НАЦИОНАЛЬНЫЙ БАНК

ПОСТАНОВЛЕНИЕ № 281
от 07-11-2024

об утверждении Регламента о требованиях к идентификации и проверке личности клиентов посредством электронных средств

Опубликован : 14-11-2024 в Monitorul Oficial № 467-469 статья № 886

На основании части (3) ст. 5[1] Закона о предупреждении и борьбе с отмыванием денег и финансированием терроризма № 308/2017 (Официальный монитор Республики Молдова, 2018, № 58-66, ст. 133), с последующими изменениями, Исполнительный комитет Национального банка Молдовы ПОСТАНОВЛЯЕТ:

1. Утвердить Регламент о требованиях к идентификации и проверке личности клиентов посредством электронных средств согласно приложению.

2. Настоящее постановление вступает в силу со дня его опубликования в Официальном мониторе Республики Молдова. Отчетные единицы, внедрившие информационные решения для установления дистанционных деловых отношений клиентов на день вступления в силу настоящего постановления, будут соответствовать новым требованиям в течение 6 месяцев.

ПРЕДСЕДАТЕЛЬ
ИСПОЛНИТЕЛЬНОГО КОМИТЕТА **Анка-Дана ДРАГУ**

№ 281. Кишинэу, 7 ноября 2024 г.

Приложение
к Постановлению Исполнительного комитета
Национального банка Молдовы
№ 281 от 7 ноября 2024 г.

Регламент
о требованиях к идентификации и проверке
личности клиентов посредством электронных средств

Глава I. Общие положения

1. Настоящий Регламент о требованиях к идентификации и проверке личности клиентов посредством электронных средств (далее – *Регламент*) направлен на установление требований в отношении необходимых политик и процедур, системы внутреннего контроля, рисков и мер защиты, а также в качестве минимальных технических требований в целях идентификации клиентов и проверки их личности отчетными единицами, указанными в п. 3, при установлении деловых отношений с клиентами без физического присутствия.

2. Требования и правила, касающиеся идентификации и проверки личности клиентов с физическим присутствием, применяются также к клиентам, дистанционная идентификация которых осуществляется в соответствии с требованиями настоящего Регламента, а меры по предупреждению и борьбе с отмыванием денег и финансированием терроризма будут применяться в соответствии с требованиями Закона о предупреждении и борьбе с отмыванием денег и финансированием терроризма № 308/2017(далее – *Закон № 308/2017*) и нормативных актов, изданных для его реализации.

3. Под действие положений настоящего Регламента подпадают отчетные единицы, предусмотренные в п. a), e), g) и i) части (1) ст. 4 Закона № 308/2017.

4. Термины и выражения, используемые в настоящем Регламенте, имеют значения, установленные Законом № 308/2017, Законом об электронной идентификации и доверительных услугах № 124/2022 (далее – *Закон № 124/2022*) и нормативными актами, изданными для их реализации. Также для целей настоящего Регламента используются следующие термины и выражения:

биометрические данные — персональные данные, полученные в результате особых методов обработки, касающиеся физических, физиологических или поведенческих характеристик физического лица, которые позволяют или подтверждают уникальную идентификацию этого лица, например изображения лица или дактилоскопические данные;

идентификация и проверка личности клиентов посредством электронных средств - процесс идентификации и проверки личности клиента дистанционно на основе соответствующей оценки риска и с использованием, в зависимости от риска, одновременно одного или нескольких методов, предусмотренных частью (2) ст. 51 Закона № 308/2017;

информационное решение для установления дистанционных деловых отношений (информационное решение) – совокупность технологических элементов, задействованных в процессе идентификации лица на расстоянии электронными средствами, посредством которых передаются данные, захваченные/загруженные изображения и/или информация, сообщаемая заявителем;

электронные средства - средства, которые используют инновационные цифровые технологии, в которых используются, среди прочего, процессы искусственного интеллекта и/или машинного обучения (machine learning), такие как приложения, которые осуществляют идентификацию лица и/или проверку документов, удостоверяющих личность (например, посредством захвата цифровых изображений), измерение биометрических сигналов лица, сравнение изображений), технологию NFC (Near Field Communication), встроенную в электронные документы, удостоверяющие личность.

