можно было использовать только в том случае, если оно находится под контролем или во владении лица, которому оно принадлежит.

- Аутентификация устанавливает требования к каждому уровню гарантии в отношении механизма аутентификации, с помощью которого физическое или юридическое лицо использует средства электронной идентификации для подтверждения своей личности доверяющей стороне.

- Управление и организация, все участники предоставляют услуги, связанные с электронной идентификацией в трансграничном контексте, должны иметь документированные методы управления информационной безопасностью, политики, подходы к управлению рисками и другие признанные средства контроля, чтобы обеспечить соответствующие органы управления схемами электронной идентификации в соответствующих государствах-членах ЕС, что эффективная практика.

Для каждого из этих четырех этапов определены три уровня доверия: низкий, существенный и высокий в соответствии со следующими критериями:

- низкий обеспечивает ограниченную степень уверенности в заявленной или заявленной личности человека и характеризуется ссылкой на технические спецификации, стандарты и процедуры, связанные с ними, включая технические средства контроля, целью которых является снижение риска неправомерного использования или изменение личности;

- существенный обеспечивает значительную степень уверенности в заявленной или заявленной личности человека и характеризуется ссылкой на технические спецификации, стандарты и процедуры, связанные с ними, включая технические средства контроля, целью которых является существенное снижение риска неправомерного использования. или изменение личности;

- высокий обеспечивает более высокую степень уверенности в заявленной или заявленной личности человека, чем средства электронной идентификации со значительным уровнем уверенности, и характеризуется ссылкой на технические спецификации, стандарты и процедуры, связанные с ними, включая технический контроль, цель который должен предотвратить неправильное использование или изменения личности.

Предполагается, что когда средства электронной идентификации, выпущенные в соответствии с уведомленной схемой электронной идентификации, удовлетворяют требованию, перечисленному на более высоком уровне гарантии, то выполняют эквивалентное требование более низкого уровня гарантии.

NIST – Американская система

- Уровень удостоверения личности (IAL) относится к надежности процесса проверки удостоверения личности, как это определено требуемыми техническими требованиями к цифровому удостоверению личности. Уровни уверенности для проверки личности в порядке повышения надежности: IAL1; IAL2; и IAL3.

- Уровень гарантии аутентификации (AAL) относится к надежности процесса аутентификации. Уровни гарантии для аутентификации (и управления жизненным циклом учетных данных) в порядке повышения надежности: AAL1; AAL2; и AAL3.

- Уровень гарантии федерации (FAL) (если применимо) относится к надежности объединенной сети, то есть к надежности (силе) утверждения, используемого для передачи результатов аутентификации и информации об атрибутах ID в объединенной среде. Уровни гарантии для федерации в порядке увеличения надежности: FAL1; FAL2; и FAL3.

Германия является одной из первых стран, которой удалось наиболее точно структурировать порядок видеоидентификации клиента при проведении финансовых операций удаленно. В Германии данными полномочиями обладает Федеральное управление финансового надзора (BaFin), которое объединяет под одной крышей надзор за банками и поставщиками финансовых услуг, страховыми организациями и торговлей ценными бумагами. Это автономное учреждение публичного права, находящееся под юридическим и техническим надзором Федерального министерства финансов. Оно финансируется за счет сборов и взносов учреждений и предприятий, находящихся под его контролем. BaFin управляется Исполнительным советом Германии.

Ниже проведен порядок должной видеоидентификации клиента в соответствии с операционным Циркуляром BAFin. Видео идентификация может выполняться только надлежащим образом обученными сотрудниками обязанной организации или третьей стороны, которой обязанная организация передала на аутсорсинг требование идентификации клиента. Дальнейшее делегирование или частичное делегирование или привлечение третьей стороны третьей стороной не разрешается.