Глава II. Политика и процедуры, касающиеся идентификации и проверки личности клиентов посредством электронных средств

Часть 1

Политики и процедуры

5. Отчетная единица разработает политику и процедуры дистанционной идентификации для выполнения своих обязательств в соответствии с п. a) части (2) ст. 5 Закона № 308/2017, в ситуациях, когда идентификация клиента осуществляется дистанционно. Эти политики и процедуры должны быть установлены в соответствии с выявленными рисками отмывания денег и финансирования терроризма и включать как минимум следующее:

a) общее описание информационного решения, которое использует для сбора, хранения, противодействия, проверки, подтверждения и обновления информации на протяжении всего процесса установления деловых отношений с удаленными клиентами. Это должно включать объяснение элементов и того, как работает информационное решение;

b) ситуации, в которых может быть использовано информационное решение, с учетом факторов риска, выявленных и оцененных в соответствии с частью (1) ст. 6 Закона № 308/2017, в рамках оценки рисков в собственной сфере деятельности, включая описание категории клиентов, продуктов и услуг, подлежащих дистанционной идентификации;

c) этапы, полностью автоматизированные, и этапы, требующие вмешательства человека;

d) проверки, установленные для обеспечения того, чтобы первая сделка с вновь зарегистрированным клиентом, который был идентифицирован дистанционно, выполнялась только после применения всех мер предосторожности в отношении клиентов, предусмотренных Законом № 308/2017;

e) описание вводных и периодических программ обучения для обеспечения осведомленности персонала, обучения и непрерывного информирования, а также понимания работы информационного решения и связанных с ним рисков;

f) требования по сохранению данных и информации, накопленных в процессе идентификации и проверки личности лица электронными средствами.

Часть 2
Предварительное внедрение информационного решения

6. Отчетная единица при анализе внедрения информационного решения по дистанционной идентификации клиентов проведет предварительную оценку этого решения. Таким образом, отчетная единица установит область применения, этапы и требования, которым необходимо следовать, в том числе в отношении записей данных, которые должны включать:

a) оценку адекватности и безопасности информационного решения с точки зрения: доступности, полноты, точности и неотказуемости данных и документов, подлежащих обработке, а также надежности, достоверности и независимости используемых источников информации;

b) оценку влияния использования информационного решения на конкретные риски субъекта, включая отмывание денег и финансирование терроризма, операционные, репутационные и юридические риски, включая оценку влияния на защиту персональных данных согласно условиям Закона о защите персональных данных № 133/2011;

c) определение возможных мер по смягчению последствий и корректирующих действий для каждого выявленного риска;

d) определение способности информационного решения снизить риск использования виртуальных частных сетей (VPN) или прокси-серверов для сокрытия местоположения или предотвращения применения требований мониторинга;

e) оценку соответствия информационного решения требованиям к проведению процедуры дистанционной идентификации лица с использованием электронных средств, установленных для квалифицированного поставщика доверительных услуг, установленных в соответствии с положениями Закон а№ 124/2022 и подзаконными нормативными актами;

f) оценку соответствия информационного решения требованиям проведения процедуры дистанционной идентификации лица с использованием электронных средств, установленных международными техническими стандартами[1];

g) тесты для оценки рисков мошенничества, включая риски мошенничества посредством кражи личных данных или выдачи себя за другое лицо;

h) оценку рисков, связанных с информационно-коммуникационными технологиями (ИКТ) и информационной безопасностью;

[1] Принять во внимание положения п. 29 Регламента.

i) сквозное тестирование работы информационного решения, направленное на клиентов, продукты и услуги, для которых оно применимо.

7. Отчетная единица в соответствии с положениями п. 49 представляет в НБМ подтверждающие документы/документацию, относящиеся к оценкам и тестам, указанным в п. 6, их результаты, а также то, как применение информационного решения обеспечивает смягчение и устранение рисков отмывания денег и финансирования терроризма, а также других рисков, определенных для типов клиентов, услуг и продуктов, к которым оно применимо. Оценки и тесты, упомянутые в пункте 6, могут быть проведены/подтверждены независимым аудитом или международно признанными сертификатами, если отчетная единица не имеет необходимых ресурсов в этом отношении.

Часть 3

Постоянный мониторинг информационного решения

8. Отчетная единица должна контролировать информационное решение на постоянной основе, чтобы гарантировать, что оно функционирует в соответствии со своим назначением. В этом контексте отчетная единица включит в политику и процедуры дистанционной идентификации, разработанные в соответствии с п. 5, как минимум следующее:

a) шаги, которые предпримет отчетная единица для обеспечения качества, полноты, точности, адекватности и безопасности данных, собранных в ходе процесса дистанционной идентификации клиентов, и которые должны быть пропорциональны рискам отмывания денег и финансирования терроризма, которым она подвергается;

b) цель и частота периодических пересмотров информационного решения; и

c) основания для инициирования и проведения специальной проверки информационного решения, которая должна включать как минимум:

- изменения в подверженности предприятия риску отмывания денег и финансирования терроризма;
- недостатки в работе информационного решения, обнаруженные в ходе мероприятий по мониторингу, аудиту или надзору;
- предполагаемое увеличение количества попыток мошенничества с личными данными клиентов, включая кражу личных данных или выдачу себя за другое лицо, выявленное отчетной единицей;
- изменения в нормативной базе, касающейся процесса дистанционной идентификации клиентов.