Указанные сотрудники должны быть знакомы с особенностями документов, разрешенных в процедуре видеоидентификации, которые могут быть проверены посредством указанной видеоидентификации (включая применимые методы проверки) вместе с общими возможностями подделки, и быть знакомым с соответствующими положениями о борьбе с отмыванием денег и защитой данных, а также с требованиями, изложенными в этом Циркуляре. Соответствующая документация должна быть доступна по принятым документам, их поддающимся проверке характеристикам и соответствующим учебным мероприятиям. Вышеупомянутому содержанию необходимо обучать сотрудников надлежащим образом до того, как они приступят к выполнению своих обязанностей по идентификации, а затем через регулярные промежутки времени, но не реже одного раза в год и по мере необходимости. Такая необходимость может быть оправдана, например, если есть изменения в правовых и / или надзорных требованиях или требованиях к защите данных, в случае значительного количества попыток мошенничества, если учреждение узнает о новых возможностях мошенничество, или если в процедуре есть другие недостатки.

В начале видео идентификации лицо, которое будет идентифицировано, должно дать свое явное согласие на весь процесс идентификации, а также на получение фотографий или снимков экрана с ним и их документа, удостоверяющего личность. Это согласие должно быть явно зарегистрировано.

При назначении случаев идентификации сотрудникам необходимо задействовать механизмы для противодействия предсказуемому распределению дел и связанной с этим возможности манипуляции. Видео идентификация должна выполняться в режиме реального времени и без перерывов. Необходимо надлежащим образом обеспечить целостность и конфиденциальность аудиовизуального общения между сотрудником и лицом, которое будет идентифицировано. По этой причине разрешены только видео чаты со сквозным шифрованием. Необходимо соблюдать рекомендации, содержащиеся в Техническом руководстве TR-02102 Федерального ведомства Германии по информационной безопасности (Bundesamt für Sicherheit in der Informationstechnik BSI). Кроме того, качество изображения и звука сообщения должно быть достаточно адекватным, чтобы без всяких сомнений можно было провести неограниченную идентификацию на основе всех проверок, предусмотренных в этом Циркуляре. В частности, они включают исследования элементов защиты, которые были отнесены к категории поддающихся визуальной проверке в белом свете, а также проверку, проводимую для проверки того, не был ли документ поврежден или подвергнут манипуляциям. Чтобы оценить качество передачи изображения, необходимо определить подходящие информативные элементы изображения, такие как гильошированные структуры и микропись. В процессе передачи видео соответствующий сотрудник должен создать фотографии / снимки экрана, на которых четко показано лицо, которое будет идентифицировано, а также лицевая и оборотная стороны документа, удостоверяющего личность, используемого этим лицом для идентификации, и информации, содержащейся в этом документе.

Разрешаются только документы, удостоверяющие личность, с элементами защиты, которые в достаточной степени

защищены от подделки, четко идентифицируемы и, следовательно, поддаются проверке как визуально в белом свете, так и с использованием доступной технологии передачи изображений, а также которые имеют машиночитаемую зону (штрих-код), могут быть используется в процессе видеоидентификации в качестве подтверждения личности в соответствии с правилами борьбы с отмыванием денег. Чтобы установить личность человека, который будет идентифицирован на основе разрешенного документа, удостоверяющего личность, сотрудник должен, прежде всего, убедиться, что документ, используемый в качестве подтверждения личности, содержит оптические элементы защиты, визуально идентифицируемые в белом свете, который такой тип обычно имеет.

В зависимости от типа документа к функциям оптической защиты относятся: дифракционные особенности (голограммы, идентиграмма, кинематические конструкции); технология персонализации (наклонные лазерные изображения, типография); материал (окно (например, персонализированное), защитная нить (индивидуальная), оптически изменяемые чернила); защитная печать (микро-буквенное обозначение; гильошированные структуры).

Соответствие предполагается, если выполняются критерии проверки по крайней мере трех элементов защиты, случайно выбранных из различных категорий в приведенном выше списке для целей идентификации и присущих документу, удостоверяющему личность. Сотрудник также должен убедиться, что документ, используемый в качестве удостоверения личности, обладает другими формальными характеристиками, визуально идентифицируемыми в белом свете и доступными для целей проверки (включая макет, количество, размер и расстояние между символами, а также типографику), которые документ такого типа обычно имеет.