9. Отчетная единица должна обеспечить наличие механизмов мониторинга, основанных на оценке рисков, которые учитывают, как минимум, следующие факторы:

a) списки скомпрометированных или украденных элементов идентификации;

b) известные сценарии мошенничества при установлении удаленных деловых отношений;

c) индикаторы нарушения конфиденциальности, целостности или аутентичности сеанса в результате процедуры идентификации;

d) реестр случаев регулярного или противоправного использования устройства доступа или информационного решения, предоставленного лицу, которое должно быть идентифицировано отчетной единицей;

e) аномальное/необычное географическое положение (местоположение) лица;

f) рискованное географическое положение (юрисдикция) лица;

g) случаи кражи, выдачи себя за другое лицо или незаконной обработки идентифицированных данных.

10. Отчетная единица установит в политике и процедурах удаленной идентификации, разработанных в соответствии с п. 5, меры по исправлению ситуации в случае выявления ошибок, влияющих на эффективность информационного решения. Эти меры будут включать как минимум:

a) проверку всех затронутых деловых отношений, чтобы оценить, правильно ли отчетная единица применила меры предосторожности в отношении клиентов, при этом приоритет отдается клиентам с повышенным риском отмывания денег и финансирования терроризма;

b) оценку на основе информации, полученной в рамках проверки п. a), определяющую, должны ли затронутые деловые отношения:

- переклассифицированы в другую категорию риска и подвергнуты повышенным мерам предосторожности;
- подвергнуты установлению лимитов по объему сделок;
- прекращены;
- сообщены в Службу по предупреждению и борьбе с отмыванием денег при выявлении подозрений в отмывании денег и/или финансировании терроризма.

11. Отчетная единица рассмотрит наиболее эффективный способ мониторинга постоянной пригодности и надежности информационного решения. С этой целью она рассмотрит одно или несколько из следующих средств, но не ограничиваясь ими:

- проверка качества;
- автоматические критические оповещения и уведомления;
- регулярные автоматические отчеты;
- выборочное тестирование;
- тесты на проникновение;
- обзоры или признанные экспертные отчеты экспертов в данной области и/или надзорных органов на национальном или международном уровне, в том числе в юрисдикциях, которые реализуют аналогичные стандарты по предупреждению отмывания денег и финансирования терроризма.

Глава III. Требования к идентификации и проверке личности клиентов посредством электронных средств

12. Отчетная единица осуществляет идентификацию и проверку личности клиента электронными средствами в отношении потенциальных

новых клиентов, с которыми отчетная единица намерена инициировать деловые отношения.

13. Отчетная единица будет идентифицировать и проверять личность клиентов с помощью электронных средств в отношении:

a) физического лица, гражданина Республики Молдова;

b) юридического лица-резидента, представители, учредители, управляющие и выгодоприобретающие собственники которого являются гражданами Республики Молдова.

14. Отчетная единица обеспечит наличие в информационно решении элементов, которые позволяют ей собирать информацию, необходимую для знакомства с клиентами, в соответствии с требованиями политики и процедур дистанционной идентификации, разработанными отчетной единицей в соответствии с п. 5, в частности, она может собирать:

a) все соответствующие данные и документы для идентификации и проверки личности физического и/или юридического лица;

b) все соответствующие данные и документы для проверки того, имеет ли физическое лицо, действующее от имени юридического лица, законное право действовать таким образом;

c) все соответствующие данные и документы для идентификации и проверки личности выгодоприобретающего собственника;

d) все соответствующие данные и документы для определения цели и желаемого характера деловых отношений.

15. Отчетная единица должна обеспечить, чтобы независимо от метода, применяемого для дистанционной идентификации и проверки личности клиентов, был обеспечен сбор и представление клиентом информации, обычно требуемой от идентифицированных клиентов с физическим присутствием. Метод сбора информации будет определяться отчетной единицей, но она будет определять, какая информация будет собираться:

a) вручную, введенная клиентом или сотрудником организации;

b) автоматически из документов, предоставленных клиентом;

c) из других внутренних или внешних источников, собранных автоматически или сотрудником предприятия.

16. Отчетная единица должна внедрить и поддерживать механизмы, обеспечивающие полноту информации, которую она собирает в электронном виде. Она должна применять меры контроля (по крайней мере ежегодно) к процессу установления удаленных деловых отношений для устранения рисков, связанных с этим процессом, включая сокрытие местоположения адресов Интернет-протокола (IP), использование таких услуг, как виртуальные частные сети (VPN) или прокси.