Посредством подходящих ИТ-программ необходимо обеспечить, чтобы оптические элементы защиты, визуально идентифицируемые в белом свете в ходе видеоидентификации, по форме и содержанию соответствовали индивидуальным характеристикам, указанным в документе, удостоверяющем личность (например, путем сравнения первичных и вторичных фотографий, таких как идентификационная диаграмма, наклонное лазерное изображение и т.д.), или что они соответствуют ссылкам из базы данных документов, удостоверяющих личность. В качестве альтернативы использованию ИТ-поддержки подобное сравнение должно быть возможным с помощью кадров, выбранных сотрудником (если возможно, из серийной записи или записанных видеопоследовательностей) и введенных в качестве обязательной части процесса идентификации. Кроме того, сотрудник всегда должен проверять, что используемый документ, удостоверяющий личность, не поврежден, не подвергался манипуляциям и, в частности, не имеет прикрепленной к нему фотографии.

Во время визуальной идентификации идентифицируемое лицо должно наклонить свой документ по горизонтали или вертикали перед камерой и выполнить любые дополнительные движения в соответствии с инструкциями сотрудника. Структура интервью с идентифицируемым лицом должна варьироваться, по крайней мере, с точки зрения последовательности и / или типа вопросов, задаваемых сотрудником. Любой подмене / манипулированию частями или элементами документа, удостоверяющего

личность, необходимо противодействовать соответствующими мерами. Для этого нужно попросить человека, которого нужно идентифицировать, например, провести пальцем по важным для безопасности частям удостоверения личности (переменным и произвольно определяемым системой) и провести рукой по лицу. Используя кадры этих перемещений, которые вырезаны и увеличены, сотрудник должен убедиться, что документ, удостоверяющий личность, вместе со всеми элементами безопасности, визуально идентифицируемыми в белом свете, полностью прикрыт в нужной точке и что в нем не обнаружены артефакты, указывающие на манипуляции.

Проверка достоверности и достоверности данных и информации, содержащихся в документе, удостоверяющем личность, должна выполняться в рамках процедуры видео идентификации. Среди прочего, это включает проверку того, совпадают ли дата выдачи и дата истечения срока действия документа, удостоверяющего личность. В частности, дата выпуска не должна быть в будущем. Кроме того, срок действия предъявленного документа, удостоверяющего личность, не должен противоречить нормам, установленным для документов, удостоверяющих личность.

Еще одним необходимым элементом процесса идентификации являются автоматический подсчет контрольных цифр в машиночитаемой зоне и перекрестная проверка предоставленной там информации с информацией, отображаемой в документе, удостоверяющем личность. Кроме того, необходимо проверить орфографию цифр, авторитетный код и используемые гарнитуры, чтобы убедиться в их правильности. Кроме того, идентифицируемое лицо должно указать полный серийный номер своего документа, удостоверяющего личность, во время передачи видео.

Сотрудник должен убедиться, что фотография и личное описание в использованном документе, удостоверяющем личность, соответствуют личности, которую нужно идентифицировать. Фотография, дата выдачи и дата рождения также должны совпадать. Посредством психологического опроса и наблюдений, сделанных во время процедуры идентификации, сотрудник должен убедиться в достоверности информации, содержащейся в документе, удостоверяющем личность, информации, предоставленной лицом, которое будет идентифицировано во время собеседования, а также заявленного намерения этого человека. Также могут быть заданы вопросы, например, относительно возраста человека для подтверждения фотографии документа, удостоверяющего личность, а также даты и места рождения, указанных в документе, удостоверяющем личность. Причина идентификации должна быть подтверждена лицом, которое будет идентифицировано, не в последнюю очередь для того, чтобы это лицо знало, почему такая процедура идентификации необходима. Сотрудники должны быть обучены, чтобы они могли без сомнения определить, что лицо, которое будет идентифицировано, покупает соответствующий продукт у соответствующего поставщика по собственному желанию (риск, связанный с фишингом, социальной инженерией, поведением под давлением со стороны другого человека и т.д.). Сотрудник также должен убедиться, что все данные о человеке, которые должны быть идентифицированы, в документе, удостоверяющем личность, совпадают с теми, которые известны обязанному

юридическому лицу и доступны сотруднику (если применимо).