17. В случае клиента-юридического лица меры идентификации применяются к физическому лицу с мандатом его представлять, и будут получены соответствующие регистрационные документы юридического лица. В этих случаях к физическому лицу, представителю юридического лица, отчетная единица применит процедуру установления дистанционных деловых отношений, аналогичную процессу установления дистанционных

деловых между клиентом и физическим лицом. В этом же контексте будут применяться меры по обеспечению проверки наличия у физического лица, действующего от имени юридического лица, законного права действовать таким образом.

18. Идентификация и проверка личности клиентов электронными средствами осуществляется с помощью автоматизированных средств проверки без участия человека-оператора либо путем проверки с участием человека-оператора (работника субъекта). Отчетная единица также может использовать информационное решение для комбинированной проверки личности лица при дистанционной идентификации клиента.

19. Идентификации клиента с использованием электронных средств предшествует выражение согласия на обработку персональных данных в соответствии с действующим законодательством.

20. При идентификации и проверке личности клиентов с помощью электронных средств отчетная единица обеспечивает информирование клиента об условиях, на которых осуществляется электронная идентификация. Условия, предоставленные клиенту, включая и до тех пор, пока клиент не получит доступ к информационному решению, будут содержать, помимо прочего:

a) «Условия использования» (электронной страницы, информационного решения, используемой платформы и т.п.) должны содержать общие условия доступа к ИТ-решению, используемому для идентификации клиента электронными средствами;

b) «Информационная записка о способе обработки и защиты данных» будет содержать информацию, которая относится к праву клиента на получение информации как физического лица или представителя юридического лица и в целом к обеспечиваемым организационным и техническим мерам, в том числе информацию, которая будет обработана в соответствии с требованиями применимых нормативных актов;

c) «Политика предупреждения отмывания денег» будет содержать краткую версию политики по идентификации клиентов, предупреждению отмывания денег, финансированию терроризма и идентификации политически уязвимых лиц.

Глава IV. Методы идентификации и проверки личности клиентов посредством электронных средств

21. В случае идентификации и проверки личности клиентов электронными средствами отчетная единица, в зависимости от степени риска отмывания денег и финансирования терроризма или других связанных с этим рисков, использует один или несколько из следующих методов дистанционной идентификации через:

a) средства электронной идентификации с достаточным уровнем безопасности и в соответствии со стандартами, установленными Законом № 124/2022 (квалифицированная электронная подпись);

b) электронные средства, совокупно обеспечивающие прямую трансляцию видео- и аудиозаписи с элементами проверки физического

присутствия и регистрацию оригинала документа, удостоверяющего личность, во время прямой трансляции и захват изображения лица клиента;

c) электронные средства, в совокупности обеспечивающие прямую трансляцию фотографии с элементами проверки физического присутствия и регистрацию оригинала документа, удостоверяющего личность;

d) другие электронные средства, предлагаемые квалифицированным надежным поставщиком услуг, аккредитованным в соответствии с Законом № 124/2022.

22. При идентификации и проверке личности клиентов с использованием средств видео/фотоидентификации клиента, с использованием средств проверки с участием человека-оператора отчетная единица обеспечивает запись процесса идентификации и соответствует следующему:

a) имеет разумную продолжительность (установленную в соответствии с нормативными актами единицы) и содержит, как минимум, следующую соответствующую информацию/данные:

- время, день, год регистрации;

- точный момент предъявления физическим лицом, подлежащим видеопроверке, своих идентификационных данных из документа, удостоверяющего личность (имя и фамилия, удостоверение личности, дата/месяц/год рождения, домашний адрес и/или место жительства), а также время/дата/месяц/год регистрации и контактный номер мобильного телефона;

- момент, когда сотрудник отчетной единицы связывается с лицом во время видео верификации и/или момент, когда клиент получает или вводит уникальный код или получает доступ к ссылке, отправленной через службу коротких сообщений (SMS) на мобильный телефон или электронную почту;

- момент, когда клиент подносит удостоверение личности ближе к камере и показывает его с обеих сторон;

b) соответствует следующим условиям:

- процесс идентификации проводится в тихом, хорошо освещенном месте и без участия третьих лиц в процессе, чтобы обеспечить четкую идентификацию лица, в противном случае процесс должен быть прерван;

- процесс видео/фото верификации осуществляется в режиме реального времени и без перерывов в непрерывном потоке. Если процесс проверки был прерван, независимо от причины прерывания, его необходимо перезапустить с начала;