Если описанная выше визуальная проверка невозможна, например, из-за плохих условий освещения или плохого качества изображения или передачи, и / или если устное общение с лицом, которое будет идентифицировано, невозможно, процесс идентификации должен быть прерван. То же самое применимо в случае любого другого несоответствия или неопределенности.

Весь процесс видео идентификации на всех его отдельных этапах должен быть записан и сохранен обязанным лицом или третьей стороной, которой обязанное лицо делегировало процедуру идентификации или которую обязанное лицо привлекло для целей внутреннего и внешнего аудита и для BaFin. Таким образом, требование к документации требует как визуальной, так и звуковой записи и сохранения всей процедуры, на которую должно быть указано вышеупомянутое согласие, предоставленное лицом, которое будет идентифицировано. Записи должны демонстрировать не только выполнение общих требований к идентификации в соответствии с законом о борьбе с отмыванием денег, но и соблюдение минимальных требований к видео идентификации, изложенных в этом Циркуляре. Записи должны храниться в течение пяти лет в соответствии с разделом 8.

Вышеупомянутые надзорные требования применяются независимо от любых других требований, которые должны соблюдаться в соответствии с разделами 7 и 8, и без ущерба для требований защиты данных, которые должны соблюдаться параллельно.

Проблема обеспечения безопасности клиента банка при работе через дистанционные каналы обслуживания

При появлении ДБО разрешились многие проблемы, но также появились новые, опасные и сложные, которые разрешить не удается уже на протяжении нескольких лет. Например, за 2020 г. через телефонное мошенничество было украдено злоумышленниками около 70 млрд. руб. у граждан, по данным российской секции Международной полицейской ассоциации. Невольным инструментом осуществления данных операций стало дистанционное банковское обслуживание. Мы видим пристальное внимание к банкам со стороны надзорных органов и бессилие по отношению к сотовым операторам, провайдерам ip-телефонии и интернета, которые обслуживают коллцентры в местах тюремного заключения и при этом не подозревают об этом. Тем самым возникает срочная необходимость приравнивания сим-карты по степени идентификации клиента к открытию банковского счета, ведь сотовые операторы тоже являются субъектами 115-ФЗ.

Действительно, социальная инженерия "умеет обходить" регулирование властей, но на инструменты идентификации повлиять все-таки можно. 499-П не обновлялся с 2015 г., в нем не учтены многие цифровые возможности качественной идентификации клиентов, которые появились за все эти 6 лет. Растут цифровые дистанционные возможности для реализации многих банковских услуг, но и неимоверно растут преступления, связанные с интернет-банком. Рассматривая классическую схему мошенничества с использованием Интернет-банка, можно выделить несколько субъектов участия – это клиент Банка, сам Банк, злоумышленник, сотовый оператор.

Сотовый оператор, как и Банк, является субъектом 115-ФЗ. Его

деятельность регулируется 126-ФЗ от 7 июля 2003 г. в лице Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, однако, отдельных положений, регулирующих порядок должной идентификации своих клиентов, нет. На данный момент практически основным способом подтверждения в ДБО является номер телефонного оператора. Отсюда возникает вопрос, почему регулирование не уделяет должного внимания на все субъекты данного взаимодействия, а не только – банки? Возможно, государству невыгодно производить изменения в законодательстве в части ужесточения порядка работы сотовых операторов со своими клиентами, поскольку все в дальнейшем отразится в ценах предоставления услуг связи для клиентов из-за технологической модернизации. Либо государство ждёт повсеместного развития нового вида идентификации в виде предоставления биометрических данных.

В рамках мер предотвращения случаев телефонного мошенничества предпринято несколько попыток, например, выявление подставных телефонов посредством передачи банком контакта сотовому оператору, от которого поступают мошеннические звонки; продвижение инициативы по созданию общей базы. Но данная мера не нашла поддержки со стороны сотовых операторов, поскольку, по их мнению, это идёт вразрез с принципами закона о связи, а также данная мера подразумевает значительные затраты, которые приведут к удорожанию услуг связи для клиентов.

В данный момент, банки ведут одиночную войну с мошенниками интернет-банков, разрабатывают внутренние положения, ведут просветительские кампании среди населения, производят технические модернизации, создают полномочные группы внутри банковских подразделений и т.п., но все это благодаря отдельным положениям, которые были введены, к сожалению, только для кредитных организаций.

ЗАКЛЮЧЕНИЕ

ДБО усовершенствовало предоставление финансовых услуг для своих клиентов. Оно позволяет быстро и оперативно совершать банковские операции, не посещая банк физически. Но в связи с этим не отпадает необходимость идентификации клиента для безопасности проведения банковских операций. Идентификации бывают разных типов, утвержденные компетентным регулирующим органом. В России существует специальное Положение (499-П) для кредитных организаций, изданное ЦБ РФ, регламентирующее порядок идентификации своего клиента. В настоящий момент основным методом идентификации при совершении повторной банковской операции удаленно является аутентификация через номер мобильного телефона. Данный метод очень удобен, поскольку не требует дорогой техники, достаточно местности, где есть покрытие сотовой связи у оператора, а также у него обширный перечень услуг, который возможно реализовать через такую идентификацию.

За период существования мобильного банка, ее влияние и распространенность возросла, вместе с этим выросли и риски для банка и его клиентов. Кибермошенничество затмило все виды мошенничества по частоте и объему украденных средств в мире и, в частности, в России. Международные сообщества, такие как FATF, очень чутко реагируют на новые вызовы, связанные с данным явлением, выпуская рекомендации, постоянно обновляя их в

соответствии с глобальной и локальной обстановкой в странах.

Рассматривая нормативно-правовую базу, регулирующую банковскую деятельность, а также специфику взаимодействия субъектов, причастные к безопасному проведению ДБО, отмечается следующий вывод. Поскольку сотовые операторы - это уже непросто поставщики телекоммуникационной связи, но и полноценные субъекты 115-ФЗ (также в нашей стране основным идентификатором при ДБО является номер сотового телефона), предлагается сформировать Положение, которое будет регламентировать порядок идентификации своих будущих и настоящих клиентов по аналогии с 499-П ЦБ РФ для кредитных организаций. Необходимо произвести унификацию требований и регулирования при идентификации клиента банками и сотовыми операторами на законодательном уровне. В настоящее время, если сотовые операторы не узнают «всех» своих клиентов, банки не смогут в должной мере осуществлять ДБО, поскольку существует данного рода риск его использования для населения, отсюда меньшее доверие к банковской системе в целом. Пока банковская система зависит от операторов сотовой связи при удаленной идентификации клиента. Она относительно недавно начала создавать свою собственную платформу для идентификации (например, биометрия) клиентов.

PROBLEMS OF PROVIDING SECURITY MEASURES FOR REMOTE BANKING SERVICES (RBS)

Vladimir Senin - Candidate of Law, Professor of the Department of Theory and Practice of Interaction between Business and Government of the Higher School of Economics, Deputy Chairman of the Management Board of Alfa-Bank JSC.

Pavel Sobolev - sobolev_1995@icloud.com

Recently, against the background of rapid technological growth, more and more advanced solutions for customer interaction have been created for banks. Almost all banks are trying to divert their services to remote channels. This allows banks to increase their customer base, reduce costs, increase the speed of processing transactions, increase the competitiveness of the bank, allow customers to perform their operations independently, without visiting the bank's office, etc.

Keywords:
Technological growth, banks, remote banking, competitiveness