- процесс идентификации обеспечивает свободное и четкое обсуждение между сотрудником отчетной единицы и клиентом, а также визуальную проверку сотрудником отчетной единицы документов, представленных клиентом, включая элементы защиты, применимые к этому документу;

- процесс идентификации обеспечивает использование оригиналов документов, удостоверяющих личность, а не предъявление на основе воспроизведения оригинального документа, такого как фотография, копия, скан документа и т.д.;

- процесс идентификации обеспечивает высокое качество изображения и звука при передаче видео, с разрешением не менее 8 мегапикселей или не менее FullHD (1920x1080), с целью безусловной идентификации и распознавания лица;

- процесс идентификации гарантирует, что передача видео в реальном времени записывается в цвете и происходит синхронно со звуком;

- процесс идентификации обеспечивает автоматический захват лица клиента и документа, удостоверяющего личность;

- процесс идентификации гарантирует, что информационное решение не позволяет загружать фотографии/видео, снятые ранее во время собеседования или идентификации по фотографии;

- процесс идентификации обеспечивает использование соответствующих технологий, обеспечивающих целостность и безопасность видео/фотозаписей, используемых при проверке личности.

23. При идентификации и проверке личности клиентов с использованием электронных средств видео/фотоидентификации клиента с использованием средств проверки без участия человека-оператора, при отсутствии взаимодействия клиента с сотрудником, отчетная единица обеспечивает запись процесса, который соответствует следующему:

a) имеет разумную продолжительность (установленную в соответствии с нормативными актами единицы) и содержит, как минимум, следующую соответствующую информацию/данные:

- время, день, год регистрации;

- точный момент предъявления физическим лицом, подлежащим видеопроверке, своих идентификационных данных из документа, удостоверяющего личность (имя и фамилия, удостоверение личности, дата/месяц/год рождения, домашний адрес и/или место жительства), а также время/дата/месяц/год регистрации и контактный номер мобильного телефона;

- момент предъявления клиентом документа, удостоверяющего личность, и это фиксируется камерой с обеих сторон;

b) соответствует следующим условиям:

- фотография (фотографии) или видеозапись сделана (сделаны) в соответствующих условиях освещения и что необходимые свойства запечатлены с необходимой четкостью, чтобы обеспечить надлежащую проверку личности клиента;

- информационное решение использует проверки обнаружения движения клиента, которые могут включать в себя процедуры, требующие от клиента определенных действий для проверки его присутствия на сеансе связи, или которые могут быть основаны на анализе полученных данных и не требовать определенного действия со стороны клиента;

- информационное решение использует технологии, использующие алгоритмы для проверки подлинности представленного документа, удостоверяющего личность, такие как проверка дизайна и элементов защиты документов, удостоверяющих личность, сопоставление данных, введенных в представленный документ, с данными, содержащимися в зонах оптического считывания (MRZ), оценка подлинности на основе цветового профиля

представленных документов, использование биометрических алгоритмов для оценки возраста и пола человека для его сверки с информацией, представленной в документе и т.д.;

- информационное решение, используемое для дистанционной идентификации, использует алгоритмы, определяющие, что используемые документы, удостоверяющие личность, являются оригинальными и не представлены на основании воспроизведения оригинального документа, такого как фотография, копия, скан документа и т. д.;

- качество изображения и звука при передаче видео должно быть высокое, с разрешением не менее 8 мегапикселей или не ниже FullHD (1920x1080), с целью безусловной идентификации и распознавания лица;

- информационное решение использует надежные алгоритмы, способные проверить, соответствуют ли сделанные фотография (фотографии) или видеозапись (видеозаписи) фотографии (фотографий), извлеченным из официального документа (документов) клиента, или фотографиям, полученным из безопасных и независимых источников;

- информационное решение не позволяет загружать фото/видео, снятые ранее во время собеседования или фото идентификации;

- информационное решение использует технологии, обеспечивающие целостность и безопасность видео/фотозаписей, используемых при проверке личности;

c) использует электронные средства.

24. В случае установления дистанционных деловых отношений электронными средствами отчетная единица осуществляет идентификацию, проверку и сохранение технических данных компьютера/устройства, используемого клиентом (например, модели, наименования, параметры оборудования, пользовательский агент, файлы cookie, установленные шрифты, часовой пояс, языковые настройки, размеры экрана, данные о сетевых подключениях), IP-адрес, его местоположение, а также другие доступные и возможно собранные данные.

25. В процессе установления дистанционных деловых отношений с использованием электронных средств отчетная единица проверит номер телефона и/или адрес электронной почты, которые будут использоваться для дальнейшего общения с клиентом, отправив лицу, проходящему дистанционную идентификацию, одноразовый код (One Time Password – OTP) или путем отправки ссылки с ограниченным сроком действия, специально созданной для этой цели, сгенерированной индивидуально (по электронной почте или SMS).

26. Процедура установления деловых отношений на расстоянии с использованием электронных средств может быть завершена только в случае завершения передачи и проверки OTP или только в случае завершения передачи и доступа по ссылке.

27. В рамках установления дистанционных деловых отношений с помощью электронных средств отчетная единица проверяет документы, удостоверяющие личность клиента, по следующим аспектам:

a) выявление порчи или подделки документа, в частности путем нанесения (наклеивания) поддельной фотографии поверх оригинала, соответствия формы, защитных элементов (например, голограмм, оптически изменяющихся элементов, специальных шрифтов и т.п.), символов и промежутки между ними с соблюдением стандартов, применимых к типу предъявляемого документа, удостоверяющего личность, наклон документа по горизонтали и вертикали;

b) проверка соответствия внешности клиента фотографии в документе, удостоверяющем личность;

c) проверка действительности документа, удостоверяющего личность;

d) подтверждение наличия и соответствия элементов защиты, которые должны присутствовать в документе, удостоверяющем личность, предъявляемом заказчиком, стандартам, применимым к соответствующему виду документов;

e) в случае возникновения подозрений относительно личности лица или подлинности представленных документов будут заданы дополнительные вопросы с целью проверки личности лица или подлинности документов либо будет проведена ручная проверка сведений сотрудником;

f) сравнение данных предъявленных документов, удостоверяющих личность, с данными Государственного регистра населения.

28. В целях проверки и подтверждения данных/информации, полученных от клиента в процессе видео верификации, отчетная единица:

a) обязана проверить клиента на предмет:

- участия в террористической деятельности или распространении оружия массового поражения;

- применения международных санкций;

- применения финансовых санкций Европейского союза;

- наличия качества политически уязвимого лица или других факторов повышенного риска;

- наличия информации, которая может повлиять на репутацию клиента путем доступа к заслуживающим доверия источникам информации и/или доступным, общедоступным базам данных и/или интернету, в том числе принадлежащим другим государственным учреждениям и организациям;

b) обязана требовать физического присутствия лица в его офисе в случае возникновения подозрений и/или сомнений в отношении дефекта согласия (физического или психологического давления или влияния) клиента со стороны третьих лиц или любых других подозрений в отношении клиента;

c) вправе требовать использования электронной подписи на копии документа, удостоверяющего личность, в качестве дополнительной меры по сравнению с видео идентификацией, в случае сомнений в достоверности предоставленной клиентом информации;

d) обязана проверять данные/информацию, полученные посредством электронной связи, в соответствии с правилами в сфере предупреждения и борьбы с отмыванием денег и финансированием терроризма.

29. Отчетная единица для установления дистанционных деловых отношений с использованием электронных средств будет использовать информационные решения, сертифицированные по действующим международным стандартам[2].

[2]
1. ISO/IEC 30107: Information technology - Biometric presentation attack detection;
2. ISO/IEC 24745: Information technology – Security techniques – Biometric information protection;
3. ISO/IEC 27034: Information technology – Security techniques – Application security;
4. ISO/IEC 15408: Information security, cybersecurity and privacy protection;
5. NIST SP 800-63: Digital Identity Guidelines;
6. NIST SP 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management.

30. Отчетная единица может использовать информационное решение для дистанционных деловых отношений с помощью электронных средств для обновления существующей информации/данных о клиентах.

31. Отчетная единица не будет инициировать деловые отношения с клиентом с помощью электронных средств, если она не может применить стандартные меры предосторожности в отношении клиентов, предусмотренные Законом № 308/2017, а также в ситуации, когда технические требования не выполняются или организация не может подтвердить личность лица в соответствии с требованиями настоящего регламента.

Глава V. Требования к системе внутреннего контроля

32. В случае установления дистанционных деловых отношений с использованием электронных средств видео/фото идентификации клиента с использованием средств верификации с человеком-оператором субъект реализует, как минимум, следующие требования:

a) для сотрудника отчетной единицы, ответственного за идентификацию клиентов электронными средствами:

- имеет достаточный уровень профессиональной квалификации в области идентификации клиентов;
- имеет опыт применения мер предосторожности к клиентам не менее 1 года;
- имеет специальную подготовку по идентификации клиентов электронными средствами;
- имеет достаточные знания правил, применимых к предупреждению и борьбе с отмыванием денег и финансированием терроризма;
- имеет достаточные знания об аспектах безопасности дистанционной проверки и достаточно обучен, чтобы предвидеть и предотвращать преднамеренное или предумышленное использование мошеннических методов, связанных с удаленной проверкой, а также обнаруживать и реагировать в случае их возникновения.

b) в отношении специального помещения, созданного для идентификации клиентов электронными средствами:

- находится под постоянным контролем и видеонаблюдением в процессе установления взаимоотношений на расстоянии с использованием электронных средств с клиентами;

- обеспечивает отсутствие других лиц и/или предметов перед видеокамерой, а также отсутствие любых шумов, которые могут ухудшить качество записи и информации.

33. Руководитель высшего звена должен обеспечить, чтобы политика и процедуры установления дистанционных деловых отношений с клиентами, разработанные организацией в соответствии с п. 5, эффективно реализовывались, периодически пересматривались и при необходимости корректировались.

34. В зависимости от риска отмывания денег или финансирования терроризма, связанного с деловыми отношениями, или других связанных с этим рисков, отчетная единица будет использовать один или несколько из следующих средств контроля в ситуациях высокого риска:

a) обеспечение осуществления клиентом операции с платежного счета, открытого в другой отчетной единице, в том числе с использованием платежного инструмента;

b) обеспечение того, чтобы клиент осуществил сделку с платежного счета, открытого в финансовом учреждении за рубежом, из юрисдикции, где существуют требования по борьбе с отмыванием денег или финансированием терроризма, как минимум аналогичные тем, которые действуют в Республике Молдова;

c) сбор биометрических данных для сравнения их с данными, полученными из других независимых и безопасных источников;

d) связь с клиентом по телефону;

e) прямая переписка (как электронная, так и почтовая) с клиентом.

35. Если отчетная единица использует элементы для автоматического считывания информации из документов, такие как алгоритмы оптического распознавания символов (OCR) или проверки зоны оптического считывания (MRZ), она должна предпринять необходимые шаги для обеспечения того, чтобы эти инструменты фиксировали информацию точным и последовательным образом, обеспечивали сохранение целостности алгоритма, используемого для генерации уникального идентификационного номера исходного документа.

36. Отчетная единица обязана незамедлительно информировать в соответствии с требованиями Закона № 308/2017 после выявления действия или обстоятельств, вызывающих подозрения, Службу по предупреждению и борьбе с отмыванием денег о клиентах, подозреваемых в причастности к подозрительным операциям и действиям или сделкам по отмыванию денег, сопутствующим преступлениям и/или финансированию терроризма, которые готовятся, предпринимаются, осуществляются или уже осуществлены.

Глава VI. Риски и меры защиты

37. В случае электронной идентификации клиента применяется риск-ориентированный подход, установленный:

a) Законом о предупреждении и борьбе с отмыванием денег и финансированием терроризма № 308/2017;

b) нормативными актами НБМ в сфере предупреждения и борьбы с отмыванием денег и финансированием терроризма;

c) нормативными актами Службы по предупреждению и борьбе с отмыванием денег в сфере предупреждения и борьбы с отмыванием денег и финансированием терроризма;

d) настоящим регламентом;

e) дополнительными повышенными мерами предосторожности, установленными в документах отчетной единицы.

38. При идентификации с помощью электронных средств отчетная единица применяет повышенные меры предосторожности, помимо предусмотренных частью (3) статьи 8 Закона № 308/2017, в следующих случаях:

a) лицо представляет бывшего клиента, деловые отношения с которым были прекращены из-за невозможности применения мер предосторожности в соответствии с частью (3) ст. 5 Закона № 308/2017;

b) лицо является резидентом, в том числе временно, юрисдикции повышенного риска;

c) является лицом, управляющим активами, находящимися в доверительном управлении (траст, инвестиционный фонд и т. д.).

39. В зависимости от риска отчетная единица может использовать один или несколько методов, предусмотренных п. 21, для управления и снижения рисков отмывания денег и финансирования терроризма, в том числе для получения дополнительной информации от клиента. В таких ситуациях используемые дополнительно методы рассматриваются не как метод удаленной идентификации клиента, а как мера, применяемая субъектом для эффективного управления рисками отмывания денег или финансирования терроризма.

40. Отчетная единица должна выявлять и адекватно управлять рисками, связанными с информационно-коммуникационными технологиями и безопасностью, связанными с использованием процесса удаленной идентификации клиентов, в том числе в случаях, когда она обращается к третьим лицам или когда услуга передается на аутсорсинг.

41. Отчетная единица использует защищенные каналы связи для взаимодействия с клиентом в процессе удаленной идентификации и обмена связанной с ним информацией. Информационное решение для удаленной идентификации клиентов должно использовать безопасные протоколы и криптографические алгоритмы в соответствии с лучшими отраслевыми практиками для обеспечения конфиденциальности, аутентичности, целостности и доступности обмениваемых данных, по необходимости.

42. Отчетная единица предоставит клиенту информацию о применимых мерах безопасности, которые необходимо принять, чтобы гарантировать безопасное использование информационного решения.

43. Отчетная единица при установлении деловых отношений посредством других методов удаленной идентификации лица с использованием цифровых средств, принятых в соответствии с условиями Закона № 124/2022, установленного и регулируемого Правительством, оценит, в какой степени они соблюдают положения настоящего Регламента и применять необходимые меры для снижения соответствующих рисков, возникающих в результате их использования. Отчетная единица должна, в

частности, рассмотреть вопрос о том, устранены ли, по крайней мере, следующие риски:

a) риск мошенничества посредством выдачи себя за другое лицо, в том числе путем изменения внешнего вида заявителя физическими и/или электронными средствами;

b) риск того, что личность клиента не будет заявленной или не будет соответствовать той, что указана в Регистре народонаселения;

c) риск подделки и фальсификации документов, удостоверяющих личность, физическими или электронными средствами;

d) риск потери, кражи, приостановления, отзыва или истечения срока действия документов, удостоверяющих личность, включая, в зависимости от обстоятельств, инструменты для обнаружения и предотвращения использования мошенничества с личными данными;

e) риск утечки персональных данных.

Глава VII. Обработка и хранение данных

44. При обработке персональных данных отчетная единица обязана соблюдать режим конфиденциальности данных, принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа, от уничтожения, изменения, блокирования, копирования, незаконного или несанкционированного распространения, а также от других неправомерных действий.

45. В целях электронной идентификации клиента отчетная единица осуществляет обработку данных, а также обеспечивает защиту персональных данных, полученных в процессе реализации положений и требований настоящего регламента, а также конфиденциальность этих данных, в соответствии с нормативными актами о защите персональных данных и настоящим регламентом.

46. Отчетная единица хранит все документы и информацию, полученные от клиентов, такие как видеозаписи, аудиозаписи, фотографии, снимки экрана, включая копии документов, удостоверяющих личность, электронные отпечатки пальцев, относящиеся к используемому компьютеру/устройству, IP-адрес, другие документы или информацию, полученные в ходе активного периода деловых отношений и в течение 5 лет после их прекращения.

47. Отчетная единица обеспечивает, чтобы в случае запроса документы и информация, касающиеся идентификации и проверки клиентов, выгодоприобретающих собственников, мониторинга операций клиентов, в том числе подтверждающие документы, связанные с операциями, доступны Национальному банку Молдовы, Службе по предупреждению и борьбе с отмыванием денег и правоохранительным органам.

Глава VIII. Ответственность

48. Применяя настоящий Регламент, отчетная единица информирует Национальный банк Молдовы о подозрительной деятельности и случаях мошенничества, которые создают риски для безопасности, надлежащего функционирования или репутации отчетной единицы.

49. Отчетная единица не позднее чем за 30 дней до начала процедуры идентификации клиентов электронными средствами обязана уведомить Национальный банк Молдовы о соблюдении следующих требований:

a) доказательство того, что отчетная единица имеет соответствующие политики и процедуры дистанционной идентификации, которые будут реализовывать требования настоящего Регламента;

b) доказательство того, что отчитывающаяся организация провела предварительную оценку информационного решения в соответствии с п. 6.;

c) подтверждение того, что сотрудники отчетной единицы, ответственные за видеоидентификацию с использованием средств проверки с участием человека-оператора, прошли обучение в соответствии с пп. a) п. 32;

d) подтверждение того, что у отчетной единицы имеется достаточно места для проведения процедуры видеоидентификации с использованием средств проверки с участием человека-оператора, в соответствии с пп. b) п. 32;

e) подтверждение наличия у отчетной единицы соответствующих методов удаленной идентификации в соответствии с требованиями гл. IV.

50. Уведомление, установленное п. 49 настоящего Регламента, осуществляется только один раз, до начала отчетной единицей процедуры идентификации клиентов электронными средствами и реализации положений настоящего Регламента.

51. Аутсорсинг процесса идентификации и проверки личности клиентов электронными средствами осуществляется отчетной единицей согласно положениям применимых нормативных актов.

52. Отчетная единица немедленно прекратит использование информационного решения для установления дистанционных деловых отношений с использованием электронных средств с клиентами по запросу Национального банка Молдовы, если будет установлено, что оно представляет значительные риски для безопасности или целостности процесса идентификация и проверки личности лиц